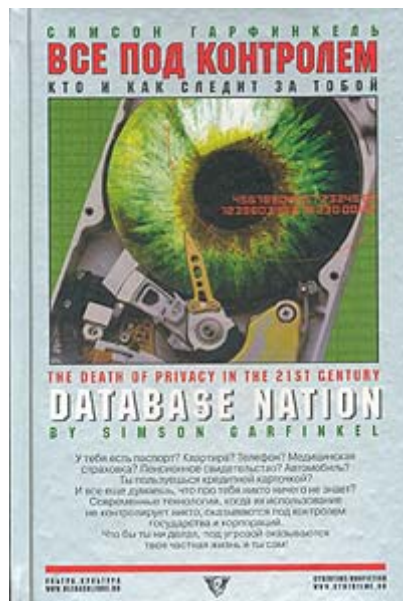


Симсон Гарфинкель Все под контролем: Кто и как следит за тобой



Симсон Гарфинкель Все под контролем: Кто и как следит за тобой

Серия киберtime/non-fiction <http://www.cybertime.ru> cybertime@mail.ru

Составитель: Владимир Харитонов

Данное издание выпущено в рамках проекта «Translation Project» при поддержке Института «Открытое общество» (Фонд Сороса) – Россия и Института «Открытое общество» – Будапешт.

Издательство «У-Фактория» выражает искреннюю признательность издательству O'Reilly в лице Синди Уэтерлунд и Кэтлин Келли за содействие и глубокую благодарность Издательству Уральского университета за организационное участие в издании этой книги.

Авторские примечания имеют цифровые сноски, сноски на примечания переводчика начинаются с «р» – прим. сост. FB2

К моим русскоязычным читателям

Для меня было большой честью узнать, что *Database Nation* переводится на русский язык, и особенно меня радует то, что вы, мой дорогой читатель, проявили интерес к этой книге.

Database Nation доказывает, что приватность является одним из базовых условий торжества демократии. Не будучи тщательно проверенными, технологии могут стать средством уничтожения приватности и разрушения демократии. Кому это хорошо известно, дорогой читатель, так это вам и другим людям, жившим во времена Советской империи. Как на членах одного из самых молодых демократических обществ в мире, на вас и ваших руководителях лежит особая обязанность обеспечения того, чтобы приватность и демократия сохранились в наступившем столетии.

Хотя книга, которую вы держите в руках, опубликована на русском языке, по мере чтения вы увидите, что многие примеры описывают Соединенные Штаты. К сожалению, здесь, в Соединенных Штатах, очень трудно узнавать о происходящем в России. Очевидным исключением, возможно, является спутниковая фотография Кембриджа (штат Массачусетс),

о которой говорится в главе 5. На этой фотографии, сделанной в 1989 году советским спутником-шпионом, изображен мой дом. Я сделал из нее большой плакат и гордо повесил на стену. Это доказательство того, что нарушающие приватность технологии не знают политических границ.

Еще раз благодарю вас за ваш интерес к приватности и за то, что вы решили прочитать *Database Nation*. Надеюсь, она вам понравится.

Симсон Гарфинкель
Массачусетс, 2003

1

Угроза неприкосновенности частной жизни

Вы просыпаетесь от телефонного звонка. Не может быть?! Несколько месяцев назад вы запрограммировали свой телефон таким образом, чтобы он не пропускал входящие звонки до 8 утра, однако на часах всего лишь 6:45. Кто может звонить в такое время? И самое главное, кто смог обойти блокировку звонков?

Вы снимаете трубку и тут же бросаете ее обратно – вас разбудила машина, проигрывающая рекламные сообщения. Реклама при помощи производимых компьютером телефонных звонков запрещена в Соединенных Штатах более десяти лет назад, но, после того как стоимость международных звонков упала ниже 10 центов за минуту, их поток хлынул в Северную Америку со всего мира. Причем почти все они – рекламные, вследствие большой популярности программируемых телефонных аппаратов. Но вас беспокоит еще одна проблема: как звонок прошел через установленный фильтр? Причину вы узнаете несколько позже: производитель купленного вами телефонного аппарата предусмотрел в его конструкции «черный ход», информация о котором отсутствует в документации. Зато информация о секретных кодах, позволяющих обойти защиту, продавалась неделю назад на онлайн-аукционе. Вы не обратили на это внимания и потеряли свой шанс выкупить свои спокойствие и неприкосновенность.

М-да...

Раз уж вы проснулись, вы решаете разобрать вчерашнюю почту. В ней обнаруживается письмо из ближайшей больницы. «Мы очень рады, что травматологическое отделение нашей больницы смогло оказать Вам необходимую помощь в нужный момент», – начинается письмо. «Как Вам известно, плата, которую мы берем в соответствии с Вашим НМО [Health Maintenance Organization], [p1] не покрывает наших расходов. Чтобы покрыть эту разницу многие больницы начинают продавать информацию о своих пациентах фирмам, занимающимся медицинскими исследованиями и изучением потребительского спроса. Вместо того чтобы следовать этой порочной практике, мы решили обратиться к Вам с просьбой помочь нам компенсировать разницу. Рекомендуемый размер пожертвования – 275 долларов – компенсирует стоимость Вашего обращения к нам. На эту же сумму будет уменьшен размер уплачиваемых Вами налогов».

Вы осознаете, что этот маленький шантаж не пустые слова, но не находите ничего особо страшного в том, что кто-то узнает о растяжении связок на вашем запястье. Вы сгибаете лист пополам и отправляете его в машинку для уничтожения бумаг в компании троицы малоинтересных предложений по кредитным картам.

Почему именно в машинку, а не просто в корзину? Еще несколько лет назад вам бы и в голову не пришло уничтожать бумажки с рекламными предложениями, пока с одним из ваших друзей не произошел неприятный инцидент: его личность «временно украли». Служащий жилого комплекса извлек из мусора полученные на имя вашего друга

p1

Форма коллективного медицинского страхования, подразумевающая определенный набор медицинских услуг для группы людей за фиксированную плату. – Здесь и далее примечания переводчика.

предложения по открытию кредитных карт, позвонил по указанному там бесплатному телефонному номеру, и ему доставили кредитные карточки. Сейчас он в Мехико, вместе с кучей дорогих вещей и электроники, приобретенных за счет вашего друга.

На этой радостной ноте вы берете свой портфель и направляетесь к двери, которая автоматически закрывается за вашей спиной.

Когда вы входите в лифт, скрытая видеокамера сканирует ваше лицо, автоматика идентифицирует личность и направляет лифт в подземный гараж. Попутчиков в лифте лучше избежать, ибо у вас нет желания повторить ситуацию, которая случилась на прошлой неделе с беднягой в доме 4G. Оказалось, что его соседка рассталась недавно со своим буйного нрава дружкой, и ему было запрещено приближаться к ней. Естественно, лифт был запрограммирован на опознание этого человека, и, когда он вошел в лифт, двери были заблокированы до приезда полиции. К несчастью, в этот момент в лифте находились и другие люди. Никто не мог предположить, что буйный нрав нарушителя не единственная его проблема, ко всему прочему он страдал не диагностированной вовремя клаустрофобией. Ситуация с захватом заложников развивалась очень быстро, но закончилась слишком плохо для мистера 4G. К счастью, все было записано на видеопленку.

Бортовой компьютер вашего автомобиля посоветовал три варианта маршрута поездки на работу сегодня утром. Вы выбрали не очень удачный и провели в автомобильных пробках более получаса. Во время вынужденного простоя компьютер каждые пять минут проигрывал рекламу булочек с начинкой, однако вы не могли его выключить: компьютер бесплатный и окупается за счет рекламы.

Ваше опоздание на работу не осталось незамеченным для корпоративной системы учета рабочего времени. В полученном от нее по электронной почте сообщении вам предлагалось несколько вариантов компенсации времени опоздания: не ходить сегодня на обед, задержаться на 45 минут вечером или вычесть это время из и так уже истощившегося отпуска. Выбор за вами.

Вы оглядываетесь по сторонам и выдавливаете на лице улыбку. Маленькая видеокамера на мониторе вашего компьютера транслирует изображение вашей улыбки боссу и коллегам. Считается, что Workplace Video Wallpaper™ способствует формированию духа товарищества, но компания-производитель этого программного обеспечения утверждает также, что постоянный мониторинг сокращает количество конфликтов на рабочем месте, предотвращает флирт и даже употребление наркотиков. Теперь на рабочих местах все улыбаются: не делать этого опасно.

Видеокамера лишь один из механизмов непрерывного мониторинга на работе. На книгах и журналах установлены электронные метки, призванные остановить постоянные хищения из библиотеки компании. После паники, случившейся в результате сообщения о бомбе, все служащие обязаны постоянно носить идентифицирующие таблички, а столы и шкафчики подвергаются периодическому досмотру. (Ходят слухи, что начальник службы безопасности сама организовала звонок с сообщением о бомбе, чтобы получить повод для введения новых порядков.)

В следующем месяце компания планирует установить в умывальных комнатах специальные устройства, которые будут следить, чтобы служащие мыли руки. Хотя первоначально эти устройства были разработаны для учреждений здравоохранения и пищевой промышленности, последние исследования показали, что регулярное мытье рук снижает распространение заболеваний среди офисных работников. Так что машины будут установлены, и с этого момента вы потеряете еще немного своей приватности и достоинства.

Это будущее. Причем не отдаленное, а самое ближайшее. Будущее, в котором исчезнут и те небольшие гарантии неприкосновенности частной жизни, которые мы имеем сейчас. Некоторые называют эту потерю «оруэллианской», имея в виду известный роман Джорджа Оруэлла [\[p2\]](#) «1984», посвященный утрате приватности и автономии. В этой книге Оруэлл

описывает будущее, в котором неприкосновенность частной жизни растоптана тоталитарным государством, использующим слежку, видеонаблюдение, исторический ревизионизм и контроль средств массовой информации для поддержания своей власти. Но времена тотального контроля со стороны государства прошли. В будущем, к которому мы движемся, опасность будет исходить не от всезнающего «Большого Брата», отслеживающего и записывающего каждый наш шаг, а от сотен «маленьких братьев», постоянно подглядывающих и вмешивающихся в нашу жизнь. Джордж Оруэлл считал, что главная угроза свободе индивидуальности исходит со стороны коммунистической системы. Но за последние 50 лет мы увидели новые виды угроз приватности, корни которых уходят совсем не в тоталитаризм, эти угрозы выросли на почве свободного капиталистического рынка, современных технологий и неконтролируемого обмена электронной информацией.

Что мы понимаем под словом приватность?

Приватность^[p3] занимает центральное место в этой книге, но это слово не до конца выражает аспект индивидуальной свободы, существование которой на пороге нового тысячелетия оказалось под угрозой со стороны передовых технологий.

Десятилетиями людей предупреждали, что развитие технологий проникающих повсюду баз данных и видеонаблюдения неизбежно приведет к смерти приватности и демократии. Но тогда у большинства людей слово «приватность» вызывало совсем другие ассоциации. В памяти всплывали рассказы о куках^[p4] – странных личностях, вооруженных дробовиками и ведущих отшельнический образ жизни в лесах. Эти люди получали почту в арендованных на вымышленное имя почтовых ящиках, сами производили все необходимое для жизни, а то, что не могли произвести самостоятельно, покупали исключительно за наличные деньги, при этом постоянно боялись быть атакованными федеральным правительством или космическими пришельцами. Если вы не один из этих оригиналов, вполне логичным с вашей стороны будет вопрос: «А почему я должен так волноваться о своей приватности? Мне нечего скрывать!»

Проблема кроется в самом слове «приватность», которое не передает всей полноты предмета обсуждения. Говоря о приватности, мы не имеем в виду просто сокрытие каких-либо фактов. Речь идет о праве на самоопределение, независимость и целостность. В компьютеризованном мире XXI века, на пороге которого мы стоим, право на приватность должно стать одним из важнейших гражданских прав. Но приватность – это не просто право людей закрыть двери и опустить занавески на окнах, потому что они, возможно, хотят заняться незаконными или просто неблагоприятными делами. Это право людей определять, какие подробности их жизни не должны покидать пределы их дома, а какие могут просачиваться наружу.

Чтобы понять роль приватности в XXI веке, мы должны еще раз осмыслить, что мы имеем в виду, употребляя это слово сегодня.

- Речь не идет о мужчине, желающем обеспечить себе полную анонимность при просмотре порнографических изображений через Интернет. Речь о женщине, которая не рискует использовать Интернет для организации группы протеста против свалки токсичных отходов, так как вкладывающие в этот бизнес деньги люди могут порыться в ее прошлом, если она станет помехой для них.

эссеист.

Русский перевод романа «1984» доступен на <http://lib.rus.ec/b/76207> (прим. составителя FB2)

p3

Privacy (англ.) – приватность, частная жизнь.

p4

Kooks (англ.) – чудаки, экстремисты.

- Речь не идет о людях, получающих по почте уведомления о штрафе за превышение скорости на магистрали, зафиксированное автоматизированной системой контроля скоростного режима. Речь о влюбленных, которые не могут в полной мере насладиться прогулкой по городским улицам и магазинам, так как знают, что каждый их шаг фиксируется камерами видеонаблюдения.

- Речь не идет о специальных обвинителях, перевернувших каждый камешек на своем пути в процессе расследования фактов коррупции и политических преступлений. Речь об обычных честных гражданах, которые отказываются идти на государственную службу, так как не хотят, чтобы кровавая пресса копалась в их старых ученических работах, медицинских записях в компьютере и электронной почте.

- Речь не идет о досмотрах, металлодетекторах и расследованиях, ставших обычным явлением нашей жизни в аэропортах, школах и зданиях федеральных учреждений. Речь об обществе, которое, рассматривая законопослушных граждан как потенциальных террористов, в то же время не делает практически ничего для защиты этих граждан от реальных угроз их безопасности.

Сегодня, как никогда ранее, мы наблюдаем, как приватность и личная свобода ежедневно подвергаются эрозии. Все мы – жертвы войны против приватности, которая ведется правительственными «прослушками», коммерсантами и просто любопытными соседями.

Многие из нас осознают эту угрозу. Согласно результатам проведенного Luis Harris & Associates в 1996 году общенационального опроса, четверть американцев (24 %) «лично столкнулась с вторжением в их личную жизнь»,¹ против 19 % по результатам опроса 1978 года. В 1995 году аналогичный опрос показал, что 80 % респондентов считают, что «потребители полностью потеряли возможность контролировать, как компании используют персональную информацию о них и кому она передается».² Ирония судьбы, но оба исследования были оплачены компанией Equifax, получающей ежегодный доход около двух миллиардов долларов именно на сборе и распространении персональных данных.

Итак, мы знаем, что неприкосновенность нашей личной жизни под угрозой. Проблема в том, что мы не знаем, как этой угрозе противостоять.

Роль технологий

Сегодняшняя война против приватности тесно связана с технологическим прогрессом последних лет. Как мы увидим далее в этой книге, неконтролируемое развитие технологий может положить конец приватности. Камеры видеонаблюдения фиксируют события личной жизни, компьютеры хранят личные данные, а сети телекоммуникаций дают возможность получить доступ к персональной информации по всему миру. Несмотря на то что некоторые специальные технологии могут быть использованы для защиты персональной информации, подавляющее большинство достижений в области современных технологий работают на противоположную цель.

Приватность тесно связана с индивидуальностью. Вся история разрушительного воздействия технологий на приватность, по сути, история того, как эти технологии использовались для установления контроля над человеческим духом, с благой целью или во вред. Действительно, технологии сами по себе не нарушают нашу приватность или что-то еще: технологии используют люди, а нарушения появляются в результате установления

¹ Harris-Equifax, *Consumer Privacy Survey*. Conducted for Equifax by Louis Harris and Associates in association with Dr. Alan Westin of Columbia University, Equifax, Atlanta, GA, 1996.

² Harris-Equifax, *Consumer Privacy Survey*. Conducted for Equifax by Louis Harris and Associates in association with Dr. Alan Westin of Columbia University, Equifax, Atlanta, GA, 1995.

неправильных процедур использования этих достижений.

Уже сегодня многие люди говорят, что, вместо того чтобы наслаждаться достижениями современного общества, мы обязательно должны позаботиться об обеспечении некоторой степени приватности. Если мы принимаем удобство покупки товаров по кредитной карте или оплату проезда по платной дороге при помощи электронного идентификатора на зеркале заднего вида, мы должны смириться с мыслью, что информация о наших покупках и маршрутах движения постоянно оседает в глобальной базе данных, контролировать использование которой мы не можем. Это, невинное на первый взгляд, соглашение очень похоже на сделку Фауста.

Я думаю, что эта сделка столь же ненужная, сколь и вредная. Он напоминает мне другой кризис нашего общества, имевший место в конце 50-х – 60-х годах XX века, – кризис окружающей среды. Тогда адвокаты большого бизнеса убеждали нас, что отравленные реки и озера – неизбежная плата за экономическое развитие, новые рабочие места и улучшение качества жизни. Отравление было эквивалентом прогресса: все, кто не соглашался с этим, просто не осознавали факты.

Теперь мы поумнели. Теперь мы знаем, что развитие жизнеспособной экономики *зависит* от сохранения окружающей среды. Действительно, сохранение окружающей среды – непреложное условие для сохранения человеческой расы. Без чистого воздуха и воды мы просто вымрем. Аналогично, когда человечество пожинает плоды современных технологий, для него как никогда важно использовать эти технологии для защиты личной свободы.

Развитие технологий обвиняется в покушении на приватность не впервые. В 1890 году двое юристов из Бостона, Самюэль Уоррен [Samuel Warren] и Луис Брэндис [Louis Brandeis], писали в *Harvard Law Review* о том, что приватность подвергается опасности «со стороны новых изобретений и методов ведения бизнеса». В своей публикации они утверждали, что состояние современного общества требует создания специального «права приватности», которое призвано помочь защитить то, что они называли «правом на приватность».³ Уоррен и Брэндис отказывались верить, что приватность должна отмереть в угоду технологическому прогрессу. Сегодня эта публикация считается самой влиятельной юридической статьей на эту тему среди когда-либо опубликованных.⁴ Ее важность и значимость возрастают с каждым годом, поскольку технологические достижения, которые вызывали беспокойство Уоррена и Брэндиса, становятся обычным делом.

Конечно, убивающие приватность технологии существуют не в вакууме, они тесно связаны с наукой, рынком и обществом. Люди создают новые технологии для удовлетворения специфических потребностей, более или менее реальных. Регулирование использования этих технологий происходит в зависимости от того, насколько общество в них нуждается.

Мало кто из инженеров стал бы специально создавать технологию, основным предназначением которой было бы разрушение приватности, мало кто из бизнесменов и потребителей стал бы ее использовать, если бы они осознавали последствия. Чаще всего наблюдается ситуация, когда про обеспечение приватности при использовании новой технологии забывают, или вспоминают, но не придают должного значения, или этот аспект учитывается, но все идет насмарку из-за ошибок при практической реализации. На практике одна ничтожная ошибка может превратить систему, разрабатываемую для защиты персональных данных, в систему, которая разрушает наши секреты.

Каким образом мы можем помешать техническому прогрессу нарушать нашу

³ Samuel Warren and Louis Brandeis, «The Right of Privacy», *Harvard Law Review* 4 (1890), 193. Несмотря на то что формулировка «право побыть одному» приписывается Уоррену и Брэндису, в статье утверждается, что впервые ее употребил в XIX веке судья Томас Кули [Thomas M. Cooley].

⁴ Turkington et al., *Privacy: Cases and materials*.

приватность в условиях свободного рынка? Один из путей – стать осторожными и информированными потребителями. Но я считаю, что не менее важную роль в этом процессе должно играть правительство.

Роль правительства

После всего того, что мы слышали о Большом Брате, можем ли мы думать о правительстве иначе, чем как о враге приватности? Несмотря на то что федеральные законы и деятельность государственных органов часто вредят приватности, я уверен, что наши лучшие надежды на защиту приватности в новом тысячелетии могут быть возложены именно на федеральное правительство.

Самая большая ошибка американского правительства в области защиты приватности состоит в том, что оно не стало развивать заложенную администрациями Никсона, Форда и Картера законодательную базу в этой области. Давайте посмотрим, каким образом она может послужить нам сегодня.

Семидесятые годы двадцатого века были для приватности и защиты прав потребителей прекрасным десятилетием. В 1970 году конгресс принял «Закон о точной отчетности по кредитам» [Fair Credit Reporting Act]. Элиот Ричардсон [Elliot Richardson], бывший в то время советником президента Никсона по вопросам здравоохранения, образования и социального обеспечения, создал в 1972 году комиссию по изучению влияния компьютерных технологий на приватность. После нескольких лет слушаний в конгрессе комиссия пришла к выводу, что повод для тревоги имеется, и в 1973 году выпустила заслуживающий внимания отчет.

Кодекс справедливого использования информации

Кодекс справедливого использования информации базируется на пяти принципах.

- Не должно существовать систем, накапливающих персональную информацию, сам факт существования которых является секретом.
- Каждый человек должен иметь возможность контролировать, какая информация о нем хранится в системе и каким образом она используется.
- Каждый человек должен иметь возможность не допустить использования информации, собранной о нем для одной цели, с другой целью.
- Каждый человек должен иметь возможность корректировать информацию о себе.
- Каждая организация, занимающаяся созданием, сопровождением, использованием или распространением массивов информации, содержащих персональные данные, должна обеспечить использование этих данных только в тех целях, для которых они собраны, и принять меры против их использования не по назначению.

Источник: Департамент здравоохранения, образования и социального обеспечения, 1973

Наиболее важным последствием отчета Ричардсона стал билль о правах в компьютерную эпоху, получивший название Кодекс справедливого использования информации [Code of Fair Information Practices]. Этот кодекс остается одним из самых значимых трудов в области обеспечения приватности при использовании компьютеров на сегодняшний день.

Однако наибольшее значение этот отчет имел не для Соединенных Штатов, а для Европы. В течение нескольких лет после публикации отчета практически все страны Европы приняли соответствующие законы, базирующиеся на изложенных выше принципах. Во многих странах для приведения в действие новых законов были созданы специальные комиссии по защите данных и другие учреждения со специальными полномочиями.⁵

⁵ David H. Flaherty, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, 1989).

Существует мнение, что повышенное внимание к электронному аспекту приватности в Европе обусловлено горьким опытом нацистской Германии в 40-е годы XX века: гитлеровская тайная полиция использовала информацию правительств и частных организаций в оккупированных странах для выявления людей, представлявших угрозу для оккупантов. Послевоенная Европа осознала всю потенциальную опасность накопления персональной информации даже самыми демократическими правительствами, прислушивающимися к общественному мнению.

Однако в Соединенных Штатах идея создания института защиты информации не была воплощена. Президент Джимми Картер проявлял интерес к вопросам обеспечения медицинской тайны, однако экономические и политические проблемы оказались более значимыми. В 1980 году Картер проиграл на выборах Рональду Рейгану, чья команда считала защиту приватности еще одной неудачной инициативой Картера. Несмотря на то что несколько законов в области защиты личной тайны были приняты во время правления Рейгана и Буша, это целиком заслуга конгресса, а не Белого дома. Пассивность законодательных инициатив со стороны Белого дома послужила причиной отсутствия общенационального закона о защите информации.

Фактически большая часть федерального правительства игнорировала важность обеспечения приватности, а некоторые словно бы придерживались какого-то «антиприватного» плана. В начале 80-х годов федеральное правительство инициировало ряд «компьютерообразных» программ для выявления злоупотреблений и мошенничеств. (К сожалению, из-за ошибочности данных от этих программ зачастую страдали невинные.⁶) В 1994 году конгресс принял «Закон о содействии правоохранительным органам в телекоммуникациях» [Communication Assistance to Law Enforcement Act], дававший

1989 году специальный уполномоченный по правам человека Британской Колумбии Дэвид Флаэрти сформулировал и позднее дополнил набор из 12 принципов и правил защиты информации для правительственных систем обработки персональных данных [Data Protection Principles and Practices for Government Personal Information Systems]. Эти принципы выглядят следующим образом (выделения курсивом добавлены Дэвидом Флаэрти в мае 1997).

- Принцип публичности и прозрачности (открытости) правительственных систем обработки персональных данных (не должно быть секретных баз данных).
- Принцип необходимости и релевантного управления процессами сбора и хранения персональной информации.
- Принцип минимизации количества собираемой, используемой и хранимой персональной информации.
- Принцип окончательности (цели сбора и последующего использования персональной информации должны устанавливаться заранее).
- Принцип назначения и контроля ответственных за эксплуатацию систем обработки персональной информации.
- Принцип контроля над объединением, пересылкой и взаимодействием массивов данных с персональной информацией.
- Принцип обязательного получения согласия субъекта на сбор персональной информации.
- Принцип соблюдения точности и законченности для систем обработки персональной информации.
- Принцип ответственности за нарушение правил работы с персональной информацией, включая гражданскую и уголовную ответственность.
- Обязательность наличия специальных правил защиты персональных данных, являющихся конфиденциальными.
- Право на доступ к своей информации и ее корректировку.
- Право стать забытым, включая полную анонимизацию или уничтожение почти всей персональной информации.

⁶ Одна из таких федеральных программ сравнивала базу данных, содержащую имена людей, не выплативших свои долги за обучение в колледже, с именами федеральных служащих из другой базы данных. В случае совпадения соответствующая сумма автоматически высчитывалась из заработной платы служащего. Проблема этой программы, как и многих других, была в том, что зачастую эти совпадения были ошибочными по причине некорректно введенных данных, созвучных и совпадающих имен. Поскольку вычеты производились автоматически, жертвы совпадения должны были доказывать свою невиновность, т. е. ошибочность совпадения.

правительству невиданные доселе полномочия по перлюстрации данных в цифровых каналах связи. В 1996 году конгресс принял закон, обязывающий все штаты помещать номер социального страхования на водительские права, и другой закон, согласно которому всем пациентам должен был быть присвоен уникальный цифровой идентификатор, даже если они сами оплачивали свои медицинские счета. К счастью, вступление этих законов в силу было отложено во многом благодаря протестам граждан.

Эту политику продолжили администрации Буша и Клинтона, всеми средствами попиравшие право пользователей компьютеров на использование частных и безопасных коммуникаций. Начиная с 1991 года обе администрации усиленно проталкивали инициативу на применение криптографической системы Clipper, которая в случае внедрения давала бы правительству возможность контролировать защищенные коммуникации. Президент Клинтон подготовил также «Закон о пристойности в сфере коммуникации» [Communication Decency Act, CDA], согласно которому предоставление несовершеннолетним доступа к информации сексуального характера объявлялось преступлением, и, как следствие, от всех Интернет-провайдеров требовалась установка всепроникающих систем мониторинга и цензуры. После того как суд Филадельфии признал этот нормативный акт неконституционным, администрация Клинтона обратилась с апелляцией в Верховный суд и проиграла.

Наконец, введенные правительством США ограничения на экспорт шифровальных технологий серьезно ограничили их использование для защиты личной переписки за пределами Соединенных Штатов.

На пороге XXI века Соединенные Штаты должны вновь и очень серьезно задуматься об обеспечении личной тайны. В последней главе этой книги приводятся возможные пути выхода из этой ситуации и предлагаются шаги, которые правительство должно осуществить на уровне федеральной программы обеспечения приватности.

Оборона

Проблема обеспечения приватности в Америке стоит так же остро, как с охраной окружающей среды в 1969 году. Тридцать лет назад река Куяхога в штате Огайо была охвачена огнем, а озеро Эри было объявлено мертвым. Но времена меняются: сегодня вполне безопасно есть выловленную в Куяхоге рыбу, озеро Эри снова ожило, а общее состояние окружающей среды в Америке намного лучше, чем несколько десятилетий назад.

Все вокруг говорит о том, что ситуацию с обеспечением приватности пора приводить к нормальному состоянию. Тема войны против приватности все чаще поднимается в печати, на телевидении и в Интернете. Люди все больше осознают, что их личная свобода ежедневно подвергается ущемлению. Многие начинают самостоятельно принимать простейшие меры защиты, вроде расчетов наличными деньгами и отказа предоставлять свой номер социального страхования (или называют вымышленный). При этом небольшая, но постоянно увеличивающаяся часть общества не просто говорит о технологиях, *обеспечивающих* приватность, она переходит от слов к делу, создавая системы и сервисы, которые не посягают на приватность, а, наоборот, обеспечивают ее.

Последние десятилетия научили нас тому, что технология – вещь гибкая, и все факты нарушения ею приватности являются результатом сознательного выбора. В частности, мы знаем, что, когда представитель банка говорит нам: «Мне очень жаль, но, несмотря на то, что Вы против печати Вашего номера социального страхования на выписке о состоянии Вашего банковского счета, мы не можем изменить форму», – это на самом деле означает: «Наши программисты включили печать номера социального страхования в форму выписки по ошибке, но мы не считаем это серьезным поводом для внесения изменений в программу. Как-нибудь в другой раз».

Сегодня мы переосмыслили этот урок и поняли, что большой бизнес и правительство все-таки поддаются давлению общественности. Рассмотрим три примера из последнего

десятилетия.

Lotus Development Corporation. В 1990 году Lotus и Equifax решили выпустить на лазерном диске информационный продукт под названием «Рынок Lotus: домохозяйства» [Lotus Marketplace: Households], который включал бы в себя имена, информации. Вскоре большинство людей просто не сможет нигде укрыться от всевидящего ока.

Нецелевое использование медицинских записей. Медицинские записи традиционно считались наиболее характерным видом конфиденциальной информации. Обязательство хранить врачебную тайну всегда рассматривалось как одно из ключевых требований к медицинскому работнику. Но обеспечение конфиденциальности пациента идет вразрез с интересами индустрии медицинского страхования: в этом виде бизнеса экономически выгоднее отвернуться от больного, чем лечить его.

Бесконтрольная реклама. Рекламные буклеты в почте, реклама по факсу, рекламные сообщения в электронной почте, рекламные звонки по телефону во время обеда – лишь начало широкомасштабной и бесконтрольной рекламной кампании. Маркетологи все больше и больше будут использовать персональную информацию для навязчивых рекламных предложений, которые будет трудно отделить от подборок новостей, личных писем и другой некоммерческой корреспонденции.

Персональная информация как товар. Идентифицирующая личность информация: имя, профессия, хобби и другие мелочи, делающие человека уникальным, – все это превратилось в ценный объект владения. Но владеют этим объектом не конкретные индивидуумы, контролирующие информацию о себе, а крупный бизнес, постоянно использующий его для получения прибыли и захвата рынка. Как можно ощущать собственную ценность, не владея в полной мере даже собственным именем?

Генетическая автономия. Прорыв в области генных исследований позволяет очень точно определять наследственные заболевания, особенности характера, уровень интеллекта и другие человеческие черты. Можно ли воспринимать человека непредвзято и адекватно, если имеются неопровержимые научные доказательства наличия у него определенных сильных и слабых сторон, предрасположенности к некоторым заболеваниям? Если нет, то как при наличии свободного доступа к этой информации нам построить демократическое общество?

Микроуправление интеллектуальной собственностью. Корпорации очень бдительно следят за правоммерностью использования своей интеллектуальной собственности. Но с пиратством чрезвычайно сложно бороться, когда технология позволяет любому потребителю стать распространителем интеллектуальной собственности. Чтобы предотвратить ее хищение, правообладатели задействуют самые изощренные технологии слежки за клиентами. А поскольку технология уже существует, маловероятно, что ее применение будет ограничено лишь защитой от пиратства.

Личность как потенциальный террорист. Наша цивилизация располагает огромным количеством смертоносных технологий. Как общество может защитить себя от угрозы террористических актов, кроме как постоянно наблюдать за каждым? Можем ли мы противостоять систематическим злоупотреблениям со стороны правоохранительных органов, даже если они происходят в интересах всего общества?

Интеллектуальные машины. Серьезную угрозу приватности представляют компьютеры, приближающиеся по своим возможностям к человеческому разуму. Обладая огромной вычислительной мощностью, они в состоянии строить связную картину окружающего мира, интерпретировать и имитировать человеческое сознание настолько правдоподобно, что могут ввести человека в заблуждение относительно их природы.

Этот перечень не охватывает всех проблем, которые могут ожидать нас в будущем. Одной из причин написания данной книги было желание показать, как многие из бурно развивающихся технологий могут неожиданно оказать серьезное влияние на приватность и продемонстрировать недопустимость подхода к решению проблемы обеспечения приватности по остаточному принципу. Теперь вы знаете, что несет нам технологическое будущее, и подготовлены к нему.

Подзаголовок этой книги предрекает смерть приватности в XXI веке, однако цель написания книги – достигнуть противоположного результата. Около 40 лет назад книга Рэйчел Карсон [Rachel Carson] «Безмолвная весна» [*Silent Spring*] дала толчок развитию движения в защиту окружающей среды. Именно благодаря всем нам предсказанная Карсон безмолвная весна никогда не настанет. «Безмолвная весна» достигла своей цели, так как помогла людям осознать все коварство влияния пестицидов на экосферу Земли, помогла нашему обществу и нашей планете изменить курс в сторону лучшего будущего.

В этой книге сделана аналогичная попытка показать все множество способов, которыми развитие технологий может лишить нас одной из наиболее ценных свобод. Назовете ли вы эту свободу правом цифрового самоопределения, правом на информационную независимость или просто правом на приватность, форма нашего будущего существования в значительной степени зависит от того, насколько глубоко мы осознаем угрозу, с которой столкнулись уже сегодня, а главное, насколько эффективно сможем ей противостоять.

2

Нация баз данных

Вашингтон, федеральный округ Колумбия, 1965 год. Предложение Бюджетного бюро [Bureau of the Budget] было столь же простым, сколь и революционным. Вместо того чтобы выделять каждому ведомству средства на приобретение компьютеров, создание технологий хранения данных, зарплату обслуживающего эту инфраструктуру персонала, правительству Соединенных Штатов предлагалось сформировать Национальный информационный центр [National Data Center]. Проект должен был начаться с объединения информации из различных ведомств: данных о населении и его размещении из Бюро переписи населения [Bureau of the Census]; данных о трудоустройстве из Бюро трудовой статистики [Bureau of Labor Statistics]; данных о налогах и сборах из Налогового управления [Internal Revenue Service] и информации о выплатах из Управления социального страхования. В дальнейшем предполагалось хранить и другую информацию.

Несмотря на то что изначальная цель заключалась в простом снижении издержек, очень скоро стало ясно, что проект таит в себе и другие выгодные моменты. Из общенационального массива данных можно легко и точно получать статистическую информацию. Создание единой общенациональной базы данных позволяет избежать трудностей, возникающих из-за неправильного написания имен, и других проблем, характерных для крупномасштабных банков данных. Единая база данных также позволяет правительству (и не только ему!) использовать накопленную информацию самым эффективным образом.

Принстонский институт перспективных исследований [Princeton Institute for Advanced Study] опубликовал отчет, с энтузиазмом поддерживающий проект создания базы данных, в котором говорилось, что централизованное хранение информации обеспечит более высокий уровень ее безопасности и таким образом лучше обеспечит приватность в национальном масштабе. Карл Кайзен [Carl Kaysen], директор института и руководитель исследовательской группы, утверждал также, что конгресс примет необходимые законодательные акты, которые обеспечат дополнительную защиту информации в базе, гарантируют ее приватность и обеспечат подконтрольность обслуживающего базу персонала. Зацикливание на идее привело к тому, что концепция Национального информационного центра переросла в желание создать огромный банк данных, содержащий самую подробную информацию о каждом гражданине США от момента рождения и до смерти. В базе данных должны были храниться: электронное свидетельство о рождении каждого гражданина, свидетельство о гражданстве, школьные оценки, данные о воинской обязанности и прохождении военной службы, записи о налогах, социальных выплатах, информация о владении недвижимостью и,

конечно, запись о смерти. ФБР могло бы даже использовать систему для хранения информации о преступлениях.

Рекламирующая проект статья появилась в *Saturday Review* 23 июля 1966 года. Ее заголовок объяснял все: «Автоматизированное правительство: Как компьютеры будут использоваться Вашингтоном для упрощения управления человеческими ресурсами на благо каждого». ⁷ Но статья не достигла своей цели. Вместо восторженной поддержки технократического подхода конгресс США инициировал серию слушаний по проблеме угроз, возникающих при использовании компьютерных банков данных. Шесть месяцев спустя *New York Times Magazine* опубликовал статью под заголовком «Не говори об этом компьютеру», злобно атаковавшую правительственную идею централизованного накопления информации. Написанная Вэнсом Паккардом [Vance Packard], автором «Обнаженного общества» [*The Naked Society*] (бестселлер, описывающий, как правительство, бизнес и образовательные учреждения вторгаются в личную жизнь), публикация в *Times* акцентировала внимание на ключевом аргументе против проекта:

Самой страшной опасностью централизованного накопления информации в компьютерных базах данных является сосредоточение огромной власти в руках людей, управляющих этими компьютерами. Когда все детали нашей жизни будут помещены в центральный компьютер или другую глобальную систему хранения информации, мы все в некоторой степени попадем в зависимость от людей, контролирующих эти машины.⁸

Времена изменились. Уже в 1968 году Бюджетное бюро заявило, что сомневается в том, что план практической реализации центра будет представлен на рассмотрение конгрессу. Тем временем специальный подкомитет палаты представителей по защите неприкосновенности частной жизни [House Special Subcommittee on Invasion of Privacy] выпустил отчет, в котором говорилось, что обеспечение приватности должно стоять на одном из первых мест при разработке проектов компьютерных банков данных, работы по созданию Национального информационного центра должны быть приостановлены до тех пор, пока проект не сможет гарантировать приватность, а Бюджетное бюро совершило ошибку, не разработав предварительно процедуры обеспечения приватности.

Опрос, проведенный Гарвардским университетом в рамках программы изучения взаимодействия технологий и общества, показал, что 56 % американцев против создания Национального информационного центра, так как он нарушит неприкосновенность личной жизни. В этом же году Джерри Розенберг [Jerry M. Rosenberg] предупреждал в своей книге «Смерть приватности» [*The Death of Privacy*]:

Когда Адольф Гитлер стремился заполучить пост канцлера Германии, он воспользовался конфиденциальной информацией, полученной в процессе европейской переписи, для устранения некоторых своих противников.

С развитием технологий процедуры централизованного сбора данных упрощаются, последствия злоупотреблений становятся более тяжелыми, а все нити управления сосредотачиваются в руках небольшой группы людей.⁹

Национальный информационный центр так и не был построен. Вместо этого каждое ведомство продолжало развивать свои собственные компьютерные системы. Взамен создания единого банка данных, который мог быть использован не слишком стесняющимся в выборе средств бюрократическим аппаратом для осуществления незаконного контроля над

⁷ «Automated Government – How Computers Are Being Used in Washington to Streamline Personnel Administration to the Individual's Benefit», *Saturday Review*, 23 июля 1966.

⁸ Vance Packard, «Don't Tell It to the Computer», *New York Times Magazine*, 8 января 1967.

⁹ Rosenberg, *The Death of Privacy*, p. 1.

судьбами отдельных людей, правительство учредило десятки банков данных.

Американский бизнес последовал примеру правительства, зачастую приобретая компьютерные системы, которые изначально были разработаны для удовлетворения нужд правительства. Политическое решение не создавать централизованное хранилище информации определило курс, которым компьютерные технологии следовали дальнейшие 30 лет. Проект централизованной базы данных подтолкнул бы развитие сверхкрупных вычислительных комплексов и высокоскоростных телекоммуникационных сетей, однако до конца 80-х годов разработчики создавали компьютеры меньшего, регионального, масштаба, практически не связанные между собой сетями. Но решение похоронить проект оказало глубокое влияние на обеспечение приватности личности, пусть это влияние и оказалось неожиданным.

Тридцать четыре года спустя

Сиэтл, 1999. Я заказал две порции кофе с молоком и белым шоколадом и протянул бармену в качестве оплаты карточку Mileage Plus First Card. Несмотря на то что напитки стоили всего по 3 доллара каждый, я предпочел заплатить комиссию за транзакцию вместо использования наличных денег. Каждая покупка по карточке приносила мне бонус, и менее чем за год я накопил более 50 тысяч миль по программе часто летающих пассажиров – достаточно для приобретения нам с женой билетов «туда и обратно» в любую точку Соединенных Штатов. Лет тридцать назад идея отслеживания при помощи компьютера каждой совершаемой покупки показалась бы частью оруэлловского кошмара. Пятьдесят лет назад гениальный математик доктор Дэвид Чом [Dr. David Chaum] придумал электронную наличность, E-Cash, – анонимную систему платежей, позволяющую потребителям совершать покупки электронно, не идентифицируя себя при этом. Кто мог предположить, что настанут времена, когда миллионы людей не только не будут возражать против отслеживания всех их покупок, а будут даже проявлять недовольство, если информация о транзакции теряется? Это только один из весьма интригующих результатов так называемых «программ приверженности», ярким примером которых является система кредитных карт United: созданные ею банки данных дают подробную электронную картинку пристрастий потребителей, и эта картинка создана благодаря поддержке и участию самих исследуемых.

Я всегда звоню маме, когда возвращаюсь домой. Я знаю, что записи о сделанных мною звонках останутся в компьютере телефонной компании, но эта мысль лишь мелькает где-то в глубине сознания. Скорее всего, записи о моих звонках никогда не будут просматриваться людьми, но почти каждый месяц я слышу об очередном крупном преступлении, когда вина подозреваемого была доказана в том числе и благодаря записям телефонной компании. В частности, во время следствия по факту взрыва федерального здания Murrah в Оклахома-Сити в 1995 году одним из самых весомых доказательств, представленных обвинением, были записи о звонках, сделанных Тимоти Маквеем [Timoty McVeigh] и Терри Николсом [Terry Nichols] по предоплаченным телефонным картам. Экстремисты правого толка полагали, что звонки, сделанные по этим картам (приобретенным за наличные), являются анонимными и неотслеживаемыми. Но на самом деле информация о каждом сделанном по такой карте звонке тщательно хранилась. Обвинение представило многостраничную распечатку звонков, сделанных на гоночные трассы, в химические компании, мотели, склады и платные стоянки грузовиков.¹⁰ Эти записи позволили обвинению доказать, что Маквей и Николс постоянно контактировали по телефону в течение нескольких месяцев, предшествовавших террористическому акту, унесшему самое большое

¹⁰ «McVeigh Prosecutor Cries During Trial», Associated Press, 8 мая 1997. Материал доступен в Интернет по адресу http://herald-mail.com/news/11997/bombing_trial/stories/may8_97.html.

число жизней из всех терактов в истории США[p5].¹¹

В 1960-е годы большая часть компьютеров в стране принадлежала правительству. Комментаторы предупреждали, что централизация персональной информации может создать почву для появления в будущем тоталитарного режима. «У меня предчувствие, что если Большой Брат все-таки появится в США, то это будет не тиран, жадно рвущийся к власти, а помешанный на эффективности неутомимый бюрократ», – писал Вэнс Паккард в своей статье в *New York Times Magazine*.

Публикации других журналистов, подобные статье Паккарда, помогли похоронить создание Национального информационного центра, но они не остановили прогресс. Сегодня огромное множество компьютеров, принадлежащих банкам, коммунальным службам и частному бизнесу, ежесекундно фиксирует невообразимый объем информации о каждом из нас. Во многих случаях в компьютерах остается и персональная информация. Вместо национального банка данных мы создали другого монстра – нацию банков данных.

Как мы дошли до этого

Если вы хотите обвинить кого-то в компьютеризации Америки, предъявите свои претензии Джорджу Вашингтону и другим авторам конституции. В 1787 году Вашингтон с единомышленниками объявил, что новая республика должна проводить перепись населения каждые десять лет. В то время это было достаточно просто, но, поскольку и территория, и численность населения Соединенных Штатов выросли, сложность переписи возросла многократно.

Проблема заключалась не во все возрастающем количестве ищущих свободы, заполонивших американские порты. Подобно другим правительственным программам перепись приобрела затяжной характер. К 1880 году она перестала быть простым подсчетом жителей: она стала инструментом более подробного изучения нации. Конгресс постановил фиксировать в данных переписи также пол, семейное положение, возраст, место рождения, образование, занятость и уровень грамотности. Вся эта информация направлялась в Вашингтон для оформления в виде таблиц. Процесс осуществлялся практически вручную: клерки выполняли над карточками однообразные операции, подсчитывая число ответов, попадающих под определенный критерий. От начала до завершения проходило 18 недель, при этом совершалось большое число ошибок, выполнять работу становилось все сложнее.



Герман Холлерит – ученый и изобретатель, сотрудник Службы переписи США, создавший машину, автоматизировавшую рутинные операции по обработке

p5

Книга Гарфинкеля была опубликована еще до терактов 11 сентября 2001 года, в результате которых погибло более двух тысяч человек.

¹¹ «Answers for the Evidence», *Detroit Free Press*, 17 декабря 1997. Материал доступен в Интернет по адресу <http://www.freepress.com/news/bombtrial/qcase17.htm>.

карточек переписи населения. Исследования Холлерита по созданию машины практически разорили его семью, но в конечном счете привели к созданию в 1896 году его собственной компании – Tabulating Machine Company. Впоследствии она была приобретена другой компанией, получившей позже название International Business Machines Corporation (IBM). [Фото любезно предоставлено Музеем компьютеров (Бостон, Массачусетс) и Историческим центром (Маунтин-Вью, Калифорния)]

Герман Холлерит пришел в службу переписи в 1879 году молодым выпускником Columbia College. Он сразу же понял основную проблему процесса переписи и загорелся идеей создать машину, которая могла бы автоматизировать работу клерков. В течение года он исследовал проблему, а затем еще год изучал машиностроение в Массачусетском технологическом институте [MIT]. Возвратившись в Вашингтон, Холлерит проработал год в Патентном управлении, потом оставил госслужбу и с 1884 года занялся изобретательством как основной деятельностью.¹²

Холлерит изобрел способ хранения информации путем пробивания определенным образом отверстий в листах плотной бумаги. Подсчитывая затем эти отверстия по различным критериям, можно было получать всю статистическую информацию, необходимую службе переписи. В 1889 году он выиграл объявленный службой переписи тендер и получил контракт на автоматизированную обработку карточек переписи с помощью своих машин в следующем году. Машинная обработка данных заняла всего шесть недель, и Холлерит стал известной в мире фигурой среди специалистов по переписи.

В 1896 году Холлерит преобразовал свой бизнес в корпорацию – Tabulating Machine Company. В 1911 году он продал свою компанию, получив за нее 1 миллион долларов и предложение сотрудничать с правопреемником – Computing-Tabulating-Recording Company (CTR). Три года спустя CTR наняла Томаса Уотсона [Thomas J. Watson], который в 1924 году переименовал ее в International Business Machines Corporation (IBM).

В 1920-е годы IBM продолжила совершенствование выпускаемых табуляторов и поиск новых рынков для своего оборудования. Фирма создала печатающий табулятор Type 1, который выводил результаты на бумагу, сортировщик Type 80, который сортировал стопку карточек в зависимости от пробитых в них отверстий. В 1928 году IBM разработала карточку с 80 колонками и 10 строками. Перфокарты этого формата применялись вплоть до 1980-х годов. (Эти 80 колонок живы по сей день: валки терминала первого телетайпа имели ширину 80 колонок, так же как и первый видеотерминал. Когда в 1981 году IBM стала продавать персональные компьютеры, ширина их экрана, естественно, тоже составила 80 символов.)

Забавно, но IBM осуществила рывок в своем развитии как раз во времена Великой депрессии. Треть рабочих лишилась своих рабочих мест, люди голодали. Тогда президент Франклин Д. Рузвельт заложил основы современных социальных гарантий со стороны государства.

В 1935 году конгресс одобрил предложенный Рузвельтом «Закон о социальном страховании» [Social Security Act]. В соответствии с положениями этого закона работодатель обязан был вычитать из выплат каждому работнику определенный процент, добавлять к нему свою «прибавку» и направлять эти суммы в правительственный Фонд социального страхования [Social Security Trust Fund]. Именно из этих денег Министерство социального страхования (так в то время называлось Управление социального страхования) выплачивало пособия по безработице, нетрудоспособности и потере кормильца.

Очень сложным моментом в деятельности молодого министерства было обеспечение персонального учета перечисленных в Фонд средств, так как размер социальных выплат

¹² Charles J. Bashe, Lyle R. Johnson, John H. Palmer, Emerson W. Pugh, *IBM's early computers* (Cambridge: MIT Press, 1986).

конкретному работнику зависел частично и от этого показателя. Это означало, что Министерство социального страхования должно не только отслеживать доходы каждого работника, но и хранить эту информацию, начиная с первого дня его трудовой деятельности и в течение достаточно большого периода после его смерти, пока семья получала выплаты по потере кормильца.

Перфокарта

Предложенные Холлеритом перфокарты были основным носителем информации для табуляторов и компьютеров со второй половины 80-х годов XIX века и до 60-х годов XX века, когда их заменили магнитные ленты. Изображенная выше перфокарта использовала формат (стандартизованный в 1928 году) с 80 колонками и 10 строками. Отверстие в определенном столбце и строке представляет отдельное число, а комбинация отверстий в одной строке – букву. Перфокарты широко использовались вплоть до 80-х годов XX века, в некоторых системах используются до сих пор. [Перфокарта любезно предоставлена Брэдли Россом (Bradley Ross)]

С момента образования в 1936 году Министерство социального страхования сразу же стало «крупнейшей бухгалтерской конторой в мировой истории». ¹³ Министерство рассчитывало, что ему придется иметь дело с 25 миллионами работников, однако цифра составила 45 миллионов. ¹⁴ Для обеспечения достоверности учета министерство присвоило каждому работающему номер социального страхования [Social Security Number, SSN]. Номер отсылался каждому работнику, а также пробивался на специальной «накопительной» перфокарте. Каждый год Министерстве социального страхования поднимало карточку каждого работающего и пробивало в ней информацию о полученных в течение этого года доходах. К 1943 году министерство оперировало более чем 100 миллионами карт, для хранения которых требовалась площадь примерно в два с половиной гектара.

В 1951 году конгресс изменил правила расчета социальных выплат. Эти изменения потребовали хранения на перфокарте дополнительной информации, и уже через пять лет на карте не оставалось места. Управление социального страхования, в которое недавно было переименовано министерство, не могло заводить на каждого работающего дополнительные карточки, так как это привело бы к резкому увеличению площадей, необходимых для их хранения. У системы социального страхования просто не осталось другого выбора, как обратить свое внимание на молодую отрасль – электронную обработку данных и недавно созданный IBM ламповый компьютер первого поколения – IBM 705. С этого момента история трудовой деятельности нации стала храниться не на перфокартах, а на магнитных лентах. Машины были установлены в 1956 году, как раз в тот момент, когда первые перфокарты уже были заполнены до 80-й колонки.

Рост популярности номеров социального страхования

Изначально не предполагалось использовать номера социального страхования (SSN) в качестве универсального идентификатора для каждого американского гражданина, однако буквально через 10 лет они стали таковыми.

• В 1943 году президент Рузвельт издал распоряжение, обязывающее все федеральные ведомства использовать номера социального страхования для идентификации граждан, вместо разработки дорогостоящих систем нумерации для каждого отдельного ведомства.

¹³ Social Security Administration official history. Материал доступен в Интернет по адресу <http://www.ssa.gov/history>.

¹⁴ Westin, Alan R, *Databanks in a Free Society*, p. 33.

- Министерство обороны отказалось от использования «серийных номеров» и перешло на использование номеров социального страхования.
- Министерство по делам ветеранов [Veterans Administration] стало использовать SSN для учета выплат уволенным военнослужащим.
- Федеральное управление авиации [Federal Aviation Administration, FAA] приняло SSN в качестве номеров лицензий пилотов.
- Комиссия по гражданской службе [Civil Service Commission] приняла SSN в качестве основного идентификатора для федеральных служащих.

Еще в начале этого процесса некоторые статистики склонялись к мнению, что выбор номера социального страхования в качестве общенационального идентификатора не очень удачен. Первая проблема заключалась собственно в номере 9-значного числа было явно недостаточно для учета всех граждан, всех временно въезжающих в страну и всех нерезидентов до конца XXI века. Вследствие малой длины SSN любое случайным образом выбранное число с большой вероятностью могло оказаться реально существующим SSN, что давало повод для различного вида мошенничества и уклонения от налогов. Другая проблема связана со способом присвоения SSN. В отличие от повсеместно распространенной практики присвоения идентификатора при рождении, SSN присваивался после направления письма в Управление социального страхования. В результате люди получали SSN в разное время, а многие вообще его не имели! И последний недостаток SSN: отсутствие так называемого «контрольного разряда» – цифры, которая не несет информации, но подтверждает корректность остальных цифр в номере. Без этой меры обнаружить опечатку в номере не представляется возможным. Все эти недостатки лишь увеличивали объем недостоверной информации, которая сохранялась в базах данных с SSN в качестве глобального идентификатора. Эти факты подтверждают, что SSN не годится на роль идентификатора, даже в своей изначальной ипостаси – для учета пенсионных и социальных выплат.

Исходя из этих соображений в 1948 году Национальная служба по учету населения [National Office of Vital Statistics] предложила использовать номера свидетельств о рождении. С 1 января 1949 года каждое свидетельство о рождении должно были получать уникальный номер, и в течение нескольких лет эти номера заменили бы собой SSN.

Но страна не захотела принять универсальный национальный идентификатор, который был хорошо спроектированным и управляемым. Профессор Колумбийского университета Алан Уэстин [Alan Westin] писал в 1967 году:

В 1949 и 1950 годах идея была подвергнута критике в газетах как направляющая нас по пути создания «полицейского государства», возбужденные карикатуристы пугали образом «Большого Брата». Оппозиция была достаточно сильна, чтобы убедить 24 штата отказаться от участия в реализации плана. Конгрессу пришлось отказаться от законодательной инициативы, выдвинутой для реализации этой федеральной программы.¹⁵

В 1961 году Налоговое управление попыталось вновь вернуться к этой теме и ввести свои собственные идентификационные номера. Однако этот план был отклонен как слишком затратный, а управлению было предписано использовать SSN, что оно и сделало в следующем году.

Хорошо это или плохо, но правительству было слишком трудно использовать SSN для идентификации граждан в своих компьютерных системах. Использование имен было невозможно: разные люди могли иметь одинаковые имена, их написание могло случайно или преднамеренно изменяться, наконец, компьютерам в то время просто трудно было работать с именами. Однако никто не был в восторге от «цифровой» альтернативы. В 1969 году, отвечая на вопрос исследователя из Гарвардского университета, один из респондентов из

¹⁵ Westin, Alan R, *Privacy and Freedom* (New York: Atheneum, 1967), p. 304.

Бостона замечательно сформулировал проблему:

Ладно, они уже имеют в своем распоряжении всю информацию... [и] если они захотят свести ее воедино, то мы все равно ничего не сможем с этим поделать. Но я не хочу носить номер, у меня есть имя. Это имя принадлежит мне, и больше никому. Я предпочитаю носить это имя до самой моей смерти, и не желаю, чтобы меня идентифицировали по номеру социального страхования.¹⁶

Америка принимает SSN

Правительство США было не единственной организацией, использующей номера социального страхования. Многие штаты использовали SSN для учета внутренних налогов и номеров водительских удостоверений; в библиотеках SSN использовались в качестве номеров библиотечных карт; учебные заведения и больницы использовали SSN в качестве идентификаторов студентов и пациентов. В мире частного бизнеса самыми агрессивными пользователями SSN стали кредитные бюро, которые компьютеризировали свою деятельность в 1960-х годах и обнаружили, что SSN очень удобны при обработке информации.

Конечно, учет кредитов начался не в 1960-х. Американцы делали крупные покупки в кредит со времен окончания Гражданской войны. С наступлением нового века кредитные бюро по всей стране хранят досье на американских граждан, в которых фиксируются их доходы и платежеспособность. Для упрощения обмена информацией о потребительских кредитах кредитные бюро даже создали свою организацию – Ассоциацию кредитных бюро [Associated Credit Bureaus, ACB].

К 1969 году бизнесмены широко использовали информацию кредитных бюро, но большинство американцев имели смутное представление о том, какая информация там хранится, равно как и о самом факте существования кредитных досье. Естественно, политика многих кредитных бюро не допускала ознакомления потребителей с собранной о них информацией.

Основной причиной такой секретности было содержание досье. Компании утверждали, что досье содержат фактическую информацию: невыплаченные займы, задержки компенсации платежей по кредитным картам, информацию о частой смене адресов людьми, скрывающихся от кредиторов. Однако профессор Алан Уэстин, выступая перед конгрессом в марте 1970 года, заявил, что «досье могут содержать факты, статистику, недостоверную информацию и слухи... практически обо всех сферах жизни человека: семейных проблемах, работе, школьных годах, детстве, сексуальных пристрастиях и политической деятельности». Очевидно, бизнесмены в то время считали, что если человек ударил свою супругу или имеет определенные сексуальные пристрастия, то он, вероятно, ненадежный заемщик. Неудивительно, что бизнесмены скрывали от общественности, какая именно информация собирается об американцах.

С 1965 по 1970 годы три сенатских комитета и законодательные органы пяти штатов провели серию слушаний, посвященных развитию индустрии сбора информации о кредитах.¹⁷ Законодатели пытались разобраться в этой ранее засекреченной индустрии. Главным свидетелем на большинстве этих слушаний был профессор Алан Уэстин, по-кавалерийски лихо атаковавший скрупулезность сбора информации о потребителях и подвергавший резкой критике практику, когда собранная информация предоставляется по

¹⁶ Westin, Alan R, *Databanks in a Free Society*, p. 472.

¹⁷ Ibid., p. 134.

первому запросу любому, кроме самих потребителей.

Но самое большое беспокойство как Уэстина, так и законодателей вызывала грядущая волна компьютеризации, которая могла привести лишь к ухудшению ситуации. В отличие от бумажных папок, содержимое которых должно было периодически урезаться, дабы не утонуть в информации, компьютерам ничего не нужно «забывать». «Перенос содержимого папок в компьютеры неизбежно приведет к возникновению угрозы гражданским свободам, приватности, самой сущности человека, потому что доступ к этой информации чрезвычайно упростится», – говорил Уэстин. С помощью компьютеров можно создать нестираемую историю человека, со всеми совершенными им ошибками, лишив его, таким образом, права на еще один шанс.

Догадке Уэстина есть практическое подтверждение. В своей книге «Обнаженное общество» Вэнс Паккард рассказывает историю одного 18-летнего юноши, который не мог устроиться на работу ни в один магазин в штате Мичиган, несмотря на положительные рекомендательные письма от учителей, пастыря и даже шефа полиции его городка. А причина крылась в том, что в 13-летнем возрасте он был пойман на мелкой краже в магазине. В результате его имя попало в компьютерную систему, к информации которой имели доступ практически все магазины в регионе. Благодаря способности компьютеров хранить информацию долгие годы и быстро предоставлять ее по первому требованию, человек навечно оказался в черных списках мичиганских торговцев.

Уэстин и другие свидетели привели в качестве примера множество историй, когда людям было отказано в выдаче кредита, страховании или приеме на работу из-за компьютерной ошибки – неправильно введенной в базу данных информации. Нередки случаи, когда перепутывались записи о двух людях с созвучными именами. Иногда возникала ситуация, когда администрация магазина выставяла покупателю счет за кредит, а покупатель отказывался его оплачивать, так как не производил соответствующих покупок. В этих случаях правда всегда была на стороне продавца, так как именно он контролировал файлы с информацией о кредитах.

В качестве контраргумента кредитные бюро заявили, что их деятельность является жизненно важной для роста национальной экономики, базирующейся на кредитах. Без достоверной информации о кредитной истории невозможно оценить риск выдачи кредита конкретному заемщику, невозможно осуществлять ипотечное кредитование, супермаркеты не будут иметь возможности продавать что-либо в кредит. Это не только может погубить кредитную отрасль экономики, но и просто больно ударить по честным заемщикам, которые не смогут получить кредит из-за отсутствия информации.

Конгрессу необходимо было найти выход из этого тупика противоречий. С одной стороны, Уэстин, Паккард и другие их сторонники утверждали, что перенос информации из бумажных папок в компьютеры создает возможности для новых видов злоупотреблений. В связи с этим компьютеризацию отрасли необходимо было ограничить. Но эксперты по информационным технологиям утверждали обратное. Компьютер сам по себе дает «больше возможностей для контроля над потенциально опасными действиями», – заявил доктор Гарри Джордан [Dr. Harry C. Jordan], основатель калифорнийской фирмы Credit Data Corporation. (В 1968 году Credit Data Corporation была приобретена компанией TRW Inc. и стала называться TRW-Credit Data, а в 1996 году снова была выделена из TRW и новая компания получила имя Experian.) На слушаниях подкомитета конгресса по защите неприкосновенности частной жизни в 1968 году Джордан заявил, что компьютеры можно даже запрограммировать таким образом, чтобы они принудительно выполняли процедуры, обеспечивающие приватность, например автоматическое стирание устаревших данных.¹⁸

В результате этих слушаний в апреле 1971 года конгресс принял окончательный

¹⁸ Ibid., p. 135.

вариант «Закона о точной отчетности по кредитам».¹⁹ Вместо того чтобы искусственно тормозить компьютеризацию кредитной отрасли, закон предоставил новые права потребителям на хранящуюся о них в кредитных базах данных информацию, включая право ознакомления со своими досье, право корректировки ошибочной информации, а также право внесения в базу данных своих версий событий, если кредитор утверждал, что невыгодная для потребителя информация верна.

Однако представители кредитной отрасли воспротивились такому подходу, ибо он грозил им лавинообразным ростом запросов потребителей на ознакомление со своими досье. Но этого не произошло. Произведенное Уэстином в 1972 году исследование показало, что после принятия закона число желающих ознакомиться со своими досье возросло незначительно – с 0,5 до 0,7 %.²⁰ Вместо лавины запросов закон просто дал возможность потребителям бороться с самыми вопиющими нарушениями их прав в кредитной отрасли, а у федеральных органов и отдельных штатов появилась возможность предъявлять кредитным компаниям иски в защиту потребителей.



Алан Уэстин

В марте 1968 года профессор Колумбийского университета Алан Уэстин выступил с показаниями перед специальным подкомитетом конгресса по защите неприкосновенности частной жизни относительно угрозы этой гражданской свободе, исходящей от кредитных бюро. Выступление Уэстина имело ключевое влияние на принятие конгрессом «Закона о точной отчетности по кредитам». Оно

¹⁹ Превосходное описание истории создания и принятия «Закона о точной отчетности по кредитам» можно найти в книге: Miller, *The Assault On Privacy*.

²⁰ Westin, *Databanks in a Free Society*, p. 137–138.

также убедило советника президента Эллиота Ричардсона [Elliot Richardson] в необходимости создания Консультативного комитета по автоматизированным системам обработки персональной информации [Advisory Committee on Automated Personal Data Systems]. В 1972 году возглавляемая Ричардсоном комиссия выпустила очень важный документ, содержащий «Кодекс справедливого использования информации». В отчете комиссии Ричардсона отмечалось также, что «федеральное правительство сыграло решающую роль в расширении использования SSN». [Иллюстрация приводится с разрешения правообладателя. © 1968 by The New York Times Co]

Периодом консолидации в кредитной отрасли стали 1970-е и 1980-е годы. Именно в эти годы отрасль сформировалась в сегодняшнем виде, когда эту нишу заняли три основные компании: Equifax (бывшая Retail Credit), Experian (бывшая Credit Data Corporation) и Trans Union. Каждая из этих компаний обладает примерно одинаковым набором информации: списком кредитных карт, банковских кредитов, студенческих кредитов и других займов за последние семь лет для каждого жителя США, включая детей. (Отрицательные оценки платежеспособности хранятся в течение семи лет, сведения о банкротстве – в течение десяти лет, «положительные» кредитные истории должны храниться пожизненно, но на практике эта информация также уничтожается по прошествии семи лет.) По каждому конкретному займу сохраняется информация об очередных выплатах, сделанных вовремя, а также о количестве задержек выплат на 30, 60 или 90 дней.

Кроме простых отчетов, Equifax, Experian и Trans Union предоставляют на базе этой информации множество других услуг. За дополнительную плату может быть рассчитан «рейтинг» заемщика, который оценивает его по 10-балльной шкале на основе анализа его кредитной истории. На основе накопленных данных могут быть также получены демографические сведения, статистические данные по населению и потребительские привычки. Несмотря на то что многие потребители желают получить информацию о своем кредитном рейтинге, она никогда не предоставляется. На первый взгляд кажется, что такая практика нарушает «Закон о точной отчетности по кредитам», но на самом деле это не так, ибо рейтинг – величина расчетная и не является частью хранимой о потребителе информации.

Несмотря на реформу 1971 года, многие потребители продолжали жаловаться, что значительный объем информации, хранимой в кредитных базах данных, либо содержит ошибки, либо полностью не соответствует действительности, в результате чего они не могут получить кредит без серьезных на то причин.

Занимающиеся оценкой кредитоспособности фирмы также пытались отстоять свое право на предоставление некоторых видов информации о потребителях (таких как имя, адрес, номер телефона и номер социального страхования) кому угодно и с какой угодно целью. Аргументировалось это тем, что данная информация не является информацией о платежеспособности и не находится под защитой «Закона о точной отчетности по кредитам», который запрещает ее предоставление в целях отличных от кредитования и страхования, таких как направленная реклама и услуги по розыску людей. В частности, Trans Union требовала у Федеральной комиссии по торговле [Federal Trade Commission, FTC] предоставить ей право на использование этой информации для целевого маркетинга.

Конечно, никто никого не обязывает брать кредит. Но в обществе, в котором потребность в кредитах на покупку дома, автомобиля, на обучение востребована практически всеми, кроме, может быть, высокообеспеченных семей, отказ в выдаче кому-либо кредита автоматически означает лишение его права стать полноценным членом общества. Главная беда кредитных бюро состоит в том, что огромному количеству людей, которым отказано в выдаче кредита, просто не повезло: они носили совпадающее с чьим-то имя, стали жертвой бюрократической ошибки либо их личностью и кредитной историей воспользовался мошенник.

Это может случиться с каждым

Многие американцы стараются соблюдать все правила, но их репутация может быть по неосторожности испорчена плохо спроектированными компьютерными системами, которые не всегда могут адекватно справиться с противоречивыми реалиями современной жизни. Достаточно вспомнить случай со Стивом и Нэнси Росс [Steve and Nancy Ross], которые много путешествовали в начале 1980-х и поплатились за это подпорченной кредитной репутацией «благодаря» Налоговому управлению.²¹

В 1983 году Нэнси Росс выиграла стипендию Японо-американского института проблем управления [Japanese American Institute for Management Sciences] и приглашение провести шесть месяцев на Гавайях. Ее муж Стив в это время был свободным журналистом и консультантом по компьютерам, поэтому семья могла спокойно отправиться навстречу приключениям вместе с детьми. По окончании путешествия они вернулись в свой дом в Лионии, штат Нью-Джерси.

Спустя несколько месяцев Нэнси получила приглашение провести год в странах Дальнего Востока и Японии. Такой шанс упускать было нельзя, поэтому Нэнси снова собрала чемоданы и уехала. Стив к тому времени получил работу на факультете журналистики Колумбийского университета, поэтому вынужден был остаться. С целью экономии Россы решили сдать свой дом в аренду, а Стив переехал в небольшую квартиру в Нью-Йорке.

Вскоре после возвращения в родной дом Стив и Нэнси получили очень неприятное письмо из Налогового управления: на их дом был наложен арест. «Я немедленно связалась по телефону с офисом Налогового управления в Холтсвиле (штат Нью-Йорк) и поинтересовалась, что собственно происходит, – вспоминает Нэнси Росс. – К счастью, мне попался отзывчивый служащий, и в течение получасовой телефонной беседы мы выяснили суть проблемы. Служащий догадался, что произошло, связался с офисом в Калифорнии, и уже через шесть часов мне позвонили из Налогового управления с заверениями, что все в порядке, к нам нет никаких претензий и нам будет выслано соответствующее письмо». Арест был немедленно снят.

Произошедшее стало результатом рокового стечения обстоятельств и ошибок, которые нередко возникают при использовании компьютеров. Поскольку и Стив и Нэнси сами обеспечивали себя работой, т. е. не работали по найму, они должны были ежеквартально уплачивать необходимые налоги самостоятельно. Находясь на Гавайях летом 1983 года, они выслали чек на 3500 долларов в региональный процессинговый центр Налогового управления в Лонг-Айленде, но почта ошибочно переправила его в процессинговый центр в Калифорнии.

Как раз летом 1983 года Налоговое управление внедряло новую компьютерную систему, и в течение года квартальные налоговые платежи не всегда попадали по назначению.

Процессинговый центр в Калифорнии вместо того, чтобы отправить информацию об уплаченном налоге по месту налогового учета, просто открыл новую учетную запись для семьи Россов.

Когда процессинговый центр в Лонг-Айленде получил налоговый отчет Россов за 1983 год, компьютер сразу же заметил, что сумма в отчете расходится с информацией о реально поступивших выплатах (по крайней мере, в нью-йоркских компьютерах) на 3500 долларов. На этом основании компьютер отправил в адрес Стива Росса письмо с требованием доплатить недостающую сумму.

Но как раз в это время Нэнси была в Японии, а Стив снимал квартиру в Нью-Йорке.

²¹ Интервью автору, 14 января 1995.

Несмотря на то что семья распорядилась пересылать поступающую на их имя корреспонденцию на новый адрес, письмо не было переслано, так как на конверте была пометка «не пересылать». В результате Стив просто не мог знать о его существовании. Тогда налоговое управление послало еще одно письмо с предупреждением о наложении ареста на недвижимость по почтовому адресу дома Россов без указания конкретного адресата. Но арендаторы проигнорировали письмо налогового ведомства, так как сами имели с ним некоторые проблемы.

Далее, Налоговое управление попыталось отыскать банковский счет Россов в Нью-Джерси, но он был закрыт, так как использовались новые счета – на Гавайях и в Нью-Йорке. Поскольку отыскать новые счета не удалось, налоговики просто наложили арест на принадлежащий Россам дом в Нью-Джерси.

Я очень подробно излагаю все детали, потому что большинство аналогичных случаев с кредитами настолько же сложны. И это всегда очень длинная история. Вот только история эта не попала в компьютеры Trans Union и Equifax. Эти компании располагали лишь информацией о том, что на дом семьи Россов стоимостью 10 тыс. долларов был наложен арест. Поэтому, когда в мае 1985 года пришло время продления семейной кредитной карты Mid Atlantic MasterCard, вместо автоматического продления, банк просто аннулировал ее.

«Сначала я позвонил в TRW, – рассказывает Стив Росс. – Там ответили, что нет никаких проблем и нам всего лишь нужно послать в их адрес письмо с объяснением ситуации, и они поместят эту информацию в наше досье. Когда я поинтересовался, будет ли недостоверная информация удалена из наших записей, то получил ответ „нет“. Они не делают этого! Если в вашей кредитной истории появляется дискредитирующая вас информация, они никогда не удаляют ее, а лишь помещают рядом ваши объяснения».

«Мы выслали две копии письма. Если верить представителям компании, информация была помещена в наши записи, кратко сформулированная в виде одного абзаца. Нас также заверили, что получено подтверждающее письмо о нашей „чистоте“ из налогового органа. Проблема заключалась в том, что обе компании [TRW и Equifax] уже продали информацию о надежности заемщиков около 187 независимым кредитным бюро, и у меня не было никакой возможности смыть с себя это пятно», – продолжает Стив.

Подобно тому, как компьютерный вирус повторно заражает только что вылеченную систему, независимые кредитные бюро снова «заразили» компьютеры TRW недостоверной информацией о наложении Налоговым управлением ареста на дом Россов в Лионии. Требование «Закона о точной отчетности по кредитам», касающееся права на корректировку информации о себе, не сработало, несмотря на все старания. «Буквально не было никакой возможности удалить эту информацию из системы», – вспоминают Россы.

В конечном счете им удалось убедить Mid Atlantic перевыпустить их семейную кредитную карту. И это было огромное достижение, ведь в течение следующих семи лет семья не смогла бы получить кредитную карту ни в одном другом финансовом учреждении, им отказывали в выдаче банковских кредитов, они даже не имели возможности перефинансировать собственное жилье. Они были «приземлены» в прямом смысле этого слова: с записью в кредитной истории о наложении ареста на недвижимость они не могли переехать и переоформить ипотечный кредит на новый дом.

Если бы не удалось восстановить карточку Mid Atlantic, ситуация могла бы развиваться куда более плохо: «Моя работа связана с поездками. Но как можно взять на прокат автомобиль без кредитной карты? Как можно оплатить без нее номер в гостинице? Кредитка – неотъемлемая часть повседневной жизни. Ее отсутствие могло лишить меня возможности зарабатывать на жизнь», – говорит Стив Росс.

«В конце 80-х суммарный годовой доход нашей семьи выражался 6-значным числом. Но вплоть до 1992 года в наш адрес поступали лишь малоинтересные предложения по кредитным картам. И лишь через семь лет, благодаря „Закона о точной отчетности по кредитам“, информация о наложении ареста на наш дом была удалена из нашего кредитного досье».

Однако точка в кредитной истории Россов на этом не была поставлена. Когда Стив впервые получил копию отчета о кредитоспособности своей семьи, он заметил в нем еще одну странную вещь – запись о заказе по каталогу Spiegel из Чикаго. «Spiegel утверждал, что мы заказали у него вещи и не заплатили за них. Удивительно, ведь мы никогда не имели с ними дела, и они никогда не выставляли нам счет. Видимо, счет должен был быть выставлен кому-то в Техасе [куда был выслан товар]. TRW не расследовала этот случай, [но, по крайней мере,] пыталась это сделать. К тому времени когда мы узнали об инциденте, Spiegel уже удалил соответствующие записи из своих компьютеров, и не было возможности проверить информацию, разве что вручную. Таким образом, она осталась только в семейном отчете о платежеспособности».

Опыт семьи Росс не является уникальным. В 1991 году Джеймс Уильямс [James Williams], сотрудник расположенной в Нью-Йорке фирмы Consolidated Information Service, занимающейся оценкой рисков ипотечного кредитования, проанализировав 1500 отчетов, полученных от TRW, Equifax и Trans Union, обнаружил, что 43 % из них содержат ошибки. В этом же году 1400 домовладельцев городка Норвич из штата Вермонт (3000 жителей) были отмечены в компьютерной системе TRW как нарушители налогового законодательства, «вследствие того что служащий TRW, собирающий ипотечную информацию, по ошибке принял налоговые счета за налоговые *штрафы*». ²² Несмотря на то что инцидент стал достоянием общественности, многим с трудом удалось добиться от TRW корректировки своих досье. Аналогичный случай имел место в Кембридже, штат Массачусетс, когда служащий Equifax также перепутал налоговые счета со штрафами.

Защитники приватности утверждают, что более половины досье содержат большое количество ошибок. Некоторые из этих ошибок, такие как неправильный адрес, несущественны. В других случаях в досье смешивается кредитная информация о двух совершенно разных людях с похожими именами, либо досье просто содержат некорректную информацию.

Особенно прискорбно, что агентства часто не вносят исправления в досье, даже когда им явно указывается на ошибки. Например, в 1989 году Бони Гитон [Bonnie Guiton], впоследствии советник Белого дома по делам потребителей, запросила копию своего кредитного отчета и обнаружила в ней информацию о совершенно неизвестном ей счете: очевидно, кто-то просто оформил кредитную карту на ее имя. Гитон обратилась в кредитное бюро с требованием удалить ошибочную информацию. «В полученном ответе утверждалось, что ошибка исправлена и эта информация удалена из моих записей», – рассказывала Гитон на слушаниях в конгрессе в сентябре 1989 года. ²³ Однако, когда через несколько месяцев она повторно запросила отчет, информация о мошенническом счете по-прежнему в нем присутствовала.

Ошибки в кредитных досье – распространенное явление. Гитон отметила также, что многие ее сотрудники запрашивали свои отчеты и находили в них множество ошибок. Лично я не знаю ни одного человека, который не находил бы ошибок в своих кредитных отчетах. Причем это были не безобидные опечатки, а информация, отрицательно влияющая на кредитный рейтинг человека.

В Ассоциации кредитных бюро, АСВ, оспаривается около 50 % случаев. По данным АСВ, среди продаваемых ею кредитных отчетов более 550 миллионов содержат небольшие ошибки. Согласно данным исследования, проведенного в 1991 году по заказу АСВ консалтинговой фирмой Arthur Andersen, ошибки, которые реально могут повлиять на решение о предоставлении кредита, встречаются менее чем в 1 % кредитных отчетов. Но это

²² Smith, *War Stories*, 1994.

²³ Hearing Before the House Subcommittee on Consumer Affairs on the Fair Credit Reporting Act on September 13, 1989 (p. 30), как изложено в книге: Smith, *War Stories*.

означает, что более двух миллионов людей получают незаслуженный отказ в предоставлении кредита.

Скорее всего, обе оценки справедливы. Многие люди находят в своих кредитных отчетах неточности, но обычно они незначительны. Конечно, эмитенты кредитных карт в курсе ситуации с ошибками, и небольшое пятнышко на кредитной репутации клиента не станет поводом для отказа в выдаче ему карты. Но такое положение дел нельзя считать справедливым, ибо оно в равной мере приводит к ситуации, когда кредит выдается человеку ненадежному, и к ситуации, когда честному гражданину в кредите отказывают.

Кража личности: Украденное «Я»

Истории, подобные произошедшей с семьей Росс, составляли основную массу проблем кредитных бюро в 1980-х и 1990-х годах. Но в последние годы наблюдается неожиданный и поистине драматический рост нового вида преступлений, ставших возможными вследствие доступности как кредитной, так и личной информации. Злоумышленник узнает номер социального страхования какого-нибудь человека, заводит себе дюжину кредитных карточек на его имя, в результате платить по счетам приходится этому человеку. (Многие банки облегчают задачу злоумышленника, печатая номера социального страхования клиентов на банковских выписках.) В одних случаях мошенники пользуются кредитками непосредственно, покупая для себя товары, отправляясь в дорогостоящие путешествия, обедая в дорогих ресторанах. Другие используют более изощренные схемы мошенничества, превращая приобретенные обманом вещи в наличные деньги. Это преступление стало настолько распространенным, что приобрело даже собственное название – *кража личности* [identity theft].

Иногда злоумышленники получали информацию из внутренних источников: в апреле 1996 года группе служащих Управления социального страхования было предъявлено обвинение в продаже личной информации 11 000 граждан криминальным кругам, которые использовали ее для активации краденых кредитных карт и оплаты с их помощью счетов на огромные суммы.²⁴ Нередки случаи, когда преступники под видом бомжей перерывали городские помойки в поисках выписок по банковским счетам и кредитам.

Случай, произошедший с вашингтонским журналистом Стивеном Шоу [Stephen Shaw], является типичным.²⁵ В один прекрасный летний день 1991 года продавец автомобилей из Орlando, штат Флорида, с похожим именем Стевен Шоу [Steven Shaw], получил доступ к кредитному отчету Стивена Шоу. Сделать это было проще простого. В течение многих лет Equifax вела агрессивную рекламную компанию своих услуг по предоставлению кредитных отчетов фирмам, торгующим автомобилями. Услуга предоставляла продавцу возможность, узнав имя потенциального покупателя, ненадолго отлучиться и быстро произвести проверку его кредитной благонадежности. Вероятнее всего, мистер Шоу из Флориды использовал эту возможность, чтобы «вычислить» кого-нибудь с созвучным именем и незапятнанной кредитной историей, считает Стивен Шоу.

Как только Стевен Шоу из Флориды узнал номер социального страхования и другую личную информацию Стивена Шоу из Вашингтона, он получил возможность «украсть личность» последнего. Помимо сведений о безупречной кредитной репутации Стивена Шоу, его кредитный отчет содержал настоящий и предыдущие адреса места жительства, девичью фамилию матери и номера всех его кредитных карт. Джекпот!

²⁴ Jim Mallory, «Social Security Workers Charged with Data Theft», Newsbytes News Network (<http://www.newsbytes.com>), 4 августа 1996.

²⁵ Интервью автору, апрель 1995. См. также «Separating the Equifax from Fiction», *Wired Magazine*, сентябрь 1995, p. 96.

«Он воспользовался моими данными для открытия 35 счетов и нанес мне ущерб в размере 100 000 долларов, – рассказывает Стивен Шоу. – Он „засветил“ меня повсюду брал кредиты на покупку автомобиля, персональные кредиты, открывал банковские счета, покупал дорогую стереоаппаратуру, мебель, домашнюю технику, вещи, авиабилеты».

Поскольку все счета были открыты на имя Стивена Шоу и с использованием его номера социального страхования, ему автоматически предъявлялись к оплате все траты, которые на самом деле производил другой Шоу – из Флориды. Коль скоро счета не оплачивались, пострадавшие фирмы сообщили Equifax и другим кредитным бюро, что Стивен Шоу, имевший ранее безупречную кредитную репутацию, стал теперь неблагонадежным.

Не все истории с кражей личности начинались с кражи кредитных отчетов или банковских выписок. Некоторые начинались с подделки заявлений на смену адреса, в результате адресованная человеку почта отправлялась в заброшенный дом. При этом не оставалось никакого документального следа! В мае 1997 года газета *Seattle Times* рассказывала на своих страницах о том, что тысячи жителей Сиэтла и окрестностей получали очень странные и подозрительные звонки. Звонивший представлялся сотрудником радиостанции, которая производит возврат денег, и сообщал, что чек будет выслан по почте, если ответивший сообщит свой номер социального страхования.

Многие сочли это все подозрительным и сообщили на радиостанцию и в полицию, но некоторые легкомысленно сообщили звонившему интересующую его информацию. Эпидемия аналогичного жульничества охватила одного из крупнейших провайдеров – America Online, где этот способ мошенничества даже получил свое название – «phishing».^[p6]

По словам Шоу, ему понадобилось около четырех лет для решения проблемы – типичный срок, о котором говорят и другие жертвы «кражи личности». Четыре года звонков из коллекторов счетов с напоминанием о необходимости оплаты, нарастающим количеством гневных писем в почтовом ящике и изматывающей неизвестностью, что еще злоумышленник сделает с вашим именем. Четыре года все кредиторы считают вас неблагонадежным. В этот период жертва практически лишена возможности получить новую кредитную карту или ипотечный кредит. Но одно из самых жестоких последствий кражи личности заключается в том, что многие его жертвы не могут найти работу: многие работодатели кроме рекомендательных писем изучают и кредитную историю претендентов на рабочее место.

Кража личности стала возможной из-за политики компаний, эмитирующих кредитные карты. Эти компании постоянно озабочены привлечением новых клиентов и не оказывают должного внимания идентификации личности заявителя при оформлении карты посредством почты или телефонного звонка. Опасность политики этих компаний заключается в том, что если вы знаете чье-либо имя, его адрес, номер телефона, номер социального страхования и девичью фамилию матери, то этого достаточно для идентификации вас как этой личности. А после того как счета за сделанные покупки не оплачиваются, крайним оказывается этот человек.

Несомненно, узнать чье-то имя, адрес, номер телефона, номер социального страхования и девичью фамилию матери относительно несложно. Кредитные бюро предоставляют эту информацию своим клиентам, поисковые службы за умеренную плату делают эту информацию доступной через Интернет, да и сами люди зачастую неосмотрительно предоставляют эту информацию по телефону человеку, который рекомендуется сотрудником банка или компании, выпускающей кредитные карты.

Кража личности не является принципиально новым преступлением. Существует множество историй – от сказок и вестернов, когда мужчина получал еду, ночлег и даже

р6

Вылавливание паролей доступа у неосторожных пользователей. Phishing – неологизм, созвучный «fishing» – рыбалка.

любовь незнакомки, представившись кем-то другим. Отличие нашего времени в том, что стремление корпораций расширить кредитный рынок делает каждого из нас беззащитным перед угрозой кражи личности и порчи репутации без нашего ведома. Поскольку кредиты предлагаются по почте или по телефону – зачастую это делает компьютерная программа или низкооплачиваемый сотрудник службы по работе с клиентами, действующий строго по предписанному сценарию, – настоящему герою сложно будет убедить даму, что его просто подменил какой-то самозванец.

Вряд ли кто-то до конца представляет себе масштабы кражи личности сегодня – оценки колеблются от 100 до 400 случаев в год, – ясно одно: их количество увеличивается. В идеале преступник должен быть подвергнут тюремному заключению, штрафу или другому наказанию. Но правоохранительные органы перегружены, а суды отказывают пострадавшим в возбуждении уголовных дел против мошенников. Это происходит потому, что закон считает в этой ситуации пострадавшими компании, выдавшие кредит, а не людей, чья личность была украдена. При этом многие банки не дают делу ход, им проще списать убытки и работать дальше.

Существует целый ряд технических мер, которые могли бы снизить количество такого рода преступлений. Одной из таких мер могло бы стать требование личной явки для оформления кредитной карты и помещение на нее фотографии владельца. Это создало бы серьезный барьер мошенничеству, так как мошенники, естественно, не хотят, чтобы их идентифицировали. Однако компании вряд ли согласятся с этим, поскольку это резко снизит эффективность бизнеса: вместо упрощенной идентификации и отсылки карточки по почте придется открывать новые офисы.

Наконец, расцвет воровства личности стал возможен потому, что от кредитующих компаний не требуется вкладывать средства в обеспечение адекватного уровня безопасности процедуры выдачи кредита, который в настоящее время явно недостаточен. Рвение, с которым компании рассылают предварительно заполненные заявления на получение кредитных карт, создает благодатную почву для мошенничества. Когда это происходит, кредиторы просто вносят информацию в кредитное досье клиента и продолжают работать дальше, а клиент остается у разбитого корыта, иначе говоря, несет в результате кражи личности материальные потери. Самым простым средством снижения количества мошенничеств может стать требование к компании, создавшей риск, принимать участие в ликвидации его последствий. Это можно сделать путем наложения наказаний на компании, вносящие незаслуженно компрометирующую информацию в кредитные досье, так же как отдельных граждан наказывают за ложное сообщение в полицию. Угроза подвергнуться наказанию заставит предоставляющие кредиты организации внимательнее относиться к идентификации личности заемщика и снизит тем самым количество краж личности.

Двигаясь в будущее, надо помнить уроки прошлого

Последние тридцать лет преподали нам немало уроков, начиная с отказа от создания Национального информационного центра и создания в образовавшемся вакууме частным бизнесом системы национального масштаба, включающей банки данных, терминалы доступа и компьютерные сети.

Возможно, самым главным уроком стало осознание того, что принятые в начале пути решения могут привести к далеко идущим последствиям. Разработанная в 1932 году система номеров социального страхования стала играть все более важную роль в жизни общества в последующие 60 лет. Независимо оттого как вы относитесь к нему, SSN – вредное изобретение. Но страна уже не может отказаться от его использования.²⁶

Год – Пользователи системы номеров социального страхования

²⁶ Источник данных – Управление социального страхования.

- 1943 Федеральные агентства используют SSN только для своих служащих
- 1961 Комиссия по гражданской службе использует SSIM для идентификации служащих
- 1962 Налоговое управление использует SSN для идентификации налогоплательщиков
- 1967 Министерство обороны использует SSN для идентификации военнослужащих
- 1972 США начали присваивать SSN всем легально въезжающим в страну иностранцам и любому получающему государственные субсидии
- 1975 Программа помощи семьям с детьми [Aid for Families with Dependent Children] начинает использовать SSN для их идентификации
- 1976 Отдельные штаты используют SSN для налоговых и благотворительных платежей, а также на водительских удостоверениях
- 1977 Программа продовольственных талонов [Food Stamp Program] использует SSN для определения членов семьи
- 1981 Программа школьных завтраков [School Lunch Program] использует SSN для определения взрослых членов семьи
- 1981 Служба призыва в армию [Selective Service System] использует SSN для учета призывников
- 1982 Федеральная программа кредитования [Federal loan program] использует SSN для учета заемщиков
- 1983 Указание SSN стало обязательным при открытии вкладных счетов (с доходом в виде процента)
- 1984 Отдельным штатам разрешено использовать SSN в Программе помощи семьям с детьми, программе Medicaid, [p7] при выплатах пособий по безработице, в программах продовольственных талонов и других государственных программах, осуществляемых по плану, утвержденному разделами I, X, XIV или XVI «Закона о социальном страховании»
- 1986 SSN может быть использован для подтверждения возможности трудоустройства
- 1986 Наличие SSN стало обязательным для идентификации налогоплательщиков с иждивенцами в возрасте от пяти лет и старше
- 1986 Министр транспорта постановил использовать SSN при выдаче лицензий на коммерческие автоперевозки
- 1988 Указание SSN стало обязательным для идентификации налогоплательщиков с иждивенцами в возрасте от двух лет и старше (требование вступило в силу в 1990 году)
- 1988 Штаты стали использовать SSN родителей при выдаче свидетельства о рождении
- 1988 Штаты и станции переливания крови стали использовать SSN для идентификации доноров
- 1988 Указание SSN стало обязательным для всех получающих пособия в соответствии с разделом II «Закона о социальном страховании»
- 1989 В Национальную систему учета кредитования студентов [National Student Loan Data System] также стали вноситься их SSN
- 1990 Указание SSN стало обязательным для идентификации налогоплательщиков с иждивенцами в возрасте от года и старше (требование вступило в силу в 1991 году)
- 1990 Указание SSN стало обязательным при осуществлении любых выплат Министерства по делам ветеранов
- 1990 Указание SSN стало обязательным для служащих продуктовых и розничных магазинов, производивших отпуск товаров по продовольственным талонам
- 1994 SSN стал использоваться при выборе присяжных
- 1994 Министерство труда утвердило SSN в качестве идентификационного номера заявок на получение выплат

p7

«Медикэйд» – программа медицинской помощи неимущим, осуществляемая на уровне штатов при финансовой поддержке федеральных властей.

1994 Указание SSN стало обязательным для идентификации налогоплательщиков с иждивенцами независимо от возраста (требование вступило в силу в 1996 году)

1996 SSN стал обязательным к указанию при соискании любых профессиональных лицензий, подаче заявления о вступлении в брак. SSN должен указываться в заявлении о разводе, выплате алиментов, определении и подтверждении опекунских прав, необходим он и при оформлении свидетельства о смерти

1996 Генеральный прокурор утвердил требование всем негражданам страны сообщать свой SSN для включения его в записи службы иммиграции и натурализации [Immigration and Naturalization Service]

1996 SSN должен наноситься на водительские удостоверения

1997

Другой важный урок заключается в том, что крупные организации, совершающие технические ошибки, редко платят за них – эти потери ложатся на клиентов. Сегодня очень легко получить выгодный кредит, всего лишь сообщив свой SSN, чем зачастую и пользуются мошенники. Но когда афера вскрывается, все проблемы приходится разрешать настоящему владельцу SSN, которому и предъявляются претензии по невыплаченному кредиту. Банки же ничем не озабочены, они просто поднимают процентные ставки, распределяя свои потери между клиентами.

Еще один урок – не упускать важных деталей. Обрывочные сведения, которые мы получаем из газет и телевидения, не отражают истинной картины. Однако все чаще именно средства массовой информации становятся трибуной для обсуждения сложных вопросов взаимодействия общества и технологий.

В Соединенных Штатах широко распространено мнение, что свободный рынок всегда прав, а попытки правительства что-то регулировать лишь создают проблемы. Эта «вера» особенно распространена среди «цифровой элиты», которая рассматривает все действия правительства как «плохие», а все действия частного бизнеса – как «хорошие». Несмотря на это, в области компьютерной приватности, чаще всего верно обратное. В 1960-е годы предоставленный самому себе частный бизнес создал систему, ущемляющую права простых граждан. Да, это был свободный информационный рынок, но на этом рынке могли играть только бизнесмены. И лишь после вмешательства правительства в форме принятия «Закона о точной отчетности по кредитам» люди получили право знакомиться со своими кредитными досье и требовать удаления из них недостоверной информации. Конечно, установленный этим законом порядок государственного регулирования вопросов приватности не решает всех проблем, но это лучше, чем ничего.

Мы постоянно наблюдаем, как бизнес сопротивляется любым попыткам регулирования в области приватности, так же как химическая промышленность в свое время боролась с попытками установить регулирование в сфере охраны окружающей среды. Причем и в том и в другом случае предсказываемые катастрофические последствия не сбылись. Фактически так же как жесткое регулирование использования окружающей среды заставило химическую отрасль стать менее расточительной (и, как следствие, более прибыльной), так и принятие даже небольшого количества мер по регулированию вопросов приватности привело к тому, что повысилось качество информации, хранимой в корпоративных и государственных банках данных, что сделало эти системы более ценными, удобными и прибыльными. Очевидно, что защита приватности и личных свобод представляет долгосрочный интерес как для общества, так и для бизнеса. Но поскольку многие бизнесмены смотрят не далее, чем на год вперед, они просто не осознают эту простую мысль.

Наше будущее в базах данных

А что мы видим в другом направлении? Нас ждет будущее, в котором технологии будут играть решающую роль в устранении неоднозначности. Все, что может быть сделано,

будет сделано, причем с очень высокой точностью. Предоставленный сам себе, частный бизнес скорее всего повторит ошибки прошлого и вновь создаст системы, которые изначально будут несправедливыми, недемократичными и неконтролируемыми.

В 1965 году Правительство Соединенных Штатов стояло на компьютерном перепутье: решался вопрос о создании глобальной правительственной базы данных. Но когда детали этого проекта стали доступны общественности, он был немедленно закрыт. Конгресс инициировал серию слушаний, посвященных исходящей со стороны компьютеров угрозе приватности, правительственная комиссия сформулировала принципы защиты информации, и у исполнительной власти была возможность принять пакет новых законов.

Но мы упустили ее. Общенациональная база данных могла бы предотвратить злоупотребления в кредитной индустрии. Система с жестким контролем над ее использованием и средствами восстановления не допустила бы появления ошибок, наводнивших сегодня разрозненное множество банков данных. Более того, в информационной системе общего пользования было бы просто невозможно тайком от общественности использовать информацию в целях отличных от тех, для которых она была собрана.

Сегодня мы снова стоим на компьютерном перепутье. Мы вновь, как это уже было в 1960-е годы, рассматриваем компьютеры как средство хранения важной финансовой, образовательной и кредитной информации. Мы на пороге технократического будущего, в котором компьютеры будут фиксировать даже самые интимные аспекты нашей жизни. Всеми своими датчиками они будут воспринимать и записывать все происходящее на планете. Они позволят нам отличать одну личность от другой с очень высокой точностью. Еще раз повторяю, что правительству просто необходимо принять меры по регулированию использования новейших информационных технологий. В противном случае мы рискуем попасть в ту информационную пропасть, которой до сих пор удавалось избежать. К сожалению, об этом почти не упоминают в открытых дискуссиях по поводу мошенничеств с кредитными картами, неправомерного использования баз данных и краж личности.

Основная проблема баз данных заключается в том, что никто не может гарантировать корректность хранящейся в них информации. Мы должны сосредоточиться на этой проблеме и попытаться построить наше общество и наши компьютерные системы таким образом, чтобы они были устойчивы против таких ошибок. Но мы делаем все с точностью до наоборот. Банкиры и правоохранительные органы, иммиграционные службы и политики — все озабочены лишь поиском технологического решения, которое урегулирует проблему идентификации личности. В следующей главе мы увидим, почему этот подход нежизнеспособен.

3

Абсолютная идентификация

Ошибки в базах данных, кража личности, нелегальная иммиграция и нераскрытые преступления стали распространенными явлениями в нашей жизни, поэтому многие политики обращают свои надежды к достижениям в области технологий биометрической идентификации. Сторонники этих технологий утверждают, что их использование позволит создать режим абсолютной идентификации, при котором каждая личность может быть уникально идентифицирована по одним лишь уникальным признакам собственного тела.

Абсолютная идентификация как политическая цель — вещь вполне достижимая. Действительно, все большее число ученых, инженеров и политиков рассматривают идентификацию человека по антропометрическим признакам не как техническую, а как политическую проблему. Если этого потребуют интересы общества, мы можем уникальным образом зарегистрировать каждого жителя Соединенных Штатов, Европы, Азии и, возможно, всей планеты. После этого мы сможем очень легко идентифицировать личность в

банке, учебном заведении, на работе и на дороге. Абсолютная идентификация поможет избавиться от взаимного несоответствия компьютерных записей, кражи личности и неоднозначности, с которыми мы постоянно сталкиваемся в повседневной жизни. Когда на смену анонимности придет абсолютная идентификация, мы сможем построить общество, каждый член которого гарантированно сможет получить положенные ему привилегии и будет полностью ответствен за все свои действия.

Абсолютная идентификация – очень соблазнительная идея. Но, к сожалению, порочная. Чтобы понять, почему, нам необходимо разобраться в недостатках самой технологии.

Про идентификацию детей

Три тысячи лет назад в Иерусалиме перед царем Соломоном предстали две женщины. У обеих недавно родились дети, а затем, когда один ребенок умер, обе стали утверждать, что оставшийся ребенок принадлежит именно ей. Соломону необходимо было справедливо разрешить спор в пользу настоящей матери.

Сегодня дилемма Соломона решается тривиально. Если только женщины не являлись однойцовыми близнецами, у них были разные наборы генов. Настоящая мать легко определяется после анализа образцов крови ребенка и обеих женщин. Такие генетические экспертизы проводятся сегодня регулярно для установления отцовства при решении дел об алиментах.

Но в распоряжении Соломона не было достижений современной биологии. Вместо этого Соломон приказал принести свой меч. Соломон сказал, что, если женщины не смогут разрешить спор самостоятельно, ребенок будет разделен на две части. Соломон знал, что настоящая мать скорее согласится на несправедливость, чем допустит смерть своего ребенка. Поэтому, когда мгновение спустя одна из женщин торопливо отказалась от младенца, Соломон точно знал, что другая женщина лжет.

Двадцать пять столетий спустя исследователь Хоайо де Баррос [Joro de Barros] описывал несколько способов идентификации маленьких детей. В опубликованной в 1563 году книге «Сочинения об Азии» [*Decadas da Asia*] де Баррос описывал, как китайские торговцы «паспортизировали» детей, делая отпечатки их ладоней и ступней при помощи бумаги и чернил. Это были не просто какие-то бумаги, это была часть торговли.²⁷ После такой фиксации признаков детей уже было сложно перепутать, что было особенно важно во времена, когда люди являлись предметом купли-продажи.

Царь Соломон мог бы установить аналогичную систему регистрации всех новорожденных в Израиле. Древние израильтяне уже знали пергамент и чернила, поэтому у них было все необходимое для реализации этого проекта. Знали древние израильтяне и об уникальности отпечатков пальцев: археологи обнаружили недавно при раскопках в Израиле наборы глиняной посуды, на каждом предмете отчетливо видны отпечатки больших пальцев. Предположительно гончар использовал свой отпечаток пальца как персональное клеймо. Однако идея создания общенациональной системы идентификации не пришла в голову Соломону и его придворным, так как проблема идентификации взрослых не стояла до настоящего времени.

Много примеров ошибочной идентификации можно найти в литературе: «Принц и нищий» Марка Твена, истории о двойниках,^[p8] многие пьесы Шекспира. Эти истории дошли до наших дней и не потеряли точности описания, потому что такого рода ошибки были редкостью. Вплоть до промышленной революции в мире не было реальной нужды в формальной системе точной идентификации. В Европе фамилии не использовались вплоть

²⁷ Как изложено в книге: Cummings and Midlo, *Finger Prints, Palms and Soles*.

до Средневековья! Большинство людей рождались и всю жизнь проживали в одном месте, где все знали друг друга, а появление чужака не могло остаться незамеченным.

Антропометрические признаки

Ряд событий второй половины XIX века заставил правительства искать лучшие пути для идентификации проживающего на территории их стран населения. Одной из причин стало развитие крупных городов, где жители ежедневно имели дело с незнакомцами. Возможность идентифицировать друг друга была жизненно необходимой, ибо давала возможность избежать обмана. Другой причиной стала легкость перемещений, повлекшая за собой наплыв иммигрантов, ищущих лучшей жизни. Очень скоро ксенофобия законодателей привела к принятию в Европе и США жестких иммиграционных законов, призванных сократить приток иностранцев. А это, в свою очередь, потребовало создания системы точной идентификации, которая позволяла бы властям отличать граждан от неграждан. Третьей причиной стала новая концепция реабилитации преступников, предоставлявшая возможность людям, совершившим ранее преступления, реабилитироваться и встать на путь исправления. Система идентификации нужна была и для отделения рецидивистов от совершивших преступление впервые.

Проблема идентификации осужденных привлекла внимание парижского антрополога Альфонса Бертильона [Alphonse Bertillon] (1853–1914). Как можно идентифицировать карманника, попавшегося впервые, если при каждом аресте преступник называет разные имена? Каким образом можно добиться постоянной идентификации без сотрудничества с самим человеком?

Бертильон заметил, что, даже если человек назовется другим именем, сменит прическу, наберет вес, некоторые части его тела останутся неизменными. Он создал систему *антропологического опознавания*, базирующуюся на этих неизменных признаках. Система была очень прямолинейной, а именно:

- когда человека арестовывали за преступление, один из помощников Бертильона производил точные измерения головы, рук, ступней и ушей подозреваемого. Фиксировалось наличие шрамов, родимых пятен, другие отличительные телесные признаки. Эта информация вместе с именем подозреваемого заносилась в специальные карты, которые затем хранились в центральном полицейском участке;

- вместо того чтобы располагать карты по именам, Бертильон предложил систему индексации по признакам. Карточки людей с размерами головы выше среднего помещались в одну группу, со средним размером – в другую, а с маленьким размером – в третью. Каждая из этих групп разбивалась на три подгруппы в зависимости от длины среднего пальца арестованного. Дальнейшая дифференциация шла по всем шести предложенным Бертильоном признакам. В результате получилось $3 \times 3 \times 3 \times 3 \times 3 \times 3 = 729$ различных групп;

- когда полицейский составлял карту на очередного задержанного, он должен был просмотреть группу близких по признакам карт, и, если находилась карта, данные которой совпадали с данными задержанного, это означало, что человек уже подвергался аресту, и позволяло установить, не пытается ли задержанный назваться другим именем.

Система Бертильона стала вехой в развитии криминалистики. Человек мог быть арестован и описан в 1881 году одним полицейским и опознан три года спустя другим полицейским в результате обнаружения совпадения признаков после просмотра картотеки. Бертильон создал систему, позволяющую идентифицировать человека по записям, в то время как ранее это мог сделать только человек с хорошей зрительной памятью.

В течение шести лет Бертильон работал над улучшением своей системы и в 1879 году выпустил 95-страничную брошюру, представленную на Международном конгрессе по исполнению наказаний в Риме. В течение следующих десяти лет Бертильон наблюдал за процессом регистрации более чем 120 тысяч представителей преступного мира в Париже.

Сегодня многие из работ Бертильона кажутся примитивными и отдают расизмом.

(Бертильон особенно интересовался возможностью различать цыган, так как немногие французы могли это сделать.) Но система работала. В течение десяти лет после ее официального принятия в декабре 1882 года парижская полиция выявила 4564 человека, назвавших полиции вымышленное имя, и все это благодаря антропометрическим измерениям. Система Бертильона дала возможность французским судьям выносить более жесткие приговоры рецидивистам. Буквально через несколько лет уровень преступности в Париже снизился. Бертильон объяснял это тем, что карманники сочли за лучшее мигрировать в места, где шанс их идентификации был ниже.

К 1896 году система Бертильона была принята двадцатью тюрьмами и семью полицейскими управлениями Соединенных Штатов. Однако очень скоро сторонники системы обнаружили, что область применения антропометрических измерений не ограничивается только идентификацией преступников. В американском издании книги Бертильона майор Р. Мак-Клаффри [R. W. McClaughry], начальник Управления исполнения наказаний штата Иллинойс, подчеркнул основную цель любой системы точной идентификации: идентификация всего населения. Мак-Клаффри обрисовал ее как надежное средство общественного контроля:

В соответствии с теорией системы и на благо всего общества, каждый человек должен быть подвергнут частичному описанию в возрасте 10 лет (в части описания формы ушей) и полному описанию при достижении им зрелости. Каждая страна должна иметь свою структуру, которая будет хранить описания всех жителей. Антропометрические измерения должны заменить паспортный контроль при пересечении границы, эти данные должны фигурировать при страховании жизни, выдаче разрешений и других документов, требующих идентификации личности. Это позволит мгновенно отыскать человека при первой необходимости, как для его блага, так и в интересах общества, в любом месте, даже если он изменит свою внешность и возьмет другое имя. Преступность будет искоренена, выборы станут честными, иммиграционные законы будут выполняться неукоснительно, многочисленные недоразумения и судебные ошибки станут невозможны, а ведение бизнеса чрезвычайно упростится.²⁸

Век спустя американские законодатели все еще находятся в поисках системы идентификации, которая служила бы строгому исполнению иммиграционного законодательства, исключила бы обман потребителей и могла бы использоваться для идентификации после смерти. Конечно, мы не собираемся устраивать тотальный замер ушей и пальцев,²⁹ но основная идея Бертильона находит отражение в современных системах биометрической и ДНК-идентификации, расширяющих возможности полномочных органов

²⁸ Bertillion, *Signalitic Instructions*, введение.

²⁹ Главным вкладом Бертильона в криминалистику стала не столько сама его система идентификации, в конечном счете признанная «громоздкой и не всегда точной», сколько выведенное им правило, что любая система идентификации должна быть систематизированной и объективной, особенно если один человек пытается осуществить идентификацию по данным, собранным другим человеком. Профессор кафедры микроанатомии медицинской школы университета Тулэйн Каммингс [Cummings] и доцент той же кафедры Мидлоу [Midlo] писали в своей книге *Finger Prints, Palms and Soles*, p. 143: «[Бертильон] пересмотрел неточные описательные методы, применявшиеся ранее для идентификации преступников, и предложил использовать измерение одиннадцати параметров тела. В качестве систематического метода, адаптированного для правоохранительных органов, система Бертильона дает лучшие результаты, чем просто визуальное опознание. Измерения сами по себе подразумевают классификацию, которая, в свою очередь, является непременным атрибутом любой системы идентификации личности, по которой можно вести поиск. Система Бертильона, громоздкая и не всегда точная, была постепенно заменена на несравнимо более качественный метод идентификации по отпечаткам пальцев, который в настоящее время повсеместно используется для регистрации преступников и находит все более широкое применение в гражданских и военных целях».

по мгновенному нахождению человека в любой момент с любой целью, где бы он ни находился.

Наука об отпечатках пальцев

Два чернокожих брата, однояйцовые близнецы, были обвинены в совершении ужасного убийства в штате Миссури. На месте преступления было обнаружено орудие убийства – окровавленный нож. Однако во время судебного разбирательства адвокат показал жюри присяжных, что на орудии преступления остались характерные отпечатки пальцев, принадлежащие убийце, но они не совпадают с отпечатками пальцев обвиняемых, а принадлежат другому человеку, находящемуся в зале суда. Суд был ошеломлен: обвинение предъявлено не тому человеку!

Это сюжет из «Простофили Вильсона», произведения Марка Твена, впервые опубликованного в 1893 году в *Century Magazine*.

Речь Вильсона, обращенная к присяжным, стала для многих американцев первым введением в науку об отпечатках пальцев:

Каждый человек сохраняет неизменными на всю жизнь, от колыбели до могилы, некоторые физические приметы, благодаря которым он может быть в любую минуту опознан, причем без малейшего сомнения. Эти приметы являются, так сказать, его подписью, его физиологическим автографом, и этот автограф не может быть ни подделан, ни изменен, ни скрыт, ни лишен четкости под влиянием времени.³⁰

Наше понимание отпечатков пальцев мало изменилось к настоящему времени. Определяемые комбинацией генов и случайными процессами во время развития плода, отпечатки пальцев на протяжении всей жизни остаются такими же, как при рождении. Этот признак действительно уникален: число возможных вариантов настолько велико, что до сих пор не было случаев (и вряд ли когда-нибудь будут), чтобы у двух разных людей был одинаковый рисунок папиллярных линий.

Возможно, один из самых главных моментов заключается в том, что отпечатки пальцев неуничтожимы. Мне довелось убедиться в этом самостоятельно, когда я изучал курс химии в колледже Брин Мор. Я проводил серию опытов с безводной уксусной кислотой. Через несколько недель я заметил, что отпечатки моих пальцев стали почти гладкими, кислота практически вытравила их. Но уже буквально через месяц после окончания опытов отпечатки восстановились в том же виде, как будто и не исчезали.

Причина такой стойкости кроется в том, что рисунок папиллярных линий формируется глубинными слоями эпидермиса, и единственный способ изменить чьи-либо отпечатки заключается в полном удалении кожи с подушечек и заменой ее кожей с других участков тела. Эта болезненная и уродующая операция была использована в 1930-е годы несколькими гангстерами, но с тех пор не применялась.

Несмотря на то что люди давно знали об уникальности отпечатков пальцев, вплоть до конца XIX века ученые не проявляли внимания к возможности использования отпечатков пальцев для идентификации. В 1880 году Генри Фолдс [Henry Faulds] (1843–1930) опубликовал в научном журнале *Nature* статью. В статье он рассказывал, что, после того как он случайно оставил на чем-то отпечаток своих пальцев, ему в голову пришла мысль, что преступник тоже оставляет отпечатки на месте преступления. Это давало возможность, рассуждал Фолдс, после задержания подозреваемого сравнить его отпечатки пальцев с оставленными на месте преступления.

³⁰ Марк Твен, *Простофиля Вильсон*.

Русский перевод книги доступен на <http://lib.rus.ec/b/57097> (прим. составителя FB2)

Но важность отпечатков пальцев для раскрытия преступлений была не только в том, что они уникальны, но и в том, что они остаются на месте преступления. В отличие от системы Бертильона нет необходимости фиксировать отпечатки пальцев всего населения, достаточно лишь сравнить обнаруженные отпечатки с отпечатками подозреваемого.

Английский чиновник в Индии Уильям Хершель [W. J. Hershel] после прочтения публикации Фолдса в *Nature* написал в журнал, что пользуется подобной техникой уже около двадцати лет. Но если Фолдс видел применение отпечатков пальцев лишь для идентификации преступников, то Хершель предложил более широкое использование отпечатков пальцев в качестве системы многоцелевой идентификации для установления личности. (Конечно, и здесь не обошлось без расизма: Хершель должен был поддерживать порядок колонии, но он не мог различать людей без снятия отпечатков пальцев.) Пять лет спустя фотограф из Сан-Франциско по имени Табор [Tabor] заинтересовался случайно оставленным отпечатком собственного испачканного чернилами пальца. После серии экспериментов он предложил использовать отпечатки пальцев как средство регистрации китайских эмигрантов, выглядевших для большинства жителей Сан-Франциско совершенно одинаково. Похожая идея – проставление отпечатков пальцев на железнодорожных билетах – была предложена в Цинциннати в 1885 году.³¹

Повышение статуса идентификации

И Бертильон, и Хершель понимали, что технологии идентификации в современном обществе могут использоваться с двумя целями. С одной стороны, эти технологии востребованы правоохранными органами. Имея в своем распоряжении реестр отпечатков пальцев, достаточно сравнить с ним отпечатки, взятые с места преступления, и установить таким образом, кому они принадлежат. Этот же реестр может быть использован и в более мирных целях, например для предотвращения мошенничеств и опознания умерших.

Правоохранные органы давно настаивали на создании такого реестра, но вплоть до 1980-х годов сталкивались с неприятием этой идеи обществом. Единственный вопрос: почему? Сторонники непогрешимости отпечатков пальцев постоянно встречались с отрицательным отношением общественности к идее поголовного дактилоскопирования. В 1943 году, в самый разгар Второй мировой войны, увидела свет книга Гарольда Камминса [Harold Cummins] и Чарльза Мидлоу [Charles Midlo] «Отпечатки пальцев, ладоней и ступней» [*Finger Prints, Palms and Soles*]. Авторы писали:

Очевидно, что недалек уже тот день, когда не останется серьезных возражений против дактилоскопирования. Противников этой идеи стало меньше, однако многие еще продолжают рассматривать эту процедуру как своего рода клеймо, ибо она вызывает у них ассоциации с порядком оформления преступников в полиции. Есть надежда, что универсальная система регистрации отпечатков пальцев будет в конечном счете реализована. Все возражения возникают исключительно из-за неправильного понимания метода, «скомпрометированного» применением в криминалистике и уверенностью, что регистрация обязательно

³¹ Cummings and Midlo, *Finger Prints, palms and Soles*. Каммингс и Мидлоу исследовали вопрос использования отпечатков с древних времен. В книге приводится фотография идентифицируемого отпечатка с палестинской лампы, возраст которой датируется IV–V вв. н. э., предоставленная доктором Бадэ [Bade] из Палестинского института в Pacific School of Religion. Также приведена фотография китайской печати III в. до н. э. «На одной стороне печати нанесено имя, а на другой – четко различимый отпечаток большого пальца. Нахождение этого отпечатка на печати позволяет предположить, что он использовался как персональное клеймо, но был ли он сделан с той же целью, что и современные системы идентификации по отпечаткам пальцев – вопрос спорный». В качестве источника некоторых приведенных фактов авторы ссылаются на книгу: Alfred C. Haddon, *Evolution in Art* (Scribner's, 1895).

нарушит основные свободы.³²

Почему же общество опасается массовой регистрации? Возможно, потому, что мы знаем: отпечатки пальцев не могут гарантировать отсутствие ошибок, а сам реестр может быть использован не по назначению. Вот несколько примеров, которые заставляют задуматься:

- идентификация по отпечаткам пальцев осуществляется людьми, а людям свойственно ошибаться;
- чьи-либо отпечатки пальцев могут оказаться на месте преступления по вполне законной причине. Присутствие идентифицируемых отпечатков создает презумпцию виновности;
- отпечатки могут быть случайно или преднамеренно перепутаны в полицейской лаборатории;
- хранимые в полиции файлы с отпечатками могут быть преднамеренно изменены с целью обвинения невиновного;
- экспертные заключения по анализу отпечатков могут быть перепутаны или специально изменены.

Чем больше мы доверяем технологиям идентификации, тем больше различных видов мошенничества получаем взамен, а возможность преднамеренного мошенничества мы не сможем исключить никогда. Именно по этой причине дактилоскопирование не может гарантировать идентификацию, оно лишь обеспечивает связь конкретного пальца с записью в файле. Измените файл, и вы измените идентификацию.

Но у монеты есть и обратная сторона: дактилоскопия как средство строгой идентификации может быть использована репрессивными и тоталитарными режимами. Люди, стоящие у руля в таких обществах, обеспечивают свою власть в том числе и благодаря тому, что любой противник существующего порядка может быть идентифицирован и будет постоянно находиться под угрозой расправы до тех пор, пока не покорится или не будет уничтожен. Пропускная система во времена апартеида в Южной Африке и идентификационные карточки, выдаваемые палестинцам на оккупированных Израилем территориях, являются типичными примерами таких систем идентификации. Недемократические режимы нуждаются в системах точной идентификации: если подвергнуть наказанию не того человека, это увеличит число противников режима и, что, вероятно, более важно, даст возможность уйти от ответственности истинному виновнику.

В Соединенных Штатах никогда не предпринимались попытки создания тотальной системы для регистрации отпечатков пальцев. Вместо этого штаты и Федеральное правительство фиксировали отпечатки пальцев только у арестованных и у людей определенных профессий. Эта информация хранилась на так называемых «десятипальцевых картах» [ten-print card] – по одному отпечатку каждого пальца рук. Карты классифицировались экспертами и хранились в специальных ящиках. Иногда полицейские управления создавали по две копии карты: одну для локального использования, вторая отсылалась в ФБР.

К концу XX века стремление к всеобщему дактилоскопированию стало ослабевать. Причина этого проста и кроется в принципиальном противоречии, которым обладает любой проект глобальной идентификации: чем больше снято отпечатков, тем сложнее идентифицировать кого-либо по одним лишь отпечаткам.

К 1987 году в ФБР хранилось 23 миллиона дактилоскопических карт с отпечатками преступников, а в одном только штате Калифорния этих карт было 7,5 миллиона.³³ В

³² Ibid.

³³ Wilson and Woodard, *Automated Fingerprint Identification System*.

действительности такой объем информации привел к тому, что систему стало можно использовать лишь для подтверждения идентификации: зная имя, следователь мог запросить конкретную дактилоскопическую карту и сравнить отпечатки. На практике оказалось невозможным лишь по набору отпечатков пальцев определить имя человека, которому они принадлежат. База отпечатков выросла настолько, что ее просто стало невозможно использовать с целью, ради которой она создавалась! В середине 1980-х годов один следователь из Сан-Франциско подсчитал, что если он будет работать по восемь часов в день без выходных, то ему понадобится 33 года, чтобы вручную просмотреть городскую дактилоскопическую картотеку, в которой хранилось 300 тысяч карт.³⁴

Автоматизированная система идентификации отпечатков пальцев

Но, несмотря на это, дактилоскопические методы все же используются. Это стало возможным в том числе и благодаря автоматизированной системе идентификации отпечатков пальцев, известной также как AFIS [Automated Fingerprint Identification System]. В 1980-х годах эта система полностью изменила роль и место дактилоскопии. Система совместила в себе относительно несложную компьютерную графику и специальные алгоритмы для анализа и поиска соответствий в изображениях отпечатков пальцев, а также использовала компьютеры с параллельными вычислениями для достижения ошеломляющих результатов в следственной науке.

Компьютеры сличают отпечатки совсем не так, как люди. Они не рассматривают изображение как сочетание дуг, петель и кривых, а преобразуют его в таблицу двумерных векторов.

Эти векторы, называемые «минутиями»,^[p9] описывают точки изображения, где отрезки линий начинаются, заканчиваются или раздваиваются. Каждая минутия имеет свои координаты на плоскости (x, y) и направление.

Обычно отпечаток пальца описывается 90 или более минутиями, сочетание которых уникально. Процедура поиска в AFIS заключается в сравнении набора минутий всех десяти пальцев, что составляет около 900 точек, со всеми хранимыми в базе данных записями. Такой поиск осуществляется специализированным компьютером, носящим название «сравнитель». В 1987 году скорость работы обычного сравнителя находилась в пределах от 500 до 600 отпечатков в секунду. Сегодня они работают в десятки раз быстрее, и база данных, содержащая миллион записей, просматривается приблизительно за 30 минут. Для ускорения процесса полиция может задействовать дополнительный сравнитель. Работая параллельно, каждое над своей частью базы данных, два устройства выполняют задачу за 15 минут. Современные системы могут объединять от пяти до десяти сравнителей, что сокращает среднее время поиска до нескольких минут.

AFIS дала полиции возможность сверять найденные отпечатки со всей базой данных. Система также позволяет вести поиск по фрагменту отпечатка, обнаруженного на месте преступления. Приведенный ниже отрывок из отчета Министерства юстиции 1987 года расхваливает удивительные достижения новой технологии:

Поиск отпечатка по базе данных AFIS полицейского управления Сан-Франциско стоил тысяч часов ручной работы в течение восьми лет. Отпечаток принадлежал убийце бывшей узницы концлагерей времен Второй мировой войны Мириам Сламович [Miriam Slamovich]. Женщина была убита выстрелом в упор в своем доме в 1978 году. Преступник оставил на месте преступления четкий

³⁴ Ibid., p. 14.

p9

Minutiae (англ.) – мелочь.

отпечаток пальца, но, в отсутствие конкретных подозреваемых и других улик, шанс найти преступника путем традиционной ручной сверки отпечатка с базой данных был ничтожен. Несмотря на это, полицейские не прекращали расследование, и когда в 1985 году система AFIS была внедрена, она нашла нужный отпечаток за шесть минут. Убийца Славович был взят под стражу в тот же день.³⁵

В 1988 году я присутствовал на проходившей в Бостоне конференции по AFIS, где познакомился с детективом Кеном Мозесом [Ken Moses] из полицейского управления Сан-Франциско. Мозес рассказал мне, что в 1984 году, когда в их полицейском управлении была внедрена автоматизированная система распознавания отпечатков пальцев, число краж в городе снизилось на 26 %.³⁶ И этому есть объяснение: в 40 % случаев краж на месте преступления остаются отпечатки пальцев, 28 % из них удается идентифицировать, а доказательство принадлежности отпечатков пальцев в 93 % случаев приводит к обвинительному приговору. К концу 1985 года в Сан-Франциско благодаря системе AFIS была доказана вина более 900 преступников.

AFIS позволила полиции Сан-Франциско сделать еще одну немыслимую ранее вещь: повернуть время вспять и успешно завершить расследование старых, нераскрытых преступлений. Начиная с дела об убийстве Славович полиции удалось раскрыть 816 нераскрытых преступлений, в том числе 52 убийства. (За предыдущий год всего 58 преступлений было раскрыто при помощи анализа оставленных преступником отпечатков пальцев.)

Опыт Сан-Франциско стал распространяться. В Калифорнии дело «Ночного stalkера» [Night Stalker] также было раскрыто при помощи AFIS благодаря идентификации оставленных на угнанных машинах отпечатков пальцев. В течение нескольких месяцев после внедрения AFIS в Балтиморе, штат Мэриленд, было идентифицировано 525 человек, назвавших при аресте вымышленное имя. Быстрый успех AFIS был настолько ошеломляющим, что Министерство юстиции писало в своем отчете:

«AFIS оказала на повышение эффективности работы правоохранительных органов такое же влияние, как начало широкого использования компьютеров в уголовно-процессуальной практике в 1960-е годы».³⁷

Поспешность внедрения AFIS привела к тому, что был упущен из виду один из ключевых вопросов, а именно вопрос о точности базовой технологии. Частично это произошло из-за того, что уникальность отпечатков пальцев уже давно была закреплена в американском законодательстве. Другой причиной стал тот факт, что в случае сомнений обнаруженное AFIS совпадение отпечатков могло быть проверено человеком визуально. Поскольку база данных AFIS строилась путем сканирования дактилоскопических карт, уже имевшихся в распоряжении полиции, система была внедрена повсеместно без учета мнения общественности. Сами же правоохранительные органы при внедрении системы были озабочены гораздо более прагматичными вопросами: определение юрисдикции систем AFIS, используемых городами, штатами и Федеральным правительством; обеспечение совместимости форматов хранения данных системами AFIS разных производителей и, конечно, постоянное пополнение базы данных цифровых отпечатков.

³⁵ Ibid., p. 1.

³⁶ Интервью автору, 11 июля 1988 года.

³⁷ *Automated Fingerprint Identification System*, p. 1.

Автоматизированная система идентификации отпечатков пальцев



Этот терминал используется для просмотра результатов компьютерного поиска в базе данных, содержащей оцифрованные изображения отпечатков пальцев. Система AFIS анализирует изображение и строит список характеристических точек – точек, в которых начинаются, заканчиваются или раздваиваются отрезки папиллярных линий. Полученная в результате матрица служит в дальнейшем ключом поиска по базе данных. Поиск осуществляется очень быстро и очень точно: требуется всего около одной минуты для просмотра базы данных, содержащей миллион изображений, для нахождения совпадающего с образцом отпечатка. Показанная система разработана специалистами на распознавании отпечатков подразделением фирмы NEC Technologies, которая создала свое биометрическое приложение около 30 лет назад и продолжает занимать лидирующее место на этом рынке. Сегодня технологии биометрической идентификации фирмы NEC используются более чем в 300 различных приложениях в 14 странах. Существуют специализированные системы для использования в здравоохранении, при лицензировании, социальном обеспечении и области безопасности. Многие города и штаты активно разворачивают подобные системы, стремясь построить глобальную базу данных, содержащую отпечатки пальцев каждого гражданина, независимо от того, привлекался он к уголовной ответственности или нет. Такая база данных, по словам сторонников, могла бы оказать существенную помощь как в раскрытии преступлений, так и в идентификации умерших или потерявшихся людей. [Фотография любезно предоставлена фирмой NEC Technologies]

С гораздо большим числом противоречий пришлось столкнуться при внедрении систем идентификации на базе ДНК. Эту технологию часто не совсем корректно называют «дактилоскопией ДНК» [DNA fingerprinting].

Идентификация по ДНК

Дезоксирибонуклеиновая кислота, более известная под названием ДНК, – молекула, которая одновременно разделяет и объединяет нас. При помощи ДНК наследственные признаки передаются следующим поколениям, сходство ДНК характерно для семей и кланов, ДНК – виртуальное связующее звено всех наций. При этом именно различие в ДНК делает каждого человека уникальным. Сходство ДНК связывает нас с обоими родителями, но ее уникальность делает нас отличными от них.

Идентификация по ДНК основана на анализе цепочек генов и является почти безупречной. Сегодня у нее три основных применения:

- установление отцовства;
- определение принадлежности крови и семенной жидкости, оставленных на месте преступления;
- идентификация человеческих останков.

Поскольку ДНК наследует признаки родителей поровну, ее относительно легко

использовать для определения отцовства: все, что необходимо, – это образцы небольшого количества клеток, взятых от ребенка, матери и предполагаемого отца. В последние десять лет анализ ДНК все чаще стал применяться и в судебных делах. Такая экспертиза идеальна для случаев, когда на месте преступления не обнаружено отпечатков пальцев, поскольку для ее проведения достаточно небольшого количества генетического материала: капли крови, слюны, семенной жидкости, волоска или частички кожи. Как сказал доктор Майкл Бэйрд [Michael Baird] из лаборатории Lifecodes Lab: «Если на вашей рубашке обнаружится пятнышко крови, совпадающее с кровью жертвы, высока вероятность, что убийца – вы³⁸».

Все чаще анализ ДНК применяется для идентификации человеческих останков. Поскольку молекула ДНК чрезвычайно стабильна, необходимый для анализа материал может быть получен из останков через годы или даже через тысячи лет после смерти человека. Исходя из этих соображений американские военные заносят в специальную базу данных информацию о ДНК каждого военнослужащего. Соединенным Штатам больше никогда не придется хоронить останки неизвестного солдата. Тем временем характер споров, постоянно ведущихся по поводу анализа ДНК, постепенно изменился. Сразу после появления этой технологии ученые, юристы и защитники гражданских свобод высказывали сомнения относительно ее научной обоснованности и эффективности. Сегодня анализ ДНК повсеместно признан абсолютно точным, и мы боремся за общественное признание этой точности.

Становление науки: анализ ДНК в 1986–1996 годах

Основой для анализа ДНК является геном человека. Каждый из нас несет в себе уникальный генетический код, состоящий из более чем трех миллиардов оснований нуклеиновых кислот: аденина (А), гуанина (G), цитозина (С) и тимина (Т). Каждая клетка человеческого тела содержит копию генетического кода этого человека, являющегося уникальным для каждого жителя планеты. В отличие от отпечатков пальцев, генетический код невозможно изменить путем операции или отрезания рук.

Несмотря на всю мощь технологий идентификации ДНК, им присущи некоторые фундаментальные проблемы. Первая проблема заключается в том, что, в отличие от отпечатков пальцев, ДНК не во всех случаях является уникальной: однайцовые близнецы по определению имеют один и тот же набор хромосом. И таких близнецов достаточно много: в Северной Америке в среднем на 83,4 рода приходится один случай появления на свет близнецов, при этом 28,2 % имеют одинаковые ДНК, так как развиваются из одной клетки. Таким образом, приблизительно 0,338 % населения являются однайцовыми близнецами, т. е. три человека из тысячи. Принятие ДНК как единственного средства идентификации в масштабе страны немедленно приведет к тому, что с ее точки зрения будет существовать миллион генетических двойников.

Вторая проблема систем идентификации на базе ДНК заключается в неполном использовании генома человека, состоящего из трех миллиардов оснований: геном слишком велик. Кроме того, использование для идентификации целого генома не имеет смысла, ибо ДНК двух отдельно взятых людей совпадают почти на 99 %. Вместо этого при экспертизе ДНК используется анализ участков этой молекулы, которые, судя по всему, не используются для каких-либо функций, их часто называют «мусорными участками» *[p10]* ДНК. Поскольку эти фрагменты генома не участвуют в жизнеобеспечении клеток или организма в целом, из поколения в поколение происходят их случайные изменения, или мутации. При производстве экспертизы ДНК идентичность представленных образцов определяется именно

³⁸ Интервью автору, 1 марта 1991.

p10

Junk (англ.) – мусор

соответствия. Для осуществления этих тестов использовались образцы с места преступления и образцы крови подозреваемого. Далее ДНК разбивается на фрагменты различного размера путем ее обработки энзимами. Фрагменты помещаются в гель и подвергаются воздействию электрического поля, в результате чего происходит их сортировка по размеру. Фрагменты обрабатываются веществом-маркером, выявляющим определенные участки хромосом. Там, где маркер задержался, появляется черная линия или полоса. Если образец ДНК имеет фрагменты же размера, что и ДНК подозреваемого, делается вывод об их совпадении. Пример предоставлен Cellmark Diagnostics, одной из ведущих лабораторий, осуществляющей судебную идентификацию ДНК. [Фотография любезно предоставлена Cellmark Diagnostics, Inc., Германтаун, штат Мэриленд].

Анализ ДНК впервые вошел в судебную практику США в 1987 году, в то время мало кто из адвокатов в достаточной степени разбирался в этой науке, чтобы подавать такие протесты. Следствие представляло анализ ДНК суду и присяжным как устоявшуюся научную теорию, несмотря на то что идея была высказана всего около года назад. К 1991 году анализ ДНК использовался при расследовании тысяч уголовных преступлений. Но не обошлось и без проблем. В 1989 году при рассмотрении дела «Народ против Кастро»⁴⁰ суд первой инстанции принял в качестве доказательства результаты анализа ДНК, руководствуясь тем, что анализ ДНК в общем признается учеными, однако Апелляционный суд отверг доказательства по причине допущенных со стороны лаборатории явных нарушений. В ноябре 1989 года Верховный суд штата Миннесота отверг результаты анализа ДНК в деле «Штат против Шварца»⁴¹ по причине низкого уровня контроля качества в лаборатории и того факта, что она не смогла предоставить данные выборки по населению, на основании которых основывалось статистическое заключение. Но в этом же году Специальный апелляционный суд штата Мэриленд постановил при рассмотрении дела «Кобей против Штата»⁴² признать результаты экспертизы ДНК в качестве доказательства, отметив при этом, что признание анализа ДНК «не является обязательным для всех уголовных расследований».

Внезапно создалась странная ситуация: как только обвинение пыталось использовать в качестве доказательства результаты анализа ДНК, расследование тут же переходило в другую плоскость – доказательство научной состоятельности самого метода анализа ДНК. Целый ряд статей и исследований отстаивал технологию, но все они были написаны людьми либо входящими в штат экспертных лабораторий, либо привлекаемыми к расследованию в качестве экспертов ФБР или прокуратурой штата. Никто из научного сообщества не мог высказать непредвзятое мнение, но все, кто имел отношение к этой науке, были в ней заинтересованы.

Чтобы положить конец спорам, в 1989 году Национальный совет по исследованиям [National Research Council, NRC] создал Комитет по технологиям ДНК в криминалистике [Committee on DNA Technology in Forensic Science], который должен был заняться изучением технологий идентификации на основе ДНК.

NRC входит в Национальную академию наук и является одной из самых престижных исследовательских организаций США, образцом объективности и научного опыта. Комитет признал корректность базовой научной теории. Однако требовалась стандартизация некоторых моментов, в частности используемых маркеров, для чего, в свою очередь, была необходима большая база с генетическими данными населения. И здесь комитет допустил большую ошибку. Пытаясь уладить статистические споры между экспертами-практиками по

⁴⁰ *People v. Castro*, 144 Misc. 2d 956, 545 N.Y.S. 2d 985 (Sup. Ct. 1989).

⁴¹ *State v. Schwartz*, 447 N.W. 2d 422 (Minn. 1989).

⁴² *Cobey v. State*, 80 Md. App. 31, 559 A.2d 391 (Md. App. 1989).

ДНК и группой, изучающей генетику, комитет рекомендовал использовать при экспертизе новый статистический подход, получивший название «принцип промежуточных ограничений». В основе принципа лежала математическая формула для расчета вероятности ошибочного совпадения,^[p11] и она была более консервативна, нежели использовавшаяся к тому времени.

«Это создало юридический клинч», – объяснял мне Марк Столорой [Mark Stolorow], менеджер по криминалистике компании Cellmark Diagnostics.⁴³ Проблема заключалась в том, что юридический принцип признания научных доказательств в суде, называемый «стандарт Фрая» [Frye standard], требовал, чтобы используемая при этом научная методика была тщательно изученной и общепринятой в научном сообществе. Но предложенный NRC принцип не был общепринятым, он был изобретен членами созданного NRC комитета.

В апреле 1993 года директор ФБР Уильям Сешенс [William Sessions] предложил NRC провести дополнительное исследование, чтобы устранить недоразумение. Несмотря на то что подобного рода пересмотр заключения не имел прецедентов, его необходимость была очевидна. Однако процесс затормозился. NRC созвал новый комитет 30 августа 1993 года, однако он не начинал свою работу до сентября 1994 года из-за неопределенности с финансированием. Новая версия отчета появилась лишь в 1996 году.

К моменту, когда NRC выпустил вторую и окончательную версию отчета, согласие уже было найдено. В ноябре 1995 года журнал *Nature* опубликовал статью, озаглавленную «Спорам об идентификации по ДНК положен конец».⁴⁴ Подтверждением названия стал тот факт, что статья была написана в соавторстве самыми яркими противниками в этом споре – Эриком Лэндером [Eric S. Lander] и Брюсом Бадюли [Bruce Budowle]. В этой статье Лэндер, ученый-генетик Центра по изучению генома при Институте Уайтхеда [Whitehead Institute Center for Genome Research], и Бадюли, руководитель Учебно-исследовательского криминалистического центра ФБР [FBI's Forensic Science Research and Training Center], согласились, что научная теория о ДНК обоснована. При условии, что лаборатории примут все меры по недопущению ошибок, анализ ДНК может считаться таким же точным способом, как и другие технологии идентификации.

Анализ ДНК сегодня

Очень сложно переоценить значение идентификации по ДНК. Сегодня эта методика коренным образом изменила процедуру определения отцовства при назначении алиментов. «Знаете, как эта процедура происходила раньше? – спросил меня доктор Дэвинг Бинг. – Ребенка представляли суду и спрашивали, похож ли он на отца».

Анализ ДНК также помогает людям, которые просто хотят *знать*, являются ли они кровными родственниками, полностью или частично, при этом их не интересует дальнейшее использование этой информации в суде. CBR Laboratories проводила несколько таких тестов для установления родства, рассказывает Бинг, в прошлом член совета директоров этой лаборатории. Для проведения теста необходимы образцы ДНК от обоих человек, желающих установить, являются ли они кровными родственниками, а также от максимального количества родственников с обеих сторон. Стоимость теста (\$200 на человека) не слишком высокая цена за душевное спокойствие, которое он дает. Анализ может быть проведен в тайне от человека и без его согласия: образцы ДНК легко можно получить с кусочка ткани,

p11

Вычисления производились путем перемножения частот встречаемости аллелей и сравнения результата со статистическими данными для указанной группы.

⁴³ Интервью автору, июль 1997.

⁴⁴ E. S. Lander and B. Budowle, «DNA Fingerprinting Dispute Laid to Rest», *Nature*, 371 (1994), p. 735–738.

которым человек пользовался. «Вообще говоря, мы не должны писать отчет, мы просто должны сделать анализ», – говорит Бинг. Для этого не требуется поручение суда, так как речь не идет о расследовании преступления, связанного с этими образцами. Результаты анализа дают ответы на очень важные вопросы. Лаборатория Бинга помогает ответить на эти вопросы любому, если его представляет юрист, врач, адвокат, социальный работник или частный детектив.

Сегодня безупречность доказательств на базе анализа ДНК используется для пересмотра обвинений, предъявленных до появления этой технологии. Действующий при юридической школе Кардозо университета Ешива проект «Невиновность» [The Innocence Project at Yeshiva University's Cardozo School of Law] специализируется на использовании в качестве доказательства анализа ДНК для инициации пересмотра дел и оправдания несправедливо осужденных. В отчете Национального института юстиции за 1996 год рассказывается о 28 прецедентах, когда несправедливо осужденного человека освобождали после подтверждения его невинности при помощи анализа ДНК. В среднем осужденные провели в заключении около семи лет.⁴⁵ Анализ ДНК использовался также для воссоединения похищенных во время «грязной войны» в Аргентине детей с их бабушками, дедушками и другими членами семьи.

Реабилитация возможна и после смерти. Сын доктора Сэма Шеппарда [Sam Sheppard] из Кливленда не терял надежды при помощи анализа ДНК доказать невинность отца, обвиненного в 1954 году в убийстве жены, Мэрилин Шеппард [Marilyn Sheppard]. Сэм Шеппард провел в тюрьме десять лет и был оправдан после пересмотра дела в 1966 году, но у многих людей остались сомнения в его невинности. Его сын Сэм Риз Шеппард [Sam Reese Sheppard] добился разрешения на эксгумацию тела отца, чтобы провести сравнительный анализ его ДНК с образцами крови и телесных жидкостей, обнаруженных на месте преступления.⁴⁶ Анализ подтвердил, что обнаруженная на месте преступления кровь принадлежит не Шеппарду или его жене, а другому человеку.

Банк данных ДНК

Утром 25 ноября 1991 года человек в маске вломился в дом молодоженов недалеко от Спрингфилда, штат Иллинойс, застрелил мужа, изнасиловал жену, после чего выстрелил в нее и оставил умирать. Удивительно, но женщина выжила. Следствие взяло для анализа семенную жидкость, оставленную преступником, и произвело сравнительный анализ по идентификации ДНК. Поиск производился в компьютерной базе данных, содержащей информацию о ДНК, но совпадений обнаружено не было. Поскольку женщина не могла опознать преступника визуально, полиция потеряла все нити, и следствие зашло в тупик.

В апреле полиция Спрингфилда при расследовании другого преступления взяла для анализа образцы ДНК мужчины, обвиняемого в изнасиловании семнадцатилетней девочки, и ввела информацию в компьютер. На этот раз компьютер обнаружил совпадение ДНК с образцами из ноябрьского дела. В конечном счете присяжные признали обвиняемого Артура Дейла Хики [Arthur Dale Hickey] виновным в убийстве первой степени и покушении на убийство, отягченными сексуальным насилием и вторжением в жилище. Хики был приговорен к смертной казни.

По данным ФБР, 67 % насильников совершают более одного нападения, причем в среднем обнаруживается 2,8 нападения, а 5,2 нападения не обнаруживается. Технология

⁴⁵ «Convicted by Juries, Exonerated by Science: Case Studies in the Use of DNA Evidence to Establish Innocence After Trial», National Institute of Justice Research Report, июнь 1996. Полный текст документа доступен по адресу <http://www.ncjrs.org/txtfiles/dnaevind.txt>.

⁴⁶ «Son in Sheppard case Wins an Exhumation Bid: Seek DNA Testing to Vindicate Father», Associated Press, *Boston Sunday Globe*, 13 июля 1997, p. A16.

идентификации по ДНК позволяет раскрыть большинство этих случаев. В связи с этим Правительство США в законодательном порядке обязало все штаты регистрировать информацию о ДНК всех осужденных за половые преступления. Но законодатели многих штатов не ограничились лишь насильниками. В некоторых штатах все осужденные за преступления, связанные с насилием, должны сдать материал для идентификации ДНК. В других штатах процедура «генетического дактилоскопирования» подвергаются все осужденные, даже за ненасильственные преступления. В некоторых штатах в базах данных хранится генетическая информация и о людях, всего лишь обвинявшихся в совершении преступлений.

«Генетические отпечатки» хранятся в базе данных ФБР, называемой «комбинированная система индексации ДНК» [Combined DNA Index System, CODIS]. Введенная в действие в 1994 году в соответствии с «Законом об идентификации ДНК» [DNA Identification Act] система представляет собой компьютерную сеть, используемую для получения профилей ДНК и поиска совпадений уполномоченными органами всех уровней: местного, уровня штата и федерального. Пилотный вариант программы функционировал с 1991 года.

Профили ДНК создаются как на базе улик, оставленных на месте преступления, так и на базе образцов, взятых от осужденных. Когда в CODIS заносится новый профиль, он автоматически проверяется на совпадение с уже имеющимися в базе профилями, относящимися к нераскрытым преступлениям. В случае обнаружения совпадения в лабораторию, поместившую новые данные, автоматически отсылается уведомление по электронной почте.

Однако наполнение базы данных стало проблемой. Летом 1997 года база CODIS содержала около 125 тысяч профилей ДНК преступников и около 20 тысяч профилей ДНК, относящихся к нераскрытым преступлениям. Остальные 400 тысяч описанных ДНК осужденных ждали своей очереди на ввод в компьютерную систему. К ноябрю 1998 года число необработанных записей в целом по США выросло до 450 тысяч.⁴⁷ ФБР запросило ассигнования в размере 22,5 миллиона долларов для «освоения» этого задела.

Но самую большую базу данных ДНК создало Министерство обороны США. Целью создания военным ведомством реестра ДНК было опознание останков погибших военнослужащих. На 31 декабря 1995 года в хранилище образцов содержалось 1,15 миллиона образцов.

На web-сайте Министерства обороны можно найти следующую информацию о хранилище:

Кровь помещается в специальные карты, на лицевую сторону которых наносятся номер социального страхования военнослужащего, дата рождения и род войск. На обратной стороне карты размещаются отпечатки пальцев, штрих-код и подпись, подтверждающая правильность образца. Карты с образцами крови содержатся в хранилище образцов в специальной вакуумной упаковке при температуре -20 °C. Мазок из полости рта (соскоб с поверхности щеки) хранится в изопропиловом спирте при комнатной температуре. Во избежание путаницы или неверной маркировки образцов приняты специальные меры безопасности.

Похоже, что однажды этот банк ДНК будет использован не только для идентификации, так как Министерство обороны хранит не просто результаты отбора отдельных ДНК, а цельные клетки крови. В конечном счете военные создали крупнейшее в мире хранилище отлично сохраненного генетического материала, причем по каждому образцу министерство обладает подробной медицинской и другой информацией. По прошествии времени, когда

⁴⁷ Paul Ferrara, chair, «Laboratory Funding Issues Working Group Report», in *Proceedings of the National Commission on the Future of DNA Evidence*, 23 ноября 1998. Копия доступна по адресу <http://www.ojp.usdoj.gov/nij/dnamt/trans3/trans-j.html>.

база разрастется, ее хранители будут подвергаться постоянному давлению с целью получения образцов для научных исследований и, возможно, для криминальных расследований. Вполне вероятно, что этот проект, ожидает постепенное изменение целей хранения, так же как и другие проекты создания федеральных банков данных.

Компьютерная биометрия

Несмотря на свою высокую точность, ни дактилоскопия, ни анализ ДНК не подходят для идентификации личности в повседневной жизни. Вариант с отпечатками пальцев неприемлем: за более чем 100 лет его сторонники не смогли избавиться использования этой технологии от ассоциаций с преступностью. Идентификация по ДНК также неприемлема, поскольку для идентификации требуется значительное время – минуты или даже часы. К счастью, последние 100 лет люди используют другой способ биометрической идентификации, почти такой же хороший, как отпечатки пальцев или анализ ДНК. Это фотография.

Сегодня наиболее распространенной формой идентификации является помещение фотографии на официальный документ. Повсюду в мире универсальным способом идентификации личности является паспорт. Во многих европейских странах паспорт дополняется идентификационной карточкой. В Соединенных Штатах водительское удостоверение с фотографией является самой распространенной формой идентификации как в частном, так и в государственном секторе.

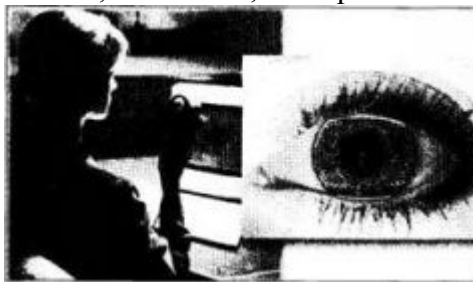
Надежность водительских удостоверений зависит от двух факторов. Во-первых, штат должен быть уверен, что удостоверение выдано соответствующему лицу. Во-вторых, само по себе удостоверение должно быть хорошо *защищено от подделки*, т. е. выпущенное удостоверение невозможно изменить. (Удостоверения, которые легко подделать, просто провоцируют преступления, так как удостоверение может быть украдено, изменено и использовано затем в мошеннических целях.) Штаты все более и более успешно используют при изготовлении удостоверений экзотические материалы, что затрудняет их подделку. Но в общем они выполняют лишь простую функцию идентификации личности водителя. Самая большая проблема с водительскими удостоверениями в США заключается в том, что каждый штат выпускает свои удостоверения, и они очень различаются по оформлению. Кассиру в штате Массачусетс очень сложно установить, действительно ли предъявленное удостоверение выпущено в штате Монтана или это подделка.

Перейдем теперь к компьютеризованным системам идентификации. Все современные системы биометрической идентификации, так же как и рассмотренная выше AFIS, состоят из двух частей. Первая – это устройство, которое производит измерение какого-либо параметра человеческого тела и преобразует его в цифровую форму. Вторая – большая база данных, хранящая результаты биометрических измерений сотен, тысяч или даже миллионов людей. Во многих случаях онлайн-база данных может свести на нет проблему подделок: если фальшивый кусок пластика изготовить можно, то ввести фальшивую запись в правительственную базу данных несравнимо труднее.

За последние десять лет было разработано множество систем биометрической идентификации. Самая простая – создание онлайн-базы водительских удостоверений с фотографиями. Однако постоянно изобретаются и проверяются все более сложные системы. Вот примеры некоторых из них.

Рисунок сетчатки глаза. Сетчатка похожа по своей индивидуальности на отпечатки пальцев. Но вместо папиллярных линий в этой системе записывается и анализируется уникальный рисунок внутри глаза человека. В 1980-е годы были популярны системы, анализирующие картину, образуемую венами и артериями глаза. Однако, в отличие от отпечатков пальцев, рисунок сетчатки подвержен изменениям: у женщин во время беременности под воздействием гормонов плода в глазу могут образовываться новые сосуды, меняющие рисунок. Общеизвестно, что эта система дискриминирует женщин,

которым приходится объяснять при каждом несовпадении изображений сетчатки, что они беременны, почему они беременны и, возможно, что произошло с плодом.



Сканирование радужной оболочки

Из всех известных систем биометрической идентификации сканирование радужной оболочки является наиболее точным и стабильным. Тонкий узор на радужке формируется еще до рождения и остается неизменным на протяжении всей жизни (кроме случаев травм и хирургического вмешательства, конечно). Изображение узора радужной оболочки может быть получено с использованием видеокамеры высокого разрешения, и оно настолько уникально, что вероятность совпадения биометрических показателей радужки двух людей составляет один шанс из 10^{78} . (Для сравнения: население Земли составляет всего около 10^{10} .) Даже однояйцовые близнецы имеют различающиеся радужные оболочки. Однако следует помнить об одной вещи: сканирование радужки идентифицирует не человека, а лишь его радужную оболочку. Узнать по результатам сканирования имя человека можно только после поиска в компьютерной базе данных. Если база данных была взломана и модифицирована, сканирование радужной оболочки не даст правильной идентификации. [Фото любезно предоставлено IriScan, Inc.]

Рисунок радужной оболочки. Особенно популярны системы на базе радужной оболочки были в 1990-е годы. Радужная оболочка формируется еще *во время внутриутробного развития*, поэтому остается неизменной на протяжении всей жизни человека. Получить ее изображение можно с помощью стандартной видеокамеры, а не дорогостоящего и неудобного сканера, как в случае с сетчаткой. Одним из лидеров в этом секторе является компания IriScan, чьи технологии используются в тюрьмах, в автоматических кассовых машинах (банкоматах), а недавно стали использоваться и на станциях метро. British Telecom, являющаяся партнером этой фирмы, разработала высокоскоростной сканер радужной оболочки, который может получать изображение радужки человека, сидящего в машине, движущейся со скоростью 90 км/час. Сегодня такой сканер очень дорог, для него требуется специальная оптика, камера высокого разрешения и управляемый компьютером объектив с сервоприводом.

Но, поскольку технологии постоянно развиваются, а цены падают, эта технология, вероятно, вскоре станет более доступной.

Анализ почерка. Анализ почерка и собственноручной подписи является одной из первых биометрических систем в мире. Сегодня изображение подписи может быть оцифровано и сравнено с имеющимися образцами. Если подпись ставится на специальном электронном планшете, компьютер может также анализировать скорость перемещения пера и силу нажатия. Комбинируя эти три параметра (траекторию, скорость и силу нажатия) можно построить биометрическую модель, которую очень сложно подделать. [\[p12\]](#)

p12

К сожалению, такие системы часто страдают обратной проблемой: иногда они не признают подпись законного владельца, при этом требуется достаточно много времени, чтобы «обучить» систему своей подписи. Одна такая система после 27 обучающих росписей признала у человека 9 (!) вариантов подписи, из которых относительно устойчивыми были только 3.

Отпечатки ладоней и их геометрия. При идентификации по отпечатку ладони и ее геометрии анализируется рисунок складок и относительная длина пальцев. Обе системы страдают нестабильностью по сравнению с анализом отпечатков пальцев, так как измеряемые параметры меняются со временем. С другой стороны, на них нет пятна «криминальности». Система идентификации по геометрии ладоней применялась для идентификации спортсменов на летних Олимпийских играх в Атланте в 1996 году.

Характеристики голоса. Системы голосового анализа пытаются идентифицировать говорящего путем сравнения произносимых им фраз с заранее записанными. Сегодня компьютерные системы распознавания голоса могут решать как задачу опознавания говорящего, т. е. определять, *кто* говорит, так и задачу распознавания речи, т. е. определять, *что* было сказано. В отличие от человека, современные компьютеры не могут идентифицировать говорящего и распознавать смысл сказанного одновременно, но с увеличением производительности они осилят и эту задачу. Маловероятно, что когда-нибудь компьютеры смогут опознавать человека по голосу со 100 %-ной точностью. Но и люди не могут этого. Иногда просто недостаточно информации для решения этой задачи.

Распознавание лица. Системы распознавания лица пытаются идентифицировать человека на базе визуального сходства. Для обеспечения работы современных систем необходимо, чтобы изображение лица занимало большую часть поля зрения видеокамеры компьютера, а фон соответствующим образом контролировался. В будущем такие системы должны будут распознавать лица в толпе, так же как это делает человек (и возможно, с той же степенью точности). Поскольку системы распознавания лица не носят на себе компрометирующего клейма, они не вызывают чувства опасности; в отличие от системы сканирования глаза, эти системы имеют шанс стать популярными в XXI столетии, что может привести к неожиданным результатам. «Люди, которым необходимо скрываться, опасаются систем распознавания лица, – говорит редактор журнала *Identity World* Стивен Шоу. – Эти системы не только вылавливают террористов, но могут опознавать и дипломатов, призраков и полицейских, работающих по легенде».⁴⁸

Термограмма лица. Идентификация по термограмме лица использует особенности расположения проходящих непосредственно под кожей кровеносных сосудов. Если внешний вид лица можно изменить с использованием косметики или новой прически, то кровеносную систему изменить сложнее. Поэтому считается, что термограмма лица более надежный способ идентификации, чем простое визуальное распознавание.

Идентификация по силуэту и особенностям походки. Это мое собственное название для очередной категории систем биометрической идентификации, но специалисты в этой области также его признают. Вы можете узнать своего друга издали, даже если не видите его лица. Вы идентифицируете его на основе ряда параметров, включая размеры и пропорции, особенности походки и одежды. И вновь мы исходим из предположения, что, если человек может осуществлять идентификацию такого рода, можно попытаться обучить этому и компьютер.

Производительность. Также возможно идентифицировать человека на основе данных о его производительности при решении определенной задачи. Будучи старшекурсником МТИ, я разработал компьютерную программу, которая могла идентифицировать человека по клавиатурному почерку – скорости печати и силе нажатия на клавиши при работе на клавиатуре. Во время своей работы в AT&T исследователь Томас Спитер [Thomas Speeter] разработал специальную плитку для пола, которая могла идентифицировать тех, кто по ней ходит.⁴⁹ Некоторые системы защиты от несанкционированного доступа определяют факт

⁴⁸ Интервью на конференции «Computer, Freedom and Privacy», 8 апреля 1999.

⁴⁹ Томас Спитер [Thomas H. Speeter] из AT & T Bell Laboratories разработал плитку для пола, которая могла идентифицировать ступающего по ней человека по весу и распределению давления. Опытный образец системы представлял собой единичную плитку размером около 30 см с сенсорной матрицей 16x16, где каждый сенсор

вторжения в компьютер, основываясь на принципе, что стиль работы нарушителя отличается от стиля работы законных пользователей.

Распознавание лица



В отличие от других систем биометрической идентификации, распознавание лица носит пассивный характер: оно может осуществляться без ведома человека, позволяя производить идентификацию в лифте или при проходе через дверь. Сегодня биометрические системы идентификации все чаще используются для идентификации в банкоматах (АТМ), в банках и бизнесе, требующем повышенных мер безопасности. Некоторые штаты рассматривают возможность применения систем распознавания лица в базах данных водительских удостоверений, чтобы иметь возможность выявлять лиц, получающих несколько удостоверений более чем на одно имя. [Иллюстрация любезно предоставлена Miros, Inc.]

Стиль написания. Все большее количество технологий используется для определения автора, будь то пьеса, новелла или музыкальный опус, на основе анализа особенностей стиля написания. В 1996 году Дональд Фостер [Donald Foster], специалист в области компьютеров из колледжа Вассар, проанализировал бестселлер «Основные цвета» [Primary Colors] и пришел к выводу, что «анонимный» автор на самом деле – Джо Кляйн [Doe Klein], обозреватель журнала *Newsweek*.⁵⁰ (Достаточно интересный факт: Кляйн не признавался в авторстве книги, пока журналистам *Washington Post* не удалось тайно заполучить образцы почерка Кляйна и фрагменты рукописи книги, проанализированные затем Маурин Кейси Оуэне [Maureen Casey Owens], бывшим ведущим экспертом по документам криминалистической лаборатории полиции Чикаго [Chicago Police Crime Laboratory].⁵¹) Аналогично Тед Качински [Ted Kaczinski] был идентифицирован как Unabomber лишь после того, как его брат опознал стиль письма и идеи в опубликованном манифесте.

Важно понимать, что *ни одна* из описанных здесь систем идентификации не прошла какого-либо научного обследования, как это было с идентификацией по ДНК в конце 1980-х – начале 1990-х годов. Вместо этого одиночки и компании тестировали эти технологии так же, как студенты проверяют готовность спагетти: бросают их на стенку и смотрят, не

представлял оказываемое на него давление числом в диапазоне от 0 до 255. При первом тестировании Спитер попросил 10 добровольцев наступить на плитку во время обычного прохождения по комнате, затем повернуться и пройти обратно. На базе выборки объемом в 188 испытаний (шагов) Спитер подсчитал, что может идентифицировать человека с вероятностью 99 % уже после трех тестовых шагов и с вероятностью 100 % – после четырех. Конечно, больший объем выборки был бы более убедительным, но исследование в любом случае показало, что шаги каждого человека обладают индивидуальностью, и компьютеры уже сегодня могут различать нас по шагам. См.: Thomas H. Speeter, «Identification Using Ground Reaction Force patterns», AT & T Bell Laboratories.

⁵⁰ Donald Foster, «Primary Culprit», *New York*, 26 февраля 1996, p. 50–57.

⁵¹ «Joe Klein Says He Is Anonymous *Primary Colors* Author», Associated Press, 17 июля 1996.

прилипли ли они. Если мы собираемся в будущем использовать биометрические системы в серьезных приложениях, они должны быть подвергнуты стандартизации гораздо более жесткой, чем используется сейчас. В противном случае мы получим огромное число неудачных или ошибочных идентификаций, что вызовет сомнения и недоверие и даже может привести к тому, что в тюрьму будет заключен человек, не сделавший ничего плохого.

Биометрия завтрашнего дня

С 1989 по 1995 год я жил в доме, замок на входной двери которого управлялся системой распознавания голоса. Замок давал мне свободу и власть. Свобода заключалась в возможности выходить из дома без боязни забыть ключи: поскольку мой голос всегда был со мной, я в любое время мог попасть обратно домой. А власть заключалась в возможности управлять доступом в мой дом с очень высокой точностью. Например, я мог зарегистрировать в системе голосовые характеристики подрядчика, который выполнял работу в моем доме, не опасаясь, что он передаст его кому-нибудь из своих служащих или сделает копию для себя. Мне не нужно было просить, чтобы кто-то вернул данный ему ключ, я просто стирал характеристику его голоса из памяти замка.

Но и здесь не обошлось без проблем. Через несколько месяцев я обнаружил, что замок не опознает мой голос при сильном ветре или шумном ливне. Я также заметил, что эта биометрическая система недемократична: некоторые люди никак не идентифицировались системой, в то время как другие распознавались ею с первого раза. (Есть сведения о подобных проблемах и в системах распознавания по отпечаткам пальцев.) В конечном итоге я создал «безголосовые коды», позволявшие людям входить без предварительного произнесения парольной фразы.

В грядущем столетии ситуации, подобные моей, будут широко распространены, ибо системы биометрической идентификации все шире заменяют собой ключи и идентификационные карточки. Биометрия будет применяться для управления дверями офисных зданий и защиты компьютерных файлов. Ваш компьютер сможет опознавать, вы ли сидите перед ним, либо по голосу, либо с помощью встроенной видеокамеры. Тому, что люди предпочитают биометрические системы, есть простое объяснение: отпадает необходимость в различного рода паролях, которые можно забыть, и идентификационных карточках, которые можно потерять. В то же время некоторые люди будут дискриминированы, если из-за их индивидуальных особенностей биометрические показатели не смогут быть правильно записаны или стабильно воспроизведены.

Представим себе университет 2020 года. В столовой студенты берут подносы, выбирают понравившиеся блюда и идут с ними в обеденный зал. Компьютерная система сканирует содержимое подносов, вычисляет стоимость обеда, после чего визуальным образом идентифицирует студента по лицу и узнает, с чьего счета снять соответствующую сумму. В библиотеке другая система распознавания лиц давно уже заменила традиционные библиотечные карточки. Компьютер санкционирует вход студента в лабораторию после сканирования его лица – это особенно важно для лабораторий с материалами, которые могут быть использованы террористами. А когда студент садится перед компьютером, система автоматически пускает его и открывает доступ к его файлам.

В университете будущего не будет необходимости изготавливать для каждого студента идентификационную карточку: присоединенная к университетской сети интеллектуальная видеокамера замечательно справится с этой работой. Но университету, возможно, все-таки придется выпускать какие-либо идентификаторы для студентов, чтобы они могли подтвердить свою принадлежность к университету за его пределами. И конечно, университет примет все меры, чтобы не допустить вторжения посторонних в свою биометрическую базу данных.

Университетская система биометрической идентификации работает потому, что университет представляет собой замкнутую среду, а студенты находятся в ней добровольно.

Поскольку студенты платят значительные суммы за получение образования, а университетские ресурсы, такие как библиотеки, спортивные залы и общежития, не являются ресурсами общего пользования, студенты сами заинтересованы в надежной их идентификации учреждением.

Многие магазины оборудованы видеокамерами, записывающими изображения всех входящих в них людей. (Часто эти камеры устроены таким образом, чтобы записывать и рост человека.) Очень скоро эти камеры, возможно, будут подключены к компьютерным сетям, что позволит идентифицировать человека по лицу и другим признакам. Компьютерная сеть магазина путем обращения к общедоступным записям сможет определить, не разыскивается ли данный человек компетентными органами. Обратившись к другим базам данных, она может установить, не замечен ли этот человек в агрессивном поведении, не задолжал ли он значительные суммы по своей кредитной карте, не обвинялся ли в магазинной краже. Поместите такую камеру снаружи здания, и вы получите автоматический замок, который закроет двери перед человеком с несоответствующей репутацией. Поскольку такого рода система не может быть идеальной, на одной чаше весов оказываются риски, которые возникнут, если ее не использовать, а на другой – судебные процессы, гражданская ответственность или просто ухудшение отношения клиентов к заведению, которые могут возникнуть в случае ошибочной идентификации. На практике можно попытаться запрограммировать компьютер таким образом, чтобы он оценивал риск по каждому конкретному покупателю.

Создание общенациональной базы данных, хранящей фотографии населения, не такая уж сложная задача, ибо большая часть этих данных уже общедоступна. В 1990-х годах в большинстве штатов стали оцифровывать фотографии с водительских удостоверений. Эти фотографии, частично уже находящиеся в общем доступе, будут все чаще продаваться частным компаниям, несмотря на то, что это запрещено законом. Процесс уже начался. В феврале 1999 года Управление общественного порядка Южной Каролины [South Carolina Public Safety Department] продало фотографии с 3,5 миллиона выданных в штате водительских удостоверений компании Image Data LLC, расположенной в Нэшуа, штат Нью-Хемпшир. Согласно опубликованной в *Washington Post* статье, стоимость сделки составила 5 тысяч долларов, или приблизительно один цент за семь фотографий.

Washington Post выступила также с разоблачением того факта, что Image Data LLC получила в 1998 году от американской Секретной службы грант в размере 1,46 миллиона долларов и техническое содействие. Компании было поручено создание общенациональной базы фотографий, которую предполагалось использовать для борьбы с мошенничествами с чеками и кредитными картами, а также для борьбы с терроризмом и верификации иммиграционного статуса.⁵²

Планы Image Data вызвали тревогу, поскольку фотографии создавали огромный потенциал для злоупотреблений. Например, если банковский программист имеет расистские убеждения, он может модифицировать программу кредитования таким образом, чтобы она учитывала цвет кожи заемщика в процессе принятия решения о выдаче кредита. Другой вариант – ошибка в компьютерной программе, особенно созданной по технологии нейронных сетей, может привести к тому, что система начнет непреднамеренно учитывать этот фактор, несмотря на то, что никто этого не планировал. Такие действия программы чрезвычайно сложно обнаружить с помощью обычных методов проверки.

Самое смешное, что есть гораздо более дешевый и простой способ использования фотографий для предотвращения мошенничества. Вместо того чтобы создавать базу данных с лицами, можно просто помещать фотографию владельца на кредитную карту и чековую книжку. Корпорация Polaroid разработала кредитную карту с фотографией еще в 1960-е

⁵² Robert O'Harrow, Jr., and Liz Leyden, «U.S. Helped Fund Photo Database of Driver IDs; Firm's Plan Seen as Way to Fight Identity Crimes», *Washington Post*, 18 февраля 1999, p. A1. Архив статьи доступен по адресу <http://wearcam.org/drivers-license-picture-sale.html>.

годы, но большинство банков воспротивилось ее использованию. Одним из аргументов было то, что, хотя фотография снижает риск мошенничества, она увеличивает стоимость карты. Другим поводом для отказа стала необходимость иметь фотографию владельца до оформления карты, что не позволяло банкам вести направленную рекламу: для оформления карты с фотографией клиенту необходимо было лично прийти в банк.

Национальная база фотографий находится в процессе создания. Но обществу необходимо обсудить, для каких целей она будет использоваться, кто будет иметь к ней доступ и каким образом будет корректироваться ошибочная информация. Было бы неправильно предоставлять частному бизнесу неограниченный доступ к этой информации без какого-либо контроля.

Биометрическое пиратство

Когда *Washington Post* опубликовала информацию о предстоящей продаже фотографий с водительских удостоверений в Южной Каролине, это вызвало взрыв негодования. Штат сразу же попытался разорвать контракт, мотивируя это нарушением права граждан. Но судья штата отклонил данный аргумент, заявив, что законодательство не запрещает такую продажу.

В результате этого и других инцидентов некоторые штаты, возможно уже в ближайшее время, примут законы, запрещающие продажу фотографий с водительских удостоверений частному бизнесу. Но гораздо труднее не допустить использования бизнесменами собственных ресурсов для создания базы данных с фотографиями. Установленные возле кассовых аппаратов видеокамеры уже сейчас фиксируют изображение каждого, кто пользуется кредитной картой. Не представляет никакой сложности совместить эту информацию с именем владельца предъявляемой карты. Эта схема настолько проста, что не заставит себя долго ждать, если только такая практика не будет запрещена законодательно.

Профессор электротехнического факультета университета Торонто Стив Ман [Steve Mann] назвал фиксацию изображения человека без его согласия *пиратством образа* [likeness piracy].⁵³ Ман доходчиво объяснил разницу между пиратством образа и нарушением авторских прав [copyright infringement]: авторское право защищает лишь произведения в фиксированной форме. Нарушение авторского права подразумевает присвоение и использование определенного изображения, в то время как пиратство образа подразумевает присвоение и использование изображения человека в принципе.

В законодательстве Соединенных Штатов и других стран вопрос пиратства образа урегулирован. Например, в штате Нью-Йорк считается преступлением использование изображения человека в рекламе без его согласия. Этот закон появился еще в начале XX века, когда торговцы начали размещать лица людей на упаковках с продуктом как форму его одобрения, не получив предварительно официального разрешения человека. Кто-то может предположить, что данный закон будет работать и в XXI веке, защищая нас от пиратства образа и биометрического пиратства. Но он будет бессилён, если политика в области биометрии будет устанавливаться на основании сложившейся в бизнесе практики.

Идентификация с использованием смарт-карт

⁵³ Steve Mann, «„Smart Clothing“: Wearable Multimedia and „Personal Imaging“ to Restore the Balance Between People and Their Intelligent Environments», *Proceedings, ACM Multimedia 1996*, 18–22 ноября 1996.



Смарт-карта, вроде изображенной на рисунке карты фирмы Gemplus, представляет собой обычную пластиковую карту с размещенным на ней тонким микрочипом. Чип может включать в себя микропроцессор и несколько килобайт памяти. Самое популярное применение смарт-карт – «электронные кошельки», когда карта используется в качестве носителя электронной наличности. Смарт-карта может быть использована и в качестве носимого банка данных, причем владелец карты не может модифицировать находящуюся на карте информацию. В приведенном примере смарт-карта используется в качестве идентификатора, содержащего оцифрованную фотографию владельца и, возможно, отпечатки пальцев. Пограничник сравнивает лицо стоящей перед ним женщины с ее фотографией, считанной со смарт-карты. Поскольку изменить записанное в карту фотоизображение гораздо сложнее, чем переклеить обычную фотографию на документе, разработчики считают такую технологию более безопасной. Хотя эта технология считается сегодня наиболее безопасной, это значит лишь, что создателей поддельной карты ждет более высокое вознаграждение. В конечном счете смарт-карта будущего окажется не более защищенной, чем кредитные карты сегодня. [Фотографии любезно предоставлены фирмой Gemplus]

Уже сегодня крупнейшая служба доставки United Parcel Service (UPS) является также и крупнейшим биометрическим пиратом. При доставке большинства отправок UPS требует, чтобы получатель расписался в качестве подтверждения получения. В 1987 году UPS начала оцифровывать изображения подписей получателей и хранить их в базе данных. Изображение могло быть отослано по факсу любому, кто позвонил в UPS по номеру 800 и запросил уведомление о вручении отправления. В 1990 году UPS усовершенствовала свою пиратскую технологию, оснастив своих курьеров портативными компьютерами, названными «устройствами для сбора информации о доставке» – DIAD [Delivery Information Acquisition Device]. Каждый компьютер оснащался встроенным считывателем штрих-кодов и специальным планшетом для подписи. Доставив отправление, курьер считывает штрих-код и предлагает получателю расписаться на планшете. Эти данные записываются в память DIAD, после чего, конечно, попадают в базы данных UPS.

Когда я обратился в компанию с жалобой на такую практику, пресс-секретарь UPS Пэт Стифен [Pat Steffen] объяснила мне, что инициатива сделать подписи доступными в электронном виде исходила от клиентов UPS. Подписи рассматривались как подтверждение доставки. Оцифровка этого подтверждения позволяла UPS работать с ними, как и с любыми другими цифровыми данными. Отправка по факсу сертификатов с подтверждением о доставке осуществляется компьютерами UPS автоматически, объяснила мне Стифен. Клиентам UPS также предоставляется возможность получить специальное программное обеспечение для отслеживания доставки и просматривать подписи непосредственно на своем персональном компьютере.⁵⁴

Самое забавное, что, сделав оцифрованную собственноручную подпись клиента широко доступной, UPS тем самым принизила ее значимость. Как только подпись оцифровывается, ее очень легко манипулировать с помощью компьютера, например поставить ее под контрактом. Система UPS особенно уязвима: вы можете отслеживать доставку отправок, зная номера накладных, которые присваиваются последовательно,

⁵⁴ Интервью автору, 25 августа 1994.

например «0930 8 164 904», «0930 8 164 913», «0930 8 164 922». Зная номер выданной в UPS квитанции, злоумышленник может использовать эту информацию для составления полного списка получателей отправок и присвоить копию подписи каждого получателя.

UPS понимает уязвимость своей системы, но не предпринимает серьезных действий по ее ликвидации. На web-сайте компании можно увидеть замечание следующего содержания:

UPS предоставляет вам возможность использовать систему отслеживания доставки только с целью контроля ваших отправок. Любое другое использование системы отслеживания и информации из нее строго запрещено.

Говоря по правде, UPS не делает практически ничего для противодействия атакам криминального характера. «Если кто-то захочет узнать номера отправок, он сможет это сделать. Если кто-то захочет сделать что-то еще, я думаю, что это ему тоже удастся. И этому сложно противостоять», – говорит Стифен. Но подобрать номер было бы сложнее, если бы UPS использовала более длинные числа для номеров накладных и не назначала их предсказуемым образом.

Финансовое сообщество нашло лучший способ внедрить биометрию в практику бизнеса. Известно, что мошенники всегда имели возможность украсть бланки чеков или напечатать свои, чтобы потом заполнить их и обналичить. Поэтому в 1997 году Sea First и множество других банков Западного побережья стали фиксировать на обратной стороне чека отпечаток большого пальца, если человек, предъявивший чек для обналичивания, не имел счета в банке. Отпечатки пальцев фиксировались с помощью специальных чернил: человек макал палец в подушечку с чернилами и ставил отпечаток на обратной стороне чека, после чего легко удалял с пальца остатки чернил. Если чек оказывался поддельным, в распоряжении Sea First оставался отпечаток пальца мошенника, причем реальный, а не хранимая в компьютере электронная копия, используя которую можно было переложить вину на другого. Поскольку SeaFirst было известно также и точное время, когда чек был предъявлен для обналичивания (оно фиксировалось на чеке и в компьютере), можно было легко получить фотографию мошенника из архивных записей системы видеонаблюдения. Поиск по отпечатку пальца мог быть также осуществлен при помощи большого количества систем AFIS. Увы, несмотря на то что данная система безупречна с технической точки зрения, ее использование имеет побочный эффект: люди, предъявляющие в банк чеки, ощущают себя неуютно, потому что с ними обращаются как с потенциальными преступниками.

Биометрия является очень мощным средством идентификации, но только для человека или компьютера, который непосредственно производит измерение. Как только биометрические данные помещаются для хранения в компьютер, вся безопасность, обеспечиваемая биометрической идентификацией, сходит на нет. Вместо измерения биометрические показатели могут быть просто скопированы из одного компьютера в другой. Эту критичную особенность биометрических систем не следует забывать. К сожалению, она настолько тонка, что очень часто не принимается во внимание людьми, разрабатывающими и использующими биометрические системы.

Идентификация тела, а не человека

Абсолютная идентификация – соблазнительная идея. Но, к сожалению, эта идея изначально порочна. Все описанные в этой главе системы идентификации обладают одним существенным недостатком: они идентифицируют не *личность*, они идентифицируют *тело*. В современном обществе юридическим субъектом является личность. Личность имеет имя, номер социального страхования и биографию. Личность покупает и продает собственность. Личность имеет обязательства. Тела же всего лишь теплокровные двуногие животные, передвигающиеся по поверхности планеты. Тела рождаются и умирают.

Когда происходит убийство, одно тело лишает жизни другое. Работа полиции заключается в установлении личностей причастных людей, т. е. идентификации жертвы и поиске преступника. В тюрьму помещается тело, но свободы лишается личность. Любой идентификационный банк данных, будь это паспорт, выданный Госдепартаментом США, или принадлежащая ФБР система CODIS, пытается установить соответствие между субъектом права (личность) и телом, в котором она обитает. Эта процедура несовершенна.

Сегодня для преступника не составляет большого труда создать себе полноценный псевдоним и получить на него водительское удостоверение, официально выданное штатом. Существует целый ряд нелегальных или полулегальных путей создания поддельной личности: для начала необходимо найти информацию о человеке, родившемся примерно в то же время, что и вы, но умершем в детском возрасте.^[p13] Далее запрашивается дубликат свидетельства о рождении и оформляется карточка социального страхования. После этого нужно начать активно использовать новое имя, например выписать на него журналы. И в какой-то момент сдать экзамен и получить водительское удостоверение.

В США не существует единого хранилища информации о рождении и смерти в масштабе страны. Города, округа и штаты ведут свои собственные архивы. Иногда информация теряется: больница может сгореть вместе с архивами, компьютерные файлы – уничтожиться. Иногда дублирование информации осуществляется, иногда нет. Некоторые архивные системы очень устарели. Отсутствие централизации информации может быть использовано знающими людьми. После присвоения личности умершего в детстве человека описанным выше способом очень сложно доказать подлог. Практически единственный случай, когда это возможно, – ситуация, когда человек ранее подвергался снятию отпечатков пальцев при аресте и эта информация хранится в базе данных, например в картотеке отпечатков пальцев полицейского управления. Но даже с помощью этой базы данных невозможно доказать, что новая личность поддельная. Все, что может быть с помощью нее доказано, – это лишь факт, что обладатель данного тела использовал когда-то другое имя.

Преступники не единственная категория, нуждающаяся в новых именах, это нужно и правительству. Создание новых личностей необходимо для внедряемых в криминальную среду полицейских, шпионов, перебежчиков и участников федеральной программы защиты свидетелей. Существование спроса со стороны правительства гарантирует, что строгая система биометрической идентификации никогда не будет создана ни в США, ни в других странах: всегда должна оставаться лазейка для внесения в поддерживаемую правительством базу данных ложной информации или изменения правильной информации по политическим мотивам.

Некоторые системы биометрической идентификации обладают еще одним недостатком: при желании их можно обмануть. В 1930-е годы некоторые гангстеры хирургически изменяли свои отпечатки пальцев путем пересадки кожи с других участков тела. Сегодня отпечатки пальцев и сетчатки глаза также могут быть удалены как по желанию человека, так и без него. Чем больше общество полагается на биометрию, тем больше риск опасности травмирования.

Вместо того чтобы полагаться на биометрию для решения социальной проблемы телесной идентификации, мы могли бы предложить социальный путь ее решения. Одним из вариантов могло бы быть ужесточение наказания за «подделку личности» при относительно слабой системе биометрической идентификации. Далее мы должны законодательно установить, что при этом ущерб наносится не только банку или учреждению, которое было непосредственно обмануто, но и человеку, чье имя при этом использовалось.

В ближайшем будущем биометрия станет неотъемлемой частью всех аспектов нашей

p13

Доступ к записям о рождении свободен, и сама просьба посмотреть регистрационные записи не будет выглядеть странной, так как в США многие люди хотят узнать свою родословную, и интерес к архиву может быть обоснован этим фактом.

жизни. Но, вследствие описанных выше недостатков и проблемы ущемления гражданских свобод, наша цивилизация вряд ли когда-нибудь создаст общество, тотально отслеживающее каждого при помощи биометрии. Вместо отслеживания каждого отдельного человека наша цивилизация все больше склоняется к более простому варианту – отслеживанию событий. Этому аспекту посвящена следующая глава.

4

Что вы делали сегодня?

В юношеские годы я начинал вести дневник. Каждый вечер, перед тем как отправиться спать, я брал ручку и подробно записывал события прошедшего дня. Как раз в это время я начал встречаться с девушками, и вскоре страницы моего блокнота были заполнены моими романтическими историями: я писал, кто мне нравился, а кто нет, с кем я встретился в школе, с кем говорил по телефону. И конечно, я записывал подробности самих свиданий: с кем мы были, куда ходили, что ели и что делали.

Приблизительно через месяц у меня получилась довольно внушительная летопись моих отроческих подвигов. Но со временем записи в дневнике становились все короче и короче, требовалось слишком много усилий, чтобы описывать все подробно. В конечном счете мой проект зачах под весом своих собственных данных.

В современном мире вести подобный дневник гораздо легче. Каждый раз, когда я покупаю что-нибудь по кредитной карте, я получаю маленький желтый слип, ^[p14] который напомним мне точное время и место покупки. Еще более детальный отчет о покупках я получаю в ближайшем супермаркете: там указывается название и количество всего, что я приобрел по своей карте. В моей карточке часто летающего пассажира указан каждый город, в который я совершал полет в течение последнего года. Если вдруг я случайно выброшу карточку, то с информацией ничего не произойдет – вся она аккуратно хранится в многочисленных банках данных.

Даже информация о моих телефонных звонках тщательно записывается, распечатывается и предоставляется мне в конце каждого месяца. Помню, когда я еще учился в колледже, моя подружка решила порвать со мной во время междугородного разговора. Мы говорили 20 минут, а затем она повесила трубку. Я звонил ей снова и снова, но каждый раз натывался на автоответчик. Через несколько недель мне пришел счет с распечаткой звонков: один разговор длительностью 20 минут, а за ним через короткие промежутки еще пять звонков по 15 секунд.

Но самое большое количество информации о моей жизни хранит жесткий диск моего компьютера: архив электронных писем начиная с младших курсов колледжа. Он занимает более 600 мегабайт, что составляет примерно 315 тысяч страниц текста, напечатанного через два интервала, или по 40 страниц каждый день начиная с 3 сентября 1983 года, когда я получил свой первый электронный почтовый ящик в MIT.

«Сохраняй все свои старые электронные письма, – сказал мне мой друг Гарольд перед самым выпуском. – Когда в будущем историки захотят написать о 80-х годах XX века, мы будем одними из тех, кто попадет в историю». И он был прав: с помощью поиска по ключевым словам и современных систем обработки текстов какому-нибудь историку в будущем будет достаточно просто воссоздать очень точную картину моей жизни начиная со студенческих лет путем анализа оставленных мною электронных записей.

Но этот архив фактов и впечатлений – обоюдоострый клинок. Кроме моего собственного дневника, я оставил великое множество «информационных теней» [data

p14

Чек, получаемый путем «прокатывания» рельефной кредитной карты через импринтер. Один экземпляр выдается покупателю, один остается у продавца, а третий предъявляется продавцом в банк для оплаты.

shadow], которые могут поведать секреты моей повседневной жизни любому, кто сможет эти тени прочесть.

Термин «информационная тень» предложил в 1960-е годы Алан Уэстин. Профессор Колумбийского университета в Нью-Йорке, Уэстин предупреждал, что записи о кредитах, банковские и страховые записи, а также другая информация, наполняющая электронную инфраструктуру Америки, могут быть легко скомбинированы для создания подробнейших электронных досье. Эта зловещая метафора удивительно точна: очень малое количество людей обращают внимание на то, куда падает их тень, и очень немногие в будущем смогут контролировать свои электронные досье, предполагал Уэстин.

Прошло три десятилетия, и информационные тени переросли из академического предположения в объективную реальность, касающуюся каждого из нас.

Мы стоим на границе информационного кризиса. Никогда ранее такое огромное количество информации о таком количестве людей не собиралось в таком количестве различных мест. Никогда раньше такое огромное количество информации не было так легко доступно такому количеству учреждений таким количеством способов и для такого количества различных целей.

В отличие от электронной почты, которую я храню в моем портативном компьютере, моя информационная тень вышла из-под моего контроля. Распыленные по компьютерам тысяч разных компаний, мои информационные тени стоят по стойке «смирно» плечом к плечу с другими тенями в банках данных корпораций и правительств по всему миру. Эти тени делают выявление человеческих секретов обычным занятием. Эти тени заставляют нас соответствовать новому стандарту ответственности. А поскольку информация, отбрасывающая эти тени, может случайно оказаться некорректной, они делают всех нас уязвимыми против наказания или воздаяния за действия, которых мы никогда не совершали.

Но есть и хорошая новость: мы можем бороться против этого глобального вторжения в частную жизнь. Мы можем бороться за прекращение фиксации всех ежедневных событий. А там, где такая фиксация необходима, мы должны установить соответствующую деловую практику и принять законы, которые будут гарантировать неприкосновенность нашей частной жизни – защиту для живущих рядом с нами информационных теней. Мы уже делали это ранее. Все, что необходимо людям, – это понять, как и где эта информация записывается и как нам это остановить.

Информационный кризис

В качестве эксперимента попробуйте составить список информационных следов, которые вы оставляете ежедневно. Рассчитались за ланч кредитной картой? Запишите. Платили за ланч наличными, но перед этим получили их в банкомате? Если да, то это снятие денег также оставляет еще одну информационную тень. Каждый междугородный звонок, каждое оставленное на автоответчике сообщение и каждый посещенный в Интернете web-сайт – все это части вашего подробнейшего досье.

Вы оставляете больше следов, если живете в городе, пользуетесь кредитной картой и если ваша работа связана с использованием телефона или компьютера. Вы будете оставлять меньше следов, если живете в сельской местности или небогаты. В этом нет ничего странного: именно накопление подробной информации сделало возможным современное развитие экономики.

Удивительно другое – объем косвенной информации, которую можно получить по этим записям. Каждый раз, когда вы снимаете деньги в банкомате, компьютер записывает не просто количество снятых денег, но сам факт вашего нахождения в конкретном месте в конкретное время. Позвоните на номер, оборудованный автоматическим определителем (АОН), и маленькая коробочка запишет не просто ваш номер (и, возможно, имя), но и точное время, когда вы сделали свой звонок. Попутешествуйте в Интернете, и web-сервер по другую сторону дисплея не просто отметит, какие страницы вы просмотрели, но и скорость вашего

модема, тип использованного браузера и даже ваше географическое местоположение.

Между тем мы не сделали страшного открытия. Еще в 1986 году Джон Дайболд [John Diebold] писал об одном банке, который:

...установил сеть банкоматов и сделал интересное наблюдение, «что необычное количество снятий денег производится каждую ночь между полуночью и 2 часами»... Заподозрив неладное, банк нанял детективов для установления истины. Выяснилось, что большинство припозднившихся клиентов снимали наличные деньги, направляясь в местный квартал красных фонарей!⁵⁵

В появившейся в *Knight News Service* после инцидента статье говорилось: «Кое-где в Америке существуют банки, которые знают, кто из клиентов платил сутенеру прошедшей ночью».⁵⁶ (Дайболд, один из компьютерных пионеров 1960-х – 1970-х годов, сначала был сторонником создания Национального информационного центра. Но к 1986 году он стал считать, что идея построения центра была огромной ошибкой, так как приводила к слишком большой концентрации информации в одном месте.)

Я называю записи, подобные архивам банкоматов, «горячими файлами» [hot files]. Они очень интересны, они могут раскрыть совершенно неожиданную информацию и находятся за пределами понимания большинства людей.

Последние 15 лет мы наблюдаем все более широкое использование этой информации. Один из ранних случаев, который я помню, произошел в 1980-е годы. Тогда американское Управление по борьбе с наркотиками [Drug Enforcement Agency, DEA] начало сопоставлять данные из садоводческих магазинов с информацией из электрических компаний. Проект назывался «Операция „Зеленый торговец“». К 1993 году DEA в сотрудничестве с местными правоохранительными органами предотвратило более 4 тысяч готовящихся операций, арестовало более полутора тысяч нарушителей и заморозило миллионы долларов капиталов в виде незаконной прибыли и имущества.⁵⁷ Однако программа подверглась критике, ее называли облавой, жертвами которой стали не только преступники, но и невинные граждане. Сыщики искали людей, тайно выращивающих марихуану. Но вместе с некоторым количеством наркофермеров пострадали и несколько невинных садовников, включая жившего по соседству с редактором газеты *New York Times*. *Times* даже опубликовала передовицу на эту тему, но это не остановило деятельность DEA.

Американцы получили и другую порцию сюрпризов в конце 1987 года, когда президент Рональд Рейган выдвинул на пост Верховного судьи США Роберта Борка [Robert Bork]. Выдвижению Борка отчаянно воспротивилась группа женщин, заявлявшая, что Борк замечен в дискриминации женщин; они опасались, что Борк может оказать давление в решении вопроса о запрете аборт. В поисках компромата журналист из либеральной газеты *City Paper* из Вашингтона, федеральный округ Колумбия, получил распечатку названий видеофильмов, которые Борк брал напрокат в ближайшей видеотеке. Журналист надеялся обличить Борка в пристрастии к порнографии, но его вкусы оказались совсем другими: из 146 взятых им напрокат фильмов большинство оказались диснеевскими мультфильмами и фильмами Хичкока.

Тем не менее репутация Борка была несколько подпорчена. Некоторые публикации о

⁵⁵ James Finn and Leonard R. Sussman, eds., *Today's American: How Free?* (New York: Freedom House, 1986), p. 111.

⁵⁶ Ibid.

⁵⁷ U.S. Department of Justice Drug Enforcement Administration, «U.S. Drug Threat Assessment: 1993. Drug Intelligence Report. Availability, Price, Purity, Use, and Trafficking of Drugs in the United States», сентябрь 1993, DEA-93042. Доступно в Интернете по адресу <http://mir.drugtext.org/druglibrary/schaffer/GOVPUBS/usdta.htm>.

Борке и множество отпускаемых на приемах бесцеремонных замечаний игнорировали тот факт, что журналист остался с пустыми руками в своих поисках порнографии. Вместо этого формировалось мнение, что Борк увлекается порнографией, или, по крайней мере, читателя подталкивали к такому выводу.

Проблема горячих файлов состоит в том, что они слишком горячие: с одной стороны, они открывают такую информацию о нас, которую большинство людей предпочитают не оглашать в приличном обществе; с другой стороны, находящуюся в них информацию легко неправильно интерпретировать. Более того, эта информация может быть и сфальсифицирована: если бы служащий видеотеки захотел, он мог бы добавить в регистрационные записи Борка пару дюжин порнографических киношек, и никто бы никогда не смог доказать, что запись фальшивая.

В нашем обществе превалируют компьютеризованные системы записи и хранения информации, и мы вскоре будем наблюдать все большее число случаев, когда информация, собираемая такими системами для одной цели, будет использована совсем для другой. Развитие современных технологий делает этот сценарий все более реалистичным. Раньше компьютеры просто не могли хранить всю доступную им информацию: системы проектировались так, чтобы периодически стирать данные, которые им больше не нужны. Но современный уровень развития технологий хранения информации достиг таких высот, что данные можно хранить месяцы и даже годы после того, как они больше не нужны для текущей работы. В результате сегодня компьютеры могут хранить гораздо более полное досье на каждого из нас, как это произошло с записями судьи Борка в видеотеке. Попробуйте найти ответ на вопрос: с какой целью в видеотеке хранились записи о фильмах, которые Борк брал напрокат, после того, как они были возвращены?

Этот океан информации создает новый стандарт подконтрольности в нашем обществе. Вместо доверия людям и презумпции невиновности мы просто сверяемся с записями и видим, кто плохой, а кто хороший. Высокая доступность персональной информации облегчает также жизнь преступникам, бродягам, шантажистам, провокаторам и другим «плохим парням». Одним из наиболее драматичных случаев стало убийство актрисы Ребекки Шефер [Rebecca Schaefer] в 1989 году. Шефер прилагала достаточно много усилий для сохранения своей приватности. Но один помешанный 19-летний поклонник, мечтавший встретиться с ней, нанял частного детектива, чтобы тот нашел домашний адрес его кумира. Детектив обратился в калифорнийское Управление по регистрации транспортных средств [Department of Motor Vehicles], которое в то время предоставляло регистрационную информацию любому желающему, так как она являлась общедоступной. После этого фанат проник в дом Шефер, прождал ее четыре часа и выстрелил ей в грудь, как только она открыла входную дверь.⁵⁸

Синдром фальшивых данных

Еще одна коварная проблема с океаном информации – это то, что я называю «синдром фальшивых данных» [false data syndrom]. Поскольку большинство данных в этом океане информации корректно, мы все предрасположены верить, что они корректны полностью – опасное заблуждение, которому легко подвергаются все. Это заблуждение поддерживают поставщики информации, скрывая недостатки своих систем.

Например, в 1997 году телефонная компания NYNEX (входящая теперь в Bell Atlantic) запустила агрессивную рекламную кампанию по продаже услуги определения номера звонящего абонента своим клиентам. Реклама подзаголовком «Узнайте, кто вам звонит, не поднимая трубки» гласила:

⁵⁸ «TV-Movie Actress Slain in Apartment,» Associated Press, 19 июля 1989. «Arizona Holds man in Killing of Actress», Associated Press, 20 июля 1989. «Suspect in Slaying Paid to Find Actress», Associated Press, 23 июля 1989.

Определитель номера позволяет вам узнать *имя* и *номер* вызывающего абонента, что дает вам возможность принять решение: ответить на звонок сейчас или перезвонить позже. Даже если звонивший не оставил сообщения, ваш определитель номера автоматически запишет имя звонившего, номер телефона и время звонка. Определитель также работает в режиме ожидания вызова, поэтому вы можете узнать, кто вам звонит *даже во время разговора с кем-то другим*.⁵⁹

Конечно, NYNEX подменила понятие идентификации личности идентификацией телефонного номера. Определитель показывает не номер телефона, принадлежащий звонившему, а номер, с которого он звонил. Так называемый «расширенный» определитель, высвечивающий имя и номер телефона, на самом деле показывает не имя звонящего, а имя человека, на которого этот номер записан в телефонном справочнике. Если я сделаю непристойный звонок, находясь у вас в гостях на вечеринке, или воспользуюсь им для угроз жизни президента США (государственное преступление), то определитель скажет, что преступник – вы, а не я.

Отслеживаем процесс: Как наша информация может быть обращена против нас

Никто не собирается создавать общество, в котором все незначительные подробности повседневной жизни постоянно записываются для будущих поколений. Но это будущее, к которому мы уверенно движемся благодаря целому ряду социальных, экономических и технологических факторов.

Человеку свойственна склонность к собирательству. Психологически гораздо проще оставить что-то, чем выбросить. Это в полной мере относится и к информации. Никто не чувствует себя комфортно, уничтожая деловую корреспонденцию или стирая старые данные: мы никогда не знаем, когда что-то может понадобиться. Современные технологии позволяют воплотить нашу коллективную мечту никогда ничего не выбрасывать, по крайней мере информацию.

Первый компьютер, который я купил в 1978 году, хранил информацию на магнитофонных кассетах. Я мог поместить 200 килобайт информации на 30-минутную кассету, и я был счастлив. Компьютер, которым я пользуюсь сейчас, имеет внутренний жесткий диск, который может хранить 6 гигабайт информации.

И это увеличение емкости в 30 тысяч раз произошло всего за два десятилетия. И эта история едва ли уникальна: повсюду в мире бизнесмены, правительства и частные лица ощутили рост своих возможностей по хранению данных. Как цивилизация, мы используем эту новую возможность для хранения все большего количества незначительных подробностей нашего будничного существования. Мы построили мировую *инфосферу* [datasphere]^[p15] – массив информации, описывающей Землю и наши действия на ней.

Построение мировой инфосферы – трехшаговый процесс, которому мы уже слепо следуем, не принимая во внимание его влияние на будущее приватности. Сначала индустриальное общество создало новые возможности для хранения данных. Затем мы чрезвычайно упростили автоматическую запись информации в компьютеры. Последний шаг – упорядочение этой информации в глобальной базе данных, из которой она может быть легко получена при необходимости в любой момент.

Поскольку ежедневные события, происходящие в нашей жизни, систематически записываются в машиночитаемой форме, эта информация начинает жить сама по себе. Для

⁵⁹ Реклама NYNEX, разосланная клиентам весной 1997 года.

нее находятся новые применения. Если мы не сделаем шаг назад и не остановим сбор и выпуск данной информации, то вскоре получим мир, в котором каждое мгновение и каждое наше действие постоянно «берутся на карандаш».

Шаг 1: делаем информацию собираемой

Первый шаг на пути построения глобальной инфосферы – создание хорошей системы сбора информации. Представим лес: сами по себе деревья не несут информации. Но если мы пройдем по лесу, пронумеруем деревья, установим их возраст и высоту, запишем точное местоположение, то создадим набор данных, представляющих интерес как для специалистов по окружающей среде, так и для деревообрабатывающей промышленности.

Первую наглядную иллюстрацию описанного шага я получил в 1988 году во время посещения расположенного рядом с Бостоном завода BASF по производству флoppi-дисков. Я узнал, что в процессе изготовления каждый диск маркируется специальным кодом – *номером лота*. Возьмите любую дискету, и вы, скорее всего, увидите на обратной стороне эти коды: A2C5114B, S2078274 или 01S1406. Эти коды идентифицируют производителя диска, завод, конкретный аппарат, на котором диск был сделан, дату и время начала производства этого лота. Иногда информация кодируется непосредственно в виде чисел, иногда это просто ссылка на запись в учетной книге или системе контроля качества. В любом случае, для декодирования номера лота необходимо обладать специальной информацией, которой производители редко делятся с общественностью.

Изначальная цель нанесения этих кодов заключалась в облегчении процесса контроля качества. При обнаружении дефектного диска производитель по номеру лота может легко определить его происхождение. Просмотрев учетные записи на заводе, инженер по контролю качества может очень точно выявить оборудование, вызвавшее проблему, что является первым шагом по предотвращению брака в дальнейшем. В конечном счете это сберегает деньги фирмы и ее репутацию.

Как только вы узнаете, как распознавать номера лотов, вы вскоре начнете замечать их повсюду: на обертках конфет, бутылочках с лекарствами, крышке фонарика. Некоторые объекты настолько важны, что каждый из них получает свой уникальный номер, который в этом случае называется *серийным номером*. Переверните мышку, присоединенную к вашему компьютеру, и вы найдете на ней такой номер. Другой серийный номер нанесен на сам компьютер, а также на большое число отдельных компонентов внутри него. Все это несколько забавно. На заре индустриальной революции одной из самых сложных технических проблем, с которой столкнулись инженеры, было производство функционально идентичных, взаимозаменяемых частей. Сегодня мы настолько хорошо научились делать вещи неотличимыми друг от друга, что должны наносить на каждую уникальный код, чтобы различать их.

Номера лотов и серийные номера служат одной фундаментальной цели: делая похожие вещи отличимыми друг от друга, номера позволяют фиксировать историю каждой вещи. Однажды нанесенные, эти номера могут быть использованы не только для простого контроля качества: серийные номера и номера лотов все шире используются в деятельности правоохранительных органов.

Номера лотов являются безусловным доказательством, например, при расследовании случаев подделки товаров. Если поддельные продукты в разных магазинах принадлежат к одному лоту, скорее всего, «левая» партия была выпущена прямо на предприятии. Если же они все из разных лотов, т. е. как бы произведены на разных фабриках, то почти очевидно, что подделка имела место прямо в магазине или кустарным способом.

Одним из самых удачных примеров маркировки является идентификационный номер транспортного средства [Vehicle Identification Number, VIN], – 17-символьный код, наносимый на приборную панель, двигатель и мост каждого выпускаемого в мире автомобиля. Как рассказал Томас Кар [Thomas Carr], менеджер по обеспечению

безопасности пассажиров Американской ассоциации производителей автотранспорта [American Automobile Manufacturer's Association], VIN был создан в 1970-е годы коалицией производителей автомобилей и правительствами, стремящимися к международной стандартизации.⁶⁰ Первые 16 символов VIN несут информацию о производителе, стране изготовления, марке и модели автомобиля, заводе, где происходила сборка, годе выпуска, ограничениях для этого автомобиля, типе трансмиссии и используемом заднем мосте для грузовиков, а также 6-значный последовательный код.

Последний символ VIN имеет специальное значение. Это так называемая контрольная цифра. Сам по себе он не несет никакой информации, а рассчитывается из остальных символов. Эта цифра дает возможность верифицировать VIN лишь по нему самому, позволяя компьютеру автоматически определять большое число опечаток, таких как случайная перемена символов местами или нажатие смежной клавиши на клавиатуре компьютера. Поскольку VIN является своеобразным ключом, используемым для поиска информации по конкретному автомобилю, чрезвычайно важно, чтобы он был напечатан правильно, объясняет Кар.

VIN используется для отслеживания автомобиля в течение всего процесса производства. После того как автомобиль покидает завод, VIN используется правительством для отслеживания того, кто им владеет, как с целью сбора налогов, так и для помощи в розыске и возвращении законному владельцу угнанного автомобиля. А в последние годы VIN стал выполнять еще одну важную функцию – идентификации автомобиля после взрыва. После взрывов во Всемирном торговом центре в Нью-Йорке^[p16] и федеральном здании Murrah в Оклахома-Сити следствию в обоих случаях удалось достаточно быстро найти мосты грузовиков, использованных в преступлении. Нанесенный на мосты VIN позволил установить владельцев машин, что, в свою очередь, позволило найти, кто их арендовал, и выйти, таким образом, на самих подрывников.

Шаг 2: делаем информацию машиночитаемой

Автоматический сбор данных – второй большой шаг, необходимый для создания инфосферы. Автоматизированные системы считывают порции информации и помещают их непосредственно в компьютер, без участия человека. Несмотря на то что автоматизированные системы могут быть достаточно дороги в установке, их функционирование приводит к существенному удешевлению процесса сбора данных, предоставляет возможность создавать огромные массивы информации и поддерживать их в актуальном состоянии. В конечном счете, когда основные игроки рынка начнут переходить на использование автоматизированных систем, остальные сразу же последуют за ними.

PSN корпорации Intel

Фирма Intel неожиданно внедрила серийные номера процессоров [Processor Serial Number, PSN] в микропроцессорах Pentium III.

Изначально эти номера были разработаны для идентификации «разогнанных» процессоров (т. е. когда процессор с тактовой частотой 500 мегагерц продавался как 600-мегагерцовый чип) и для облегчения отслеживания перемещения компьютеров в крупных организациях. Когда высшее руководство узнало об этой возможности, PSN были преподнесены как решение для электронной коммерции: Intel предложила web-сайтам

⁶⁰ Интервью автору, 9 сентября 1997.

p16

Речь идет не об 11 сентября 2001 года, а о более раннем случае.

использовать специальное программное обеспечение для считывания PSN клиентских компьютеров через Интернет.

Когда в январе 1999 года PSN были анонсированы, Intel сделала акцент на их применимости в электронной коммерции, а не как средства активного слежения. Буквально через неделю несколько групп пользователей организовали бойкот микропроцессора, справедливо предположив, что, скорее всего, PSN будут применяться для отслеживания перемещений пользователей по сайтам Интернета. Тем временем известный эксперт в области криптографии Брюс Шнайер [Bruce Schneier] опубликовал разгромную статью, в которой подверг PSN резкой критике, так как не существовало безопасного способа считывания этих номеров. Он писал:

Когда web-сервер запрашивает идентификатор процессора, он не может узнать, является ли полученное в ответ число истинным или поддельным. Аналогично, когда какая-нибудь программа запрашивает PSN, она не может достоверно знать, действительно ли ей возвращен реальный идентификатор или специальным образом модифицированная операционная система перехватила вызов и вернула поддельное число. Поскольку Intel не озаботилась параллельным созданием безопасного способа считывания идентификатора, безопасность нарушить очень легко.⁶¹

Американская банковская система, в числе крупнейших секторов экономики, одной из первых перешла на использование машиночитаемых кодов. В 1963 году некоторые банки начали печатать чеки с использованием специальных магнитных чернил, что позволило компьютерам автоматически считывать 9-значный код банка, номера счетов и номера чеков, отпечатанные внизу каждого чека. Это была замечательная идея: к 1969 году 90 % чеков в США печатались блестящими черными цифрами, существенно снижая время, необходимое на их обработку.⁶² В 1970-е годы банковская индустрия стала помещать на кредитные карты магнитную полосу, что позволяло считывать информацию проводя картой по считывателю. До этого информация с карты вводилась в компьютер вручную, потом переводилась на слип с использованием копировальной бумаги и ролика.

Другие отрасли гораздо медленнее двигались в сторону автоматически считывающих информацию систем. Только в середине 1990-х годов General Motors стала дополнительно наносить на таблички с VIN-кодами машиночитаемый штрих-код. В отличие от старого способа, когда VIN мог быть прочитан только человеком, штрих-код мог считываться высокопроизводительным лазерным сканером с расстояния более шести метров. Быстро появились сторонники нанесения штрих-кодов на VIN.

Одним из первых новинкой воспользовалось агентство по прокату автомобилей Avis, начавшее применять лазерные сканеры для автоматической идентификации автомобилей по возвращении их на стоянку. В ближайшие годы машиночитаемый VIN будет иметь все большее значение. Например, городские парковки могут использовать штрих-коды для автоматического открывания ворот постоянным клиентам. Другие компании уже разработали системы технического зрения, которые могут считывать номер стоящего или движущегося автомобиля, и работают над созданием системы, которая могла бы идентифицировать автомобиль на расстоянии.

Считыватель номеров автомобилей

⁶¹ Bruce Schneier, «Why Intel's ID Tracker Won't Work», *ZDNet News*, 26 января 1999. Повторно опубликовано в списке рассылки RISK Digest 20:19. Доступно в Интернете по адресу <http://catless.ncl.ac.uk/Risks/20.19.html#subj4>.

⁶² Westin, *Databanks in a Free Society*, p. 93.

Электронные метки служат не только для опознавания машин на открытой дороге. Американская таможня установила считыватели номеров автомобилей на большинстве пограничных пунктов между США и Канадой. Используемая в этих системах видеокамера высокого разрешения позволяет обнаружить и считать номер машины в течение нескольких миллисекунд. Изображенный на рисунке считыватель фирмы Perceptics определяет как сам номер, так и выдавший его штат или округ. В компании говорят: «С нашим считывателем любая магистраль становится открытой книгой». [Фотография любезно предоставлена фирмой Perceptics]



Новейшие машиночитаемые метки используются не магнитными или оптическими системами, а сканируются при помощи радиоволн. Эта технология называется RFID (Radio Frequency Identification Device – радиочастотные идентификационные устройства) и состоит из двух частей: крошечного кремниевого чипа с маленькой антенной, называемого *меткой*, и *считывателя* в форме пистолета. Каждый чип выпускается с уникальным кодом. Достаточно навести считыватель на чип, и на экране высветится соответствующий код. Код передается в присоединенный к считывателю компьютер. Чип не имеет движущихся частей, не нуждается в источниках питания и имеет неограниченный срок службы.

Когда вы направляете считыватель на транспондер и нажимаете на кнопку, устройство начинает излучать в сторону чипа радиоволны определенной частоты. Энергия этих радиоволн улавливается антенной транспондера и питает микрочип транспондера со встроенным в него миниатюрным радиопередатчиком. Транспондер в ответ посылает уникальный код чипа (в современных чипах используется 64-битный код) на другой частоте.

Радиочастотные идентификационные устройства (RFID)



Системы на основе радиочастотных идентификационных устройств позволяют встраивать машиночитаемые серийные номера в автомобили и газовые баллоны, вживлять в тело домашних животных и даже в человеческое тело. В основе системы лежит электронная метка, активируемая слабым радиосигналом, под воздействием которого метка начинает передавать серийный номер. RFID-метки выпускаются различными компаниями, некоторые теги могут читаться с расстояния в несколько футов. Они используются в качестве идентификаторов для лыжников, в качестве идентификационных табличек сотрудников и для отслеживания перемещения животных. Похожая технология используется на большинстве магистралей в автоматизированных системах оплаты. Поскольку система

пассивна и ничем себя не выдает, информация может быть прочитана незаметно (и без предварительного решения) человека, несущего радиометку.

Как и другие системы идентификации, RFID-системы на самом деле идентифицируют не машину, домашнее животное или человека, они лишь идентифицируют метку. Поскольку в современных RFID-системах не используются криптографические методы защиты, передаваемые идентификационные коды могут быть перехвачены, фальсифицированы или подделаны как-то еще.^[p17] Метка может быть прочитана незаметно для ее владельца. Так как современные метки не имеют внутренней памяти, то определить, сколько раз метка была считана, может лишь тот, кто ее читает, но не владелец. Похоже, ни производители этих систем, ни их пользователи не беспокоятся о недостаточном уровне безопасности, который они предоставляют. [Фотографии любезно предоставлены фирмой Trovan]

RFID-системы выпускаются несколькими компаниями. Одна из крупнейших называется Trovan и располагается в Великобритании. Самое крупное из выпускаемых Trovan устройств имеет размер около 7 см и может читаться с расстояния примерно 60 см; а самое маленькое имеет размеры рисового зерна. Эта метка читается примерно с полуметра, она разработана для вшивания под подкладку одежды для упрощения инвентаризации. Trovan производит также специальные имплантируемые метки, которые выпускаются в стерильных, готовых к применению одноразовых шприцах, позволяющих поместить метку под кожу животного менее чем за 20 секунд.⁶³

Дилеры фирмы Yamaha в Великобритании используют устройства Trovan для борьбы с хищениями мотоциклов. За 65 фунтов стерлингов (около 100 долларов США) вы можете установить чипы Trovan в раму мотоцикла, колеса, топливный бак и сиденье. Если мотоцикл будет похищен целиком или по частям, то любая часть может быть идентифицирована, когда кто-нибудь попытается ее продать.

В США RFID-системы применяются для *активного менеджмента* – техники управления бизнесом, которая позволяет снизить затраты путем тщательного учета использования приобретенных вещей. Одно из применений – отслеживание газовых баллонов. В горле баллона сверлится небольшое отверстие, и в него помещается RFID-устройство, в результате чего появляется возможность очень точно отслеживать перемещения каждого баллона между заводом и клиентами. Другие компании встраивают RFID-устройства в ручной инструмент, который каждый рабочий должен получать и сдавать обратно, как книги в библиотеке.

Тем временем имплантируемые метки начали использоваться в зоопарках для маркировки экзотических животных. В Северной Америке их используют и для маркировки домашних животных: к лету 1997 года как минимум 200 тысячам американских кошек и собак были имплантированы RFID-чипы. Несколько компаний поддерживают

p17

Работы в этом направлении уже ведутся. Современная микроэлектроника позволяет реализовать в микрочипе криптографический алгоритм «трехшагового рукопожатия», исключающий возможность фальсификации ответа.

⁶³ Аналогичные системы предлагаются компаниями: American Veterinary Identification Devices (AVID), которая поддерживает сеть «PETtrac recovery»; HomeAgain, продающей чипы Destron, InfoPet Systems, продающей системы Trovan, и PetNet, продающей чипы Anitech. Уже три года ветеринары и защитники домашних животных продолжают спорить, какой чип лучше, какой дешевле, какой легче читается и т. д. Компании отвечают на это попытками сконструировать считыватели, которые умеют читать все виды чипов, бесплатно передают считыватели приютам (в надежде на увеличение продаж чипов), буквально наступая друг другу на пятки. Промышленные приложения оставили системы «чипирования» животных далеко позади. Например, Trovan продает усиленную версию микротранспондера ID 100 под названием ID 103. Эта модель специально разработана для промышленных приложений и швейной промышленности. Оболочка имеет стеклянные стенки двойной толщины, выдерживающие воздействие валков и гладильного пресса. Чип выдерживает температуру до 180 °C. Он может быть вплавлен в пластмассовые детали, становясь неотъемлемой частью предмета.

общенациональную базу данных, в которой для каждого идентификатора чипа записаны имя владельца животного, его адрес и телефон. Организации вроде Американского общества защиты животных [The American Society for the Prevention of Cruelty to Animals, ASPCA] в Нью-Йорке, в графстве Сан-Диего в Калифорнии, в Миннеаполисе и Сент-Поле приобретают считыватели. Теперь обнаруженные на улице беспризорные животные перед отправкой в приют проходят сканирование.

Как показывают эти факты, преимущество технологии RFID в том, что, как только радиометка имплантируется в объект, она становится частью этого объекта. Серийные номера на оружии могут быть перебиты или просто вытравлены кислотой. Коды VIN могут быть удалены с автомобиля. Татуировка может зарости волосами или просто быть прикрыта одеждой. Но поместите чип вовнутрь и получите серийный номер – невидимый, нестираемый, определяемый на расстоянии.

Несмотря на то что очевидной мотивацией для маркировки и отслеживания было предотвращение потерь, вскоре появились на свет и другие преимущества повышенного контроля. Американские фермеры обнаружили, что, как только каждое животное получает серийный номер, появляется возможность хранить очень точные долговременные записи. Отслеживая животное от рождения до забоя, сохраняя подробные записи о вакцинации, кормлении, весе, содержании и даже проводимом иногда ультразвуковым сканировании, фермеры могут использовать научно обоснованные методики управления во всех аспектах своей деятельности

В конечном счете эта дополнительная работа может увеличить рыночную стоимость животного приблизительно с 700 до 1000 долларов. Тем временем американское министерство сельского хозяйства собирается в скором времени ввести обязательную электронную маркировку рогатого скота для борьбы с болезнями.⁶⁴

Шаг 3: строим большую базу данных

Внедрившие метки американские фермеры извлекли из этого полезный урок: хорошая база данных – это именно то, что отличает неорганизованную «свалку» данных от упорядоченной информации. Но сама организация базы данных и установление политики доступа к содержащейся в ней информации могут самым серьезным образом повлиять на обеспечение приватности всего предприятия с отслеживанием.

Рассмотрим электронную систему сбора дорожных платежей [Electronic Toll Collection, ETC]. В последние десять лет системы, позволяющие водителям автомобилей вносить плату за проезд по магистралям и мостам, с энтузиазмом воспринимаются во всем мире. И это закономерно: системы ETC положили конец скоплениям транспорта. Теперь водителям не нужно останавливаться, чтобы опустить несколько монеток в приемник или отдать деньги кассиру, вместо этого большинство ETC-систем используют радиометки, уникально идентифицирующие каждую машину и счет, с которого автоматически снимется соответствующая сумма.

В 1988 году фирма Micro Design ASA оборудовала одной из первых систем магистраль в Норвегии на севере от Тронхейма. Технология быстро развивалась. Сегодня системы, производимые шведской фирмой Saab Combitech, могут считать содержимое электронной метки менее чем за 10 миллисекунд при скорости машины более 160 км/час. Система Saab также определяет скорость автомобиля путем измерения доплеровского смещения отраженного радиосигнала.

В 1994 году Triborough Bridge and Tunnel Authority (TBTA), Нью-Йорк, установила ETC-систему под названием E-ZPass на пунктах оплаты проезда через мост Верразано. После

⁶⁴ Murphy, Kate, «Get Along Little Dogie #384-591E: Laptop Cowboys Riding Herd on the Electronic Frontier», *New York Times*, понедельник, 21 июля 1997.

некоторых ограничений, имевших место вначале, E-ZPass вскоре выполнила свое предназначение, увеличив пропускную способность каждого направления с 250 до 1000 автомобилей в час. Общественность восприняла это с энтузиазмом – в течение первых двух лет ТВТА выпустила более 550 тысяч меток E-ZPass.

«Каждый рабочий день мы получаем 280 тысяч платежей за проезд в электронном виде, что составляет 42 % всех транзакций», – писал Майкл Эйчер [Michael Ascher], президент ТВТА в отраслевом сборнике в марте 1997 года.⁶⁵ Подобная система – E-Pass также была с энтузиазмом принята водителями Флориды на дороге Orlando – Orange County Expressway.

Для администраций местных и федеральных магистралей главными вопросами являются стоимость, надежность и взаимодействие ЕТС-систем. Во многих штатах внедрены системы, использующие несовместимые метки: в E-ZPass используются метки, монтируемые на ветровом стекле, в то время как E-Pass во Флориде использует радиотранспондеры размером с фонарик, монтируемые под передним бампером автомобиля. Администрации магистралей надеются, что в течение нескольких лет Соединенные Штаты примут единую общенациональную систему, которая позволит оплачивать проезд по всем мостам и магистралям от Калифорнии до Нью-Йорка с помощью электроники.

Но администрации не уделяют должного внимания проблеме влияния внедряемых систем на обеспечение приватности. А влияние это существенно. Системы ЕТС хранят подробную информацию о том, какой автомобиль и в какое время вносил плату за проезд. Официально системы ЕТС хранят информацию, чтобы ежемесячно высылать водителям подробный отчет о сделанных ими платежах. Но эта база данных просто кладезь персональной информации, которая используется далеко не только для банальной отчетности. Рестораны могли бы сканировать ее для составления списка тех, кто проезжает мимо них. Частные детективы могут использовать эту информацию для отслеживания перемещения неверных супругов. Репортеры могут следить за знаменитостями, а преступники использовать ее для поиска жертв.

Поскольку штаты накапливают столь большой объем информации о перемещениях, рано или поздно она будет использована не по назначению. Нуждающиеся в деньгах правительства штатов уже продают свои базы данных водительских удостоверений компаниям вроде R. L. Polk, которые используют эту информацию для составления списков по рассылке рекламы.⁶⁶ Но даже если информация не продается, сам факт ее существования означает, что рано или поздно какой-нибудь плохой парень подкупит чиновника штата, чтобы получить доступ к свежей информации.

Похоже, администрация магистралей не придает серьезного значения этим рискам. В 1995 году Massachusetts Turnpike Authority (МТА) опубликовала «Запрос о предложении» толщиной три дюйма, адресованный подрядчикам, заинтересованным в поставке штату системы ЕТС. Слова «приватность» и «сохранность личной информации» в нем не упоминались. Я позвонил исполнительному директору МТА Джону Джаджу [John Judge], чтобы спросить его о причинах. «Приватность не является проблемой», – ответил Джадж:

Я считаю так, исходя из общенационального опыта, по крайней мере, в отношении электронных систем сбора дорожных платежей. Приватность не является общенациональной проблемой. Мое мнение базируется на том, что это добровольная система. Если, по вашему мнению, проблема существует, вы можете не участвовать в этой программе и использовать традиционные методы оплаты. Я

⁶⁵ *ITS America News*, апрель 1997, р. 6–8.

⁶⁶ Принятый в 1997 году «Закон о защите приватности водителей» [Driver's Privacy and Protection Act] требовал от штатов предоставления людям возможности изымать свои данные из автомобильной базы данных до того, как она будет предоставлена на рынок.

не думаю, что здесь проблем больше, чем с кредитными картами.⁶⁷

Прискорбно, но американское правосудие согласилось с Джаддом, хотя и по другим причинам. 26 июня 1997 года судья Колин Макмагон [Colleen McMahon] постановил, что ТВТА должна предоставлять информацию о перемещениях по запросу полиции. До этого ТВТА требовала от полиции постановления суда на получение этой информации, что, по мнению Макмагона, слишком сковывало ее действия. Он аргументировал это тем, что перемещения владельцев E-ZPass легко прослеживаются, поэтому электронные записи также должны быть публично доступны.⁶⁸

Информация о местонахождении является важной частью систем сотовой телефонной связи, которые должны постоянно отслеживать местонахождение трубок, чтобы входящие вызовы достигали абонентов. В 1997 году British Telecom анонсировала разработку нового мобильного телефона, который передавал вызываемому абоненту координаты вызывающего с точностью до 9 метров. «Сотрудники теперь не могут позвонить на работу и назваться больными, находясь на пляже; перемещения неверных супругов также могут быть отслежены», – с энтузиазмом сообщалось в статье, опубликованной в *Electronic Telegraph*.⁶⁹ В рамках развития американской Службы спасения 911 к 2001 году операторы сотовой связи должны были обеспечить обнаружение местонахождения 60 % всех телефонов в пределах 150 метров. Как и любые другие данные о местонахождении, эта информация может быть использована с различными целями. Она не только позволяет быстрее послать машины скорой помощи к месту автомобильной аварии – полиция все чаще запрашивает эту информацию у сотовых операторов при осуществлении прослушивания в рамках оперативно-розыскных мероприятий.

Подобный подход к приватности перемещений наблюдается по ту сторону канадской границы. Шоссе 407 в Онтарио оборудовано сложной системой автоматического выставления счетов владельцам автомобилей, в зависимости от количества миль, которое они проехали по общественной магистрали. Система захватывает изображение номера автомобиля при помощи видеокамеры. Стоимость проезда рассчитывается и предъявляется к оплате при обновлении регистрации автомобиля: при отказе от оплаты регистрация не продляется.

Электронный сбор дорожных платежей

Эта выписка Управления дороги Orlando – Orange County Fxpressway показывает все передвижения автомобиля по системе платных магистралей штата. Передвижения автомобилей отслеживаются при помощи пассивного электронного тега, размещаемого на ветровом стекле или под рамой автомобиля. Несмотря на то что система E-Pass разработана для автоматического сбора дорожных платежей, ее также можно использовать для точного вычисления скорости автомобиля, отслеживания угнанных машин или даже слежки за неверными супругами. В будущем эти записи могут быть использованы также и для осуществления маркетинга. Автоматически системы сбора дорожных платежей – золотое дно приватной информации. Несмотря на это, публичных обсуждений целевого

⁶⁷ Интервью автору, 27 июня 1997.

⁶⁸ *Police Commissioner v. Triborough Bridge and Tunnel Authority* (Sup. Ct. NYC IA part 50R, 26 июля), по данным *Privacy Journal*, октябрь 1997.

⁶⁹ Robert Uhlig, «Spy Phones Trace Cheating Husbands», *Electronic Telegraph*, 27 августа 1997. Доступно в Интернете по адресу: <http://www.telegraph.co.uk/k:80et?ac=002093890%205%2054028&rtwo=r3bhbhhx&atmo=99999999&pg=/et/97/8/27/nbt27.html>, как сообщалось в выпуске RISK Digest от 29 августа 1997.

использования этих данных практически не проводилось. [Образец выписки любезно предоставлен Orlando – Orange County Expressway Authority]



Самая большая база данных в мире

Наверное, самая большая база данных сегодня – это совокупность web-страниц в Интернете. «Всемирную паутину» заполняют не только порнографические изображения, журнальные статьи и реклама всевозможной продукции, в ней находится также поразительное количество персональной информации: личные домашние странички, сообщения электронной почты и публикации в группах новостей. Эти записи могут быть автоматически исследованы для поиска разоблачений, случайного признания вины и других видов потенциально ценной информации.

Еще до взрывоподобного роста Всемирной паутины студент, впоследствии преподаватель Аризонского университета Рик Гейтс [Rick Gates], заинтересовался исследованием возможностей Интернета как базы данных. В сентябре 1992 года он создал Internet Hunt,^[p18] «мусорщика», ежемесячно выискивающего информацию в Сети. Первые поиски были направлены на розыск фотографий с метеорологических спутников и текстов речей Белого дома. Искатель пользовался особой популярностью среди библиотекарей, которые в то время были озабочены проблемой создания удобного «справочника Интернета».

В июне 1993 года Гейтс решил осуществить поиск другого рода. Основной целью было найти как можно больше информации о человеке по его адресу электронной почты.

В течение недели группа из 32 искателей собрала 148 различных фрагментов информации о жизни Росса Стэплтона [Ross Stapleton].⁷⁰ Компьютер Мичиганского университета сообщил, что Стэплтон имеет степень бакалавра по русскому языку и литературе и по информатике. Компьютер Аризонского университета сообщил, что он имеет кандидатскую степень в области управления информационными системами. Компьютер информационного центра сети американского Министерства обороны [US Military's Defense Data Network (DDN) Network Information Center] раскрыл текущие и предыдущие адрес и номер телефона Стэплтона. Полученная с Gopher-сервера^[p19] конференции «Профессионалы в области информатики за социальную ответственность» [Computer

p18

Hunt (англ.) – искатель, охотник.

⁷⁰ Интервью автору, август 1997.

p19

Gopher – название устаревшего протокола и программы для работы с информацией в Интернете. После начала распространения технологии WWW практически не используется.

Professionals for Social Responsibility] брошюра сообщила, что Стэплтон был одним из выступающих и что он является аналитиком Управления научных и оборонных исследований [Office of Scientific and Weapons Research] Центрального разведывательного управления США.

Но наиболее ценную информацию группа смогла собрать из публикаций, сделанных самим Стэплтоном. Просканировав сообщения, отосланные им в список рассылки COM-PRIV (по иронии судьбы он как раз посвящен вопросам приватности), группа узнала, что Стэплтон использует операционную систему OS/2 и не имеет факс-аппарата. Группа узнала также, что Стэплтон сотрудничал с Джорджтаунским университетом, где был адъюнкт-профессором и читал курс «Информационная эпоха». Они узнали, что Стэплтон подписан на *Arlington Journal*, *Chronicle of Higher Education* и *Prodigy*. Он является членом Американской ассоциации развития славистики [American Association for the Advancement of Slavic Studies, AAASS]. Его членский номер в Cleveland Freenet был #ak287.

Из предисловия к тезисам диссертации Стэплтона «Персональные компьютеры в странах СЭВ» [*Personal Computing in the CEMA Community*] исследователи узнали, что родителей Стэплтона звали Том и Ширли. Из заголовка другого посланного им почтового сообщения им удалось установить, что он помолвлен и что имя его возлюбленной – Сара Грей. Они также откопали запись выступления Стэплтона на II конференции «Компьютеры, свобода и приватность» [*Second Conference on Computers, Freedom and Privacy*].⁷¹

«Оглядываясь немного назад и оценив результаты поиска в целом, можно сказать, что имеется ужасающе большое количество информации о ком-нибудь, которое может быть найдено, даже если ограничиться только свободно доступными публичными сетями, – писал Рик Гейтс в отчете о результатах поиска. – Я надеюсь, что люди помнят об этом, когда отправляют сообщения в списки рассылки и группы новостей. Они вносят свой вклад в единое информационное пространство Сети, и все, что они высказывают в ограниченной дискуссии по [закрытой] теме, будет доступно еще долгое время».

Противоположный эффект, возникающий при пользовании глобальной базой данных, заключается в том, что в ней легко найти информацию о человеке с уникальным или необычным именем. Например, в феврале 1998 года я попробовал найти в Интернете словосочетание «Tom and Shirle». Поисковая система HotBot нашла слово «Тот» на 1 833 334 страницах, а слово «and» – на 63 502 825 страницах. Но слово «Shirle» нашлось только на 333 страницах, а фраза «Tom and Shirle» – только на шести, все из которых были копиями отчета Гейтса, написанного в июне 1993-го.

«Я был приятно удивлен количеством информации, которое я произвел и которую они смогли найти, – сказал Стэплтон, когда я брал у него интервью при написании этой главы. – Я бы не сказал, что что-нибудь из найденного во время этого поиска меня тревожит». Но Стэплтон опасался, что у кого-нибудь из ЦРУ может вызвать недовольство тот факт, что он раскрыл свое имя и имя работодателя в таком количестве общественных форумов. «Это только вопрос времени, когда кто-нибудь спросит меня на работе: „Эй, что ты сделал?“»

Пожалуй, наиболее примечательным в этом поиске было то, что возможность сбора подробной информации о человеке только лишь по открытым источникам перестала быть чем-то необычным. Исследование онлайн-источников информации вкупе с использованием поддерживаемых рекламой поисковых систем типа Yahoo, Lycos и AltaVista[p20] сделало возможным очень легко собирать такие подробные досье. И конечно,

⁷¹ The Second Conference on Computers, Freedom and Privacy, Washington, D.C., 1992. См.: <http://www.cpsr.org/dox/conferences/cfp92/home.html>.

некоторые сервисы, в особенности DejaNews/[p21] и HotBot, прямо рекламируют такую возможность.

Эра публичных заявлений

Постинги в форумы электронной почты, группы новостей и онлайн-чаты являются разновидностями публичных заявлений. Большинство людей, решивших занять свое место в киберпространстве, рано или поздно начинают делать такие заявления. И эти заявления не похожи ни на какие другие, произносимые когда-либо в человеческой истории. В прошлом публичные заявления часто терялись. Конечно, они могли быть записаны, но эти записи было не так-то просто найти, если они вообще были доступны. Раздраженный фермер мог выступить на городском собрании, и его имя записалось в протоколе, но через десять лет, если кто-нибудь захотел порыться в прошлом этого фермера, он вряд ли нашел бы материалы этого выступления, особенно если этот фермер переехал в Сиэтл и начал новую жизнь, поступив программистом в Microsoft. Письма, написанные в газеты в 50-е, 60-е, 70-е и 80-е годы XX века, конечно, были опубликованы для всеобщего обозрения, но маловероятно, что их поместили в компьютерные банки данных, проиндексировали и сделали постоянно доступными из любой точки земного шара.

Это новое поколение публичных заявлений имеет в первую очередь количественные отличия от всего, что было раньше. Все они могут быть мгновенно отысканы и просмотрены потенциальным работодателем, человеком, с которым у вас только что состоялась первая встреча, или коллегой, который хочет причинить вам вред. Как только вы сделали заявление, вы сразу же теряете контроль над ним: вернуть его назад уже невозможно.

Именно возможность поиска привела к появлению нового типа *абсолютной подотчетности*. Очень просто использовать поиск в Интернете для составления списков людей, замеченных в употреблении ЛСД, запятнавших себя расистскими высказываниями в печати или причастных к организации профсоюзов. Стэплтон говорит: «Какому-нибудь сотруднику службы по работе с персоналом очень просто сказать: „Посмотрите, Джо здесь высказался, что скайдайвинг/[p22] – это круто. Должны ли мы дальше держать его в штате, понимая, что он может разбиться? А Джейн здесь представляет стиль жизни, который не нравится нашему президенту. Мы не должны продвигать ее в интересах общего дела“. Я не занимаюсь общественной деятельностью, о которой не хотел бы писать. Если я что-то делаю, я должен быть очень осторожным».

В конечном счете широкая доступность этой информации может создать новые мощные социальные фильтры, через которые смогут пройти только очень настойчивые и избранные. Существование этой информации делает самоуверенных людей уязвимыми ко всем видам злонамеренных атак. Получающие все более распространение запись и индексирование публичных заявлений могут хранить самые лучшие и яркие высказывания всех, когда-либо занимавших выборные должности.

Waste. com

p21

Портал DejaNews позднее был приобретен поисковой системой Google, поэтому поиск в архивах конференций (в том числе и русскоязычных) можно осуществить по адресу <http://groups.google.com>.

p22

Skydiving (англ.) – упражнения в воздухе в свободном падении.



12 мая 1999 года Boston Herald опубликовала на первой странице статью под названием «Waste.com». ⁷² В статье подробно освещались результаты проведенного Herald расследования, посвященного изучению использования Интернета государственными служащими, а также других подключений к Интернету, оплачиваемых налогоплательщиками. Было установлено, что учетная запись, зарегистрированная на службу аудита штата, использовалась для спекуляции билетами на спортивные мероприятия, что являлось нарушением закона штата. Журналисты обнаружили, что учетная запись, принадлежащая MassEd.net, бюджетной организации, субсидировавшей доступ в Интернет учителям и школам, была использована «для продвижения web-сайта сексуального содержания». Обнаружилось, что учетная запись Министерства общественных работ «использовалась для покупки и продажи японских эротических мультфильмов, включая серию „Насильник“, прославляющую изнасилование». Замечено, что пользователь Интернета из Госдепартамента послал 324 сообщения на тему телевизионных шоу, включая «Симпсонов». Также были обнаружены студенты, использующие предоставляемый им учебными заведениями доступ в Интернет для подачи объявлений об изготовлении и приобретении ЛСД и других галлюциногенов.

Исходные материалы для расследования практически полностью были получены путем поиска в Интернете при помощи поисковой системы DeJa.com, архивирующей все сообщения в группы новостей и электронные доски объявлений. Несмотря на то что сообщения в Интернете легко могут быть подделаны, об этом в статье не упоминалось.

Этот отчет вызвал немедленную реакцию официальных лиц, которые заверили, что ужесточат существующую политику использования Интернета и введут новую – с целью недопущения нецелевого использования Интернета. Это еще раз доказало важность архивов Интернета для контроля использования людьми компьютерных систем.

В конце уже упомянутого отчета 1993 года об Internet Hunt можно найти очень точное замечание: «Говоря кратко, мы имеем дело с уникальным окружением. Оно чем-то похоже на устное обсуждение, но гораздо более длительно и вовлекает миллионы людей».

Забавно, но отчет Гейтса доступен сегодня и, видимо, будет доступен еще в течение десятилетий. Это происходит потому, что текст в цифровой форме легко переносится, очень компактен и легко поддается поиску. Несмотря на то что компьютер, на котором был набран тот текст и с которого он был отправлен, уже давно не используется, информация копируется снова, снова и снова.

Умные машины создают активные банки данных

⁷² Joseph Malia, «Waste.com: Public Employees Using Internet for Sex, Drugs, and Rock 'n' Roll», *Boston Herald*, 12 мая 1999, р. 1. Полный текст доступен в Интернете по адресам <http://www.bostonherald.com/bostonherald/lonw/mai05121999.htm> и <http://www.mapinc.org/drugnews/v99.n505.all.html/lsd>.

Компания Hewlett-Packard, производящая компьютеры, 14 апреля 1999 года опубликовала в *Wall Street Journal* трехстраничную рекламу. Первые две страницы занимало черно-белое объявление, в котором был изображен хорошо оборудованный гараж с пустым местом посередине. Машина уехала недавно. Текст гласил:

Ваша дочь наследовала ее от вас. Это шаг вперед. И вы оставили свой коллекционный «ягуар» в гараже. Вы так думаете. Но когда вас нет в городе, вы не уверены... Используйте e-service. Е-что? Микросхему безопасности, которая опознает ключи вашей дочери и включает режим «мягких ограничений», не позволяющих машине развивать скорость свыше 105 км в час. Но, конечно, она попытается это сделать. В это же мгновение машина пошлет сигнал в сервис, на который вы подписаны, предупреждая вас о происходящем. Находясь в трех тысячах миль от этого места, вы отрываетесь от обеденного стола и направляетесь к лобби, чтобы сделать звонок. Ваша дочь не успела отъехать и трех кварталов от выездной дорожки вашего дома, как в машине начинает звонить телефон: «Опять за старое?» Бизнес предоставляет услуги с использованием Интернета, и это давно уже вышло за рамки обычных web-сайтов. Термин «услуга» перешел в другое измерение. Очередная глава истории Интернета почти закончена. Вам больше не надо работать во Всемирной паутине. Вместо этого Интернет будет работать на вас.

www.hp.com/e-services

The next E. E-services. Hewlett-Packard.

Видение активного мира Hewlett-Packard рисует не очень доброжелательное будущее, ожидающее всех нас. Почему встроенная в «ягуар» микросхема НР не позволяет превышать скорость только дочери, но не ее родителям? Почему машина звонит родителям, а не в местную полицию? Почему страховая компания не предупреждена о небезопасном водителе? Почему продавец автомобиля не получает отчет о скоростном режиме, чтобы на его основании аннулировать гарантию на трансмиссию? Возможно, следующая глава развития Интернета позволит автомобилям автоматически снимать штраф за превышение скорости прямо с вашего банковского счета, не требуя от общества дополнительных затрат на офицера полиции, который должен вас останавливать.

Зачем вам, субъекту этой информации, контролировать информационные тени всех ваших сегодняшних поступков?

Поворот вспять информационного потока

Более быстрые машины, более емкие жесткие диски и интеллектуальные системы управления базами данных – все это представляет большую угрозу приватности. В то время как возможности компьютеров по хранению информации увеличиваются на 60–70 % в год, население Земли растет всего на 1,6 %. Пройдет время, все встанет на свои места, и все больший процент наших ежедневных действий будет фиксироваться всемирной инфосферой.

Что же делать? Неужели мы стоим перед будущим, в котором вся наша жизнь может быть прочитана как открытая книга, в котором все наши секреты будут храниться в прозрачных папочках? Будем ли мы все в большей степени подвергаться наблюдению со стороны наших соседей, нашей семьи и даже наших машин, пока все мы не заживем в абсолютно прозрачном обществе? Возможно. Однако мы имеем право выбора. Мы не можем повернуть время вспять, но мы можем построить мир, в котором критичная информация уважается и хранится в секрете.

Вспомним случай судьи Борка. По факту получения журналистом записей о Борке в видеотеке на Капитолийском холме была инициирована серия слушаний. Циники говорили, что сенаторы и конгрессмены боятся, что их собственные записи могут быть использованы в грязной игре, и законодателям вроде Борка есть что скрывать. Но, независимо от мотивов

слушаний, в результате стало ясно, что случай с Борком далеко не единичный. «[На слушаниях] было упомянуто множество примеров использования информации о взятых напрокат фильмах, включая попытки использовать эту информацию для доказательства, что супруг является плохим родителем, а один из ответчиков по делу о домогательстве к ребенку пытался доказать, что обвинения ребенка базируются на фильмах, просмотренных дома», — сообщало Министерство торговли.⁷³

Слушания не прошли впустую. В конце законодательной сессии конгресс одобрил, а президент Буш подписал Video Privacy Protection Act/p23/1988 (18 USC 2710). Согласно закону, «поставщик услуг по прокату видеофильмов, который умышленно раскрыл кому бы то ни было идентифицируемую персональную информацию о любом клиенте», бравшем напрокат видеофильмы, несет перед клиентом гражданскую ответственность в размере 2500 долларов, подвергается штрафу, оплачивает услуга адвоката и другие издержки, которые суд сочтет необходимыми. Запретив пунктам проката видеофильмов предоставлять информацию о названиях фильмов, которые вы брали (за исключением случаев, когда это делается по постановлению суда), закон изъясил из оборота записи о прокате. Установив размер гражданской ответственности, конгресс устранил проблему, которая всегда возникала при подаче исков за нарушение приватности: необходимо было доказать, что нанесен ущерб. Более того, давая возможность истцу требовать оплаты услуг адвоката, конгресс надеялся, что по совокупности признаков юристы будут охотнее браться за такие дела.

В любом случае закон 1988 года не привел к существенным подвижкам: владельцам пунктов видеопроката по-прежнему разрешалось хранить регистрационные записи после возврата кассет, вместо требования обязательного уничтожения этих записей. Закон также не запрещал этим компаниям строить на основе индивидуальных данных агрегированные массивы информации, которые потенциально могут послужить для нарушения приватности личности. Невзирая на это, Video Privacy Protection Act был потрясающе эффективен. Его нарушения чрезвычайно редки. Американцы знают, что могут взять напрокат любой понравившийся видеофильм и не отвечать за это ни перед кем.

Video Privacy Protection Act доказал то, о чем многие защитники личных свобод говорили с 1960-х годов: свободный рынок и добровольно принятые стандарты обеспечения приватности зачастую недостаточны для защиты приватности потребителей. Появившаяся в *USA Today* передовица освещала это так: «Только в идеальном мире добровольное согласие предпочтительно, в реальном мире оно не работает. В реальности отсутствие государственного регулирования приводит к тому, что очень многие компании практически ничего не делают для защиты прав потребителей на неприкосновенность частной жизни».⁷⁴

Многие фирмы собирают огромный объем персональной информации в процессе своей повседневной деятельности. Но из самого факта, что информация собрана, не следует, что у фирм появляется право делать ее доступной для общественности, продавать на открытом рынке или использовать в маркетинговых целях. Данные должны быть «убраны со стола». Строгое законодательство в области защиты личной информации стимулирует бизнес поступать именно так.

Другой не менее верный способ обеспечения приватности заключается, в первую очередь, в запрете накопления персональной информации. Например, вместо построения

⁷³ U.S. Department of Commerce, *Privacy and the Nil: Safeguarding Telecommunications-Related Personal Information*, октябрь 1995. Доступно в Интернете по адресу <http://nsi.org/Library/Comm/privnii.html>.

p23

Закон о защите неприкосновенности частной жизни, примени тельно к просмотру видеофильмов. Является «надстройкой» к принято му в 1980 году. «Закону о неприкосновенности частной жизни» [Privaq Protection Act].

⁷⁴ Редакционная статья *USA Today*, 25 октября 1995.

ЕТС-системы, которая хранит балансовые счета и информацию о движении в централизованной базе данных, можно построить анонимную систему. Такие системы реализуются на базе смарт-карт и используют для оплаты дорожных платежей «электронную наличность». Смарт-карты в таких системах могут программироваться для хранения информации о пользовании платными магистралями только для личного использования водителем или программироваться на уничтожение этой информации. Создание и эксплуатация распределенных систем на базе смарт-карт обойдутся дешевле, чем создание и эксплуатация централизованных систем на базе мощных компьютеров. К сожалению, они менее популярны – видимо, потому, что эту технологию сложнее объяснить лицам, принимающим решения.

Вообще, информированные и организованные гражданские объединения вряд ли потерпят неудачу при проталкивании строгих мер обеспечения приватности. Рассмотрим пример Гонконга: в 1980-е годы колониальное правительство построило сложную систему электронной оплаты проезда по дорогам. Вскоре после внедрения системы водители начали получать извещения, в которых подробно сообщалось, где и когда они проезжали, – и это их встревожило. Опасаясь того, что система может быть использована для слежки за человеком в политических целях, особенно после передачи в 1997 году Гонконга под управление Китая, граждане потребовали закрыть систему.⁷⁵

Ошибка в принятии решения всегда имеет прямые последствия. Когда люди осознают, что их информация может быть использована против них самих, они начинают сопротивляться – либо преднамеренно отказываясь предоставлять информацию, либо специально помещая в систему ложные данные. Например, многие пользователи Интернета борются с проблемой непрошеной почты, «спамом», используя искаженный адрес электронной почты на своих web-страницах и при написании сообщений в группы новостей.^[p24] Многие люди используют выдуманные или умышленно неправильно записанные имена при подписке на журналы. И конечно многие используют для оплаты наличные деньги вместо кредитных карт, даже если это не совсем удобно делать. Если эти меры оказываются недостаточными, применяются еще более изощренные техники.

5

Взгляд с высоты

На поверхности нашей планеты, в глубине океанов и в небе над ней с неистовой силой разворачивается беспорядочный проект. Проект по разворачиванию целого сонма камер, подслушивающих устройств и сенсоров, объединенный в глобальную компьютерную сеть, которая будет знать, записывать и сохранять информацию обо всем происходящем. Проект по превращению планеты в единый научный инструмент и созданию глобальной библиотеки происходящих фактов.

Еще в 50-е и 60-е годы XX века многие борцы за гражданские права были обеспокоены прослушиванием правительством частных домов и офисов. В последние годы в газетах появилась информация о «шпионских магазинах», торгующих сложным оборудованием для

⁷⁵ The Diebold Institute for Public Policy Studies, Inc., *Transportation Infrastructures* (Westport, CT: Praeger, 1995).

p24

Речь идет, видимо, о борьбе с «автоматическим» спамом, т. е. с программами, автоматически собирающими в Интернете адреса электронной почты для последующего использования в массовых рассылках. Для этого адрес вида name@company.com записывают, например, в виде name@NOSPAMcompany.com. Если посетитель сервера захочет написать автору, он догадается убрать «NOSPAM», программа же, выискивающая строки по шаблону «*@*» получит несуществующий адрес.

дистанционного прослушивания, миниатюрными радиопередатчиками, включающимися от звука голоса магнитофонами и лазерными микрофонами, позволяющими по вибрации стекол узнать, о чем говорится внутри помещения. Но сегодня становится все яснее, что реальная угроза приватности исходит не от прослушивания частных домов, что по большей части незаконно и мало распространено. Нет, реальную угрозу представляет постоянный мониторинг общественных мест, доступность и законность которого сделали наблюдение свободным для всех.

В последующие 50 лет все шире распространяющийся сетевой мониторинг коренным образом изменит наше представление о том, что значит быть «на публике». Забавно, но эта смена заставит нас буквально воспринимать слова «общественные места». В прошлом большинство общественных мест были на самом деле частными. Прогуливаясь в одиночестве по городским улицам или беседуя с другом в парке, мы ощущали себя защищенными, знали, что нас никто не записывает. Но постоянный мониторинг изменил наши представления на прямо противоположные. Мы справедливо полагаем, что приватность гарантируется нам в наших домах, но мы не строим таких же предположений относительно общественных мест. И чем больше все происходящее фиксируется, записывается, индексируется и легко извлекается на свет при необходимости, тем меньше приходится рассчитывать на анонимность в общественных местах.

В будущем общественность будет знать все, что происходит в общественных местах.

Эй, я здесь живу!

У меня на стене висит постер с видом нашей планеты из космоса, но этот вид никогда не открывался астронавтам или спутникам. На этой картинке наша планета освобождена от покрова облаков. Северное и Южное полушария изображены в разгар лета, одетые в зелень, с шапками льда, сдвинутыми на полюса. Полностью видны все горные массивы Земли, а окраска океанов показывает перепады глубин и морские течения.

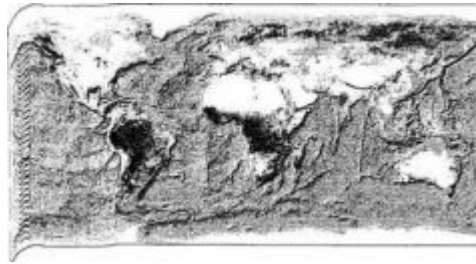
Постер «Земля: новый вид планеты со спутника с выделением рельефа» выпущен небольшой фирмой WorldSat, расположенной в Онтарио (Канада). Этот постер не только подтверждает возможности искусственных спутников Земли, но и наше увлечение географической информацией. Возможность создавать географические мозаики, вроде созданной WorldSat, имеет глубокое влияние на будущее приватности. География неизбежна. Все находится где-то.

Впервые я увидел постеры WorldSat в книжном магазине Вашингтонского университета. Я зашел, чтобы купить новую авторучку. Минут десять я рассматривал ручки, а затем целый час – картинки со спутника, ведь кроме «Земли» в магазине также были представлены виды из космоса Австралии, Азии, Европы и Северной Америки. И я был не одинок: одна пара неподалеку от меня минут двадцать рассматривала созданный фирмой NovaGraphics постер «Земля ночью», пытаюсь определить каждый город по его огням.

В течение следующих двух недель я часто заходил в этот магазин, чтобы полюбоваться изображениями. Они словно околдовали меня. В конечном счете, я купил постер «Земля» и повесил его на стену. А потом я связался с WorldSat, чтобы узнать не только как был сделан постер, но и причину, по которой фирма занялась этой продукцией.

WorldSat была основана в 1986 году Робертом Стейси [Robert Stacy], профессиональным водолазом, увидевшим спутниковые изображения в книжном магазине в Онтарио. В Онтарио он выздоравливал после несчастного случая. Очарованный, как и я, и не имеющий возможности вернуться к своей прежней профессии, Стейси решил организовать фирму, которая создавала бы из этих изображений постеры на продажу.

Постер «Планета Земля» от WorldSat



Очищенный от облаков и сезонного снежного покрова, освещенный 24-часовым солнцем, такой вид планеты Земля никогда не открывался astronautам, наблюдавшим за ней невооруженным взглядом. И все же этот вид в некотором роде больше соответствует действительности, чем отдельные снимки. Это изображение, созданное WorldSat, демонстрирует огромные возможности комбинирования множества изображений со спутников и их компьютерной обработки. [Изображение любезно предоставлено фирмой WorldSat]

WorldSat получила большинство изображений бесплатно. Исходными данными для серии постеров «Мир» стали изображения с метеорологических спутников Национальной организации по изучению океанов и атмосферы [National Oceanic and Atmospheric Administration, NOAA], орбита которых проходит на высоте 820 км. Скрупулезно комбинируя тысячи изображений, в конечном счете можно получить электронное изображение нашей планеты без облаков. Используя пару снимков, сделанных спутником с разных точек на определенном удалении, можно создать стереоскопическое изображение поверхности планеты. Эта информация используется для подчеркивания рельефа, и карта выглядит как трехмерная. Данные о рельефе океанского дна получаются путем комбинирования спутниковых и наземных исследований.

«Создание изображений было технологическим соревнованием, так как использовался огромный объем данных», – рассказывает доктор Эмери Миллер [Dr. Emery Miller], вице-президент по развитию бизнеса компании WorldSat.⁷⁶ Как и любое другое изображение на экране компьютера, «Земля из космоса» состоит из маленьких квадратных точек, называемых пикселями. Эта картинка была создана с разрешением в один километр, т. е. каждый пиксель в районе экватора представляет квадрат со стороной в один километр. Земля представляет собой почти правильную сферу с окружностью около 40 тыс. км⁷⁷ и площадью около 127 796 494 км². Таким образом, ее изображение в компьютере WorldSat занимало около 128 миллионов пикселей. [p25] По словам доктора Миллера, для хранения этих 128 миллионов пикселей в компьютере, использованном при создании постера, потребовалось хранилище размером более шести гигабайт. В 1994 году, когда впервые

⁷⁶ Интервью автору, 20 февраля 1997.

⁷⁷ На самом деле окружность Земли по экватору составляет 40 074 км, а по меридиану (через полюса) – 40 000 км. Числа выглядят подозрительно? Действительно, метр был определен в 1791 году Французской Академией наук как 1/10 000 000 четверти дуги окружности Земли, проведенной с Северного полюса к экватору через Париж. В 1889 году Международная палата мер и весов переопределила метр как расстояние между рисками, нанесенными на эталонном металлическом бруске, хранящемся в Париже. (Гораздо проще было с высокой точностью измерить брусок, чем расстояние от Северного полюса до экватора!) В 1960 году метр был переопределен снова в рамках Международной системы единиц и стал равен 1650763,73 длинам волн в вакууме оранжево-красной линии в спектре атома криптона-86. В 1983 метр был переопределен еще раз Генеральной конференцией по мерам и весам и стал равен расстоянию, которое свет проходит в вакууме за 1/299792458 секунды. Каждое переопределение метра позволяло ученым во всем мире производить свои измерения с все большей точностью. Новые определения таким образом соотносились с увеличивающейся точностью научных инструментов и возможностью измерить определенные виды явлений с повышенной точностью.

создавался этот набор данных, WorldSat столкнулась с ограниченной производительностью самых быстрых компьютеров в мире. Земля – очень большое место.

Компактный размер изображения Земли на постерах WorldSat делает практически невозможным рассмотреть на них что-либо рукотворное. Сжатие 40 тысяч километров в 90-сантиметровый постер означает, что в каждом сантиметре содержится 437 км. На самом деле, если вы возьмете увеличительное стекло и посмотрите на места, где расположены крупные города, все, что вы увидите, – маленькое красноватое пятнышко, окруженное зеленым океаном. Эти точки – сочетание пыли, загрязнения, дорог и строений. Природа имеет зеленый цвет.

Хотя лично меня пленило изображение всей планеты. Миллер говорит, что множество людей хочет изображения более местного характера. «Мы обнаружили, что наибольший интерес вызывает возможность найти свой дом», – говорит он. Люди хотят показать на карту и сказать: «Я живу здесь! Посмотрите на это!»

Постеры WorldSat лишь начало. Если у вас есть терпение, компьютер и 50 долларов, вы уже сейчас можете получить больше: вы можете заказать спутниковую фотографию вашего дома, сделанную самым современным шпионским спутником. Еще в начале 1980-х некоторыми космическими державами были предприняты усилия по превращению спутниковых фотографий из чисто правительственного инструмента в рыночный товар, доступный не только бизнесу, но и обычным потребителям. Это еще один пример неизменной демократизации современных технологий.

Глаза в небе

Соединенные Штаты запустили свой первый шпионский спутник в 1959 году. Совершенно секретный проект под названием Corona, по сути, стал первой американской космической программой. Каждый спутник Corona был оснащен специальными объективами ультравысокого разрешения, специальной фотопленкой, которая выдерживала космический холод, и спускаемыми аппаратами, которые должны были возвращать отснятый материал на Землю. Камеры имели разрешающую способность до 1,5 метра. Это означало, что любой наземный объект, имевший размер как минимум 1,5 метра: автомобиль, палатка или шахтная ракетная установка, – мог быть различен из космоса.

Панорамная съемка поверхности – самое очевидное использование спутников-шпионов, но она тогда только зарождалась.

Разрешение в 1,5 метра позволяло проводить относительно сложные исследования. Например, аналитик мог различать типы самолетов по силуэтам, что было очень важно для военных планов. Вы могли бы подсчитать число находящихся на парковке машин, чтобы определить примерное число работающих в определенном здании, будь то фабрика или «безопасная фирма».

Преимущество спутников перед самолетами-разведчиками¹¹² заключалось в том, что они были беспилотными и позволяли вести постоянное наблюдение за несравнимо большими территориями. Спутники предоставляли недостижимую другими методами степень точности и повторяемости. И американские военные всю пользовались, открывшейся возможностью. Ежемесячно фотографируя один и тот же участок, можно было со всеми подробностями отслеживать развитие промышленности в СССР, перемещения войск и даже некоторые аспекты экономики страны. В 1996 году, когда проект Corona был рассекречен, *Technology Review* писала:

«С 1960 по 1972 год в рамках проекта Corona на орбиту Земли был выведен 121 спутник, отснявший 800 тысяч изображений или около 689 тысяч метров пленки».⁷⁸

⁷⁸ *Technology Review*, октябрь 1996. См. <http://www.tech-rereview.com/articles/oct96/Shulman.html>.

Спутниковое наблюдение не нарушало никаких законов или соглашений. Все происходившее за пределами помещений, в общественных местах по определению было публичным. Но если говорить по правде, имелись более практические причины для возражений. Советский Союз не протестовал против высотных полетов самолетов U2 до 1960 года, когда он смог сбить самолет-разведчик, пилотируемый Гарри Пауэрсом [Gary Powers]. Но от спутников-шпионов не было защиты, кроме пасмурных дней и нахождения в помещениях. Выставление формального протеста могло быть истолковано как государственное бессилие.

В течение десятилетий разрешающая способность спутников-шпионов не шла ни в какое сравнение с гражданскими орбитальными объектами. Однако это не делало фотографирование с более низким разрешением менее востребованным. Спутники Landsat 5 и Landsat 6, запущенные в 1982 и 1984 годах, имели на борту оборудование, позволявшее фотографировать поверхность Земли с 30-метровым разрешением в шести различных спектральных диапазонах.⁷⁹ Хотя изначальной целью создания этих спутников было исследование природных ресурсов (об этом говорит и их официальное наименование – технологические спутники по исследованию ресурсов Земли [Earth Resources Technology Satellites]), изображения с Landsat также использовались для мониторинга атмосферных и океанских условий, определения уровня загрязненности, поиска нефти, наблюдения за посевами зерновых и лесами и, конечно, для создания постеров. Спутники Landsat пролетают над каждым участком земной поверхности каждые 18 дней. Вы можете приобрести снимки с Landsat, охватывающие территорию в 160 км², за 3500 долларов, получив скидку при приобретении более старых данных.

Представленное Landsat 30-метровое разрешение идеально подходит для обзора посевов зерновых и больших ферм. Но Landsat не очень хорошо подходит для мониторинга прямых последствий деятельности человека. Большинство дорог и зданий имеют размер менее 30 метров, поэтому просто невидимы для камер Landsat.

Положение дел изменила Франция, запустившая в 1986 году первый коммерческий спутник-шпион под названием SPOT 1 (SPOT – сокращение от французского Satellite Pour l'Observation de la Terre – спутник для наблюдения за Землей). Первые три спутника SPOT были оборудованы двумя камерами. Одна из них была черно-белой, дававшей разрешение в 10 метров. Вторая камера записывала зеленые, красные и околоинфракрасные изображения с разрешением в 20 метров. Изображения с обеих камер могли быть скомбинированы для получения полноцветной картинки высокого разрешения. Эти камеры вошли в историю месяц спустя, когда спутник SPOT 1, оказавшийся в этот момент над территорией Украины, снял взрыв на Чернобыльской атомной электростанции. Советский Союз скрывал факт аварии, но история вскрылась благодаря этим фотографиям.

Находясь на орбите 830 километров над поверхностью Земли, спутники SPOT 1 и SPOT 3 полностью охватывают поверхность планеты каждые 26 дней. Имея размер и вес как у фургона, эти камеры фотографируют участки шириной 60 и 117 километров, находящиеся под траекторией движения спутника. Изображения шифруются и передаются в пакетном режиме непосредственно на Землю, где принимаются наземной станцией SPOT.

Крупнейшими клиентами SPOT являются «черные» агентства – разведывательные службы США и других стран. Глянцевый рекламный листок SPOT показывает спутниковые изображения, сделанные во время войны в Персидском заливе. На одном снимке изображена секретная военная установка, состоящая из нескольких десятков групп строений. На следующей фотографии показаны те же самые строения, но вместо их белых крыш виднеются черные пятна. «Черный цвет на многих структурах означает пожар», – сухо

⁷⁹ Информация о спутниках Landsat, Seasat, TIROS, Transit и Vela из энциклопедии «Britannica», издание 1997 года. Онлайн-версия доступна по адресу <http://www.eb.com>.

гласит пояснительная надпись. Похожие изображения множества домов мирных жителей без крыш были показаны силами НАТО в апреле 1999 года для демонстрации результатов проведенной сербами в Косово «этнической зачистки». Благодаря этим изображениям НАТО получило общественную поддержку бомбардировок Сербии.

«В 1986 году, сразу после запуска системы, многие люди считали, что это повредит национальной безопасности и приватности. „Нашей приватности пришел конец“, – говорили они», – рассказывает Кларк Нельсон [Clark Nelson], менеджер по маркетингу и коммуникациям SPOT.⁸⁰ Но прошли годы, критики научились жить под взглядом орбитальных глаз, а бизнес и правительство научились использовать его.

SPOT продает фотографии для корректировки карт, мониторинга изменений окружающей среды и предоставления визуального наполнения для компьютерных геоинформационных систем. Фермеры могут использовать снимки SPOT для наблюдения за своими полями: менее чем за 50 центов за акр [0,404 га] они могут определить, какие посевы нуждаются в ирригации или удобрении. Люди, использующие сегодня эти изображения, «продвинутые фермеры-джентльмены, – говорит Нельсон. – Они говорят: „Я устал от трактора. Мне нужна современная цифровая обработка изображений со спутника“». Но уже через несколько лет спутниковые изображения станут базовым инструментом в агробизнесе.

За первопроходцами следуют массы. Сети быстрого питания McDonald's и KFC начали использовать спутниковые фотографии для выбора места размещения своих заведений в быстро растущих областях, т. е. там, где муниципальные карты еще не показывают точно, какие дороги уже построены и где возводятся новые дома. Спутниковые фотографии все больше используются для иллюстрации бизнес-отчетов.

Типичным бизнес-продуктом, созданным при помощи SPOT, является MetroView – улучшенные спутниковые изображения основных городов США, которые могут быть легко использованы в программах для персонального компьютера типа Adobe PhotoShop. Изображение всего метрополиса продается по цене от 400 до 600 долларов, более мелкие «ячейки» стоят по 100 долларов. SPOT также играет важную роль при определении места размещения базовых станций операторов сотовой связи в развивающемся мире. Изображения дают очень подробную карту, включая перепад высот местности, расположение дорог, плотность застройки и высоту зданий. «Это самое замечательное равновесие, которое я мог наблюдать за последние 11 лет, – говорит Нельсон. – У нас есть данные, которые им нужны, а у них есть деньги, чтобы заплатить за них. Охватим мы этот проклятый мир или нет? Мы предоставляем очень подробные карты удаленных районов, а они [коммуникационные компании] обеспечивают их телекоммуникациями».

Вид Китая со спутника наблюдения

Изображение территории Китая в трехмерной перспективе полностью создано на основе фотографий, полученных с французских спутников наблюдения SPOT (за исключением нарисованного художником рисунка справа вверху). Данные, из которых получено это изображение, были помещены в компьютерную программу, разработанную фирмой Qualcomm Inc. (Сан-Диего, штат Калифорния), и использованы для расчета мест установки вышек базовых станций сотовой связи. Используя эту систему в Гонконге, Qualcomm смогла сократить необходимое число базовых станций с 83 до 80, сэкономив 3 миллиона долларов на строительстве станций и 1,5 миллиона долларов на тестировании. [Фотографии и рисунок любезно предоставлены SPOT Imaging]

⁸⁰ Интервью автору, апрель 1997.



SPOT разработала также мобильную базовую станцию Eaglevision.^[p26] Разработанная для оказания помощи в чрезвычайных ситуациях и военных операциях, эта станция состоит из тарелки диаметром 3,5 метра, которая может непосредственно принимать сигналы со спутника, и двух грузовиков с компьютерами и оборудованием для их обработки. Система может получать изображение с пролетающего над ней спутника SPOT и строить подробную карту окружающей местности. Система может также строить трехмерную модель, которую можно затем поместить в летный тренажер и использовать для подготовки к спасательной операции или бомбометанию.

SPOT всего лишь одна из большого количества компаний, либо продающих доступ к информации с правительственных спутников, либо имеющих свои собственные. В 1984 году корпорация Lockheed Martin приобрела компанию Earth Observation Satellite Company (EOSAT), целью создания которой была коммерциализация американских правительственных спутников Landsat. В 1990-х годах Landsat перешла на использование спутников-шпионов с высоким разрешением. Первоначально Landsat сотрудничала с правительством Индии, приобретя эксклюзивные права на продажу изображений с индийского спутника IRS-1C, который был запущен в декабре 1985 года и имел разрешающую способность в 5,8 метра. В 1996 году EOSAT была приобретена расположенной в Колорадо компанией Space Imaging, которая теперь обладает самым большим количеством гражданских наблюдательных спутников на орбите. Недавно компания запустила свой собственный спутник, обладающий разрешающей способностью в 1 метр.

Кто нуждается в спутниковых изображениях высокого разрешения? Практически все, утверждает в рекламе Space Imaging. Компания видит свой рынок сбыта в сельском хозяйстве, правительственных кругах, в исследовании окружающей среды, картографии, коммунальных предприятиях, на рынке носителей информации и даже среди конечных потребителей, как это следует из приведенной ниже цитаты с web-сайта компании:

Обзор Земли с высоты открывает новые возможности на потребительском рынке, и невообразимыми доселе способами. Ориентированные на конечного потребителя продукты Space Imaging могут быть использованы в широком спектре приложений, начиная от обучения и развлечений и заканчивая решением проблем и персональной навигацией.

Спутниковые изображения Земли предлагаются сегодня в разрешении, которое никогда раньше не было доступно на коммерческом рынке, и предоставляют неограниченную информацию о планете клиентам, которые традиционно и не представляли, какую степень подробности дают спутниковые

изображения. Цель Space Imaging – как можно шире внедрить изображения Земли в самые различные продукты клиентов, включая симуляторы полетов, сборники карт, планировщики путешествий, хранители экрана, энциклопедии, видеофильмы о путешествиях, разрезные мозаики, почтовые открытки и картинки в рамках.⁸¹

Возможно, более красноречива рекламная литература, которую я получил на торговой выставке в Сिएтле в 1997 году. На выставке, посвященной современным технологиям наблюдения, EOSAT раздавала рекламную брошюру, описывающую, как местные органы власти могут использовать изображения с индийского спутника с 5-метровым разрешением для слежки за своими гражданами.

Конечно, налоговая служба может арендовать самолет в местном аэропорту и произвести собственную аэрофотосъемку. Но поскольку спутниковые фотографии дешевле, менее противоречивы и их легко использовать в разведывательных агентствах, то их также просто использовать и в гражданских учреждениях, местных или на уровне штата.

На этой же конференции я посетил сессию, спонсированную департаментом ресурсов штата Миннесота, разработавшим в 1997 году систему наблюдения за лесными и сельскохозяйственными угодьями штата. До перехода на спутниковые данные штат использовал данные воздушного наблюдения и был счастлив, если обновлял информацию о конкретном участке раз в 10 лет. Со спутниковыми изображениями Миннесота может полностью обновлять базу данных каждый месяц.

Взимание недоимок при помощи данных 5-метрового разрешения

Шесть лет назад семья Джонсов переехала в новый, построенный по индивидуальному проекту дом в пригороде. С того времени они пристроили еще одну комнату, построили бассейн и сделали другие изменения, не потратив и цента на налоги, оплату разрешений и другие выплаты. Городская администрация не в курсе данной ситуации, поэтому она не выставила Джонсам счет и недополучила средства в бюджет.

Этот сценарий представляет распространенную проблему городских администраций. Недополученные средства в виде налогов, разрешительных и других платежей составляют миллионы долларов, которые могли бы быть направлены на реализацию важных муниципальных программ. Как же вернуть недополученные средства? Для этого можно воспользоваться представляемыми EOSAT IRS-1C данными 5-метрового разрешения.⁸²

Наблюдение за поверхностью Земли из космоса настолько всеобъемлюще и настолько просто в использовании, что спутниковые фотографии создают историю развития земной поверхности, не имеющую прецедентов в человеческой истории. Когда в 1996 году президент Клинтон рассекретил программы Corona, Argon и Lanyard, общественности стали доступны более 860 тысяч изображений земной поверхности, сделанных с 1960 по 1972 год.⁸³ Сегодня вы можете сами оценить степень ущерба, нанесенного окружающей среде во время советской власти путем сравнения изображений с системы Corona 1960 года и изображений, сделанных SPOT или IRS в 1996-м. Библиотеки спутниковых изображений становятся своеобразной машиной времени.

⁸¹ С web-сайта Space Imaging, <http://www.spaceimage.com/about-us/overview6.html#consumer>, 24 апреля 1999.

⁸² Выдержка из Government Technology Industry Profile: EOSAT (рекламный сборник), 1996. С тех пор EOSAT была переименована в Space Imaging и располагает в настоящее время изображениями с разрешением 1 метр, получаемыми со спутника IKONOS (лучше, чем данные IRS-1C). См. <http://www.spaceimaging.com>.

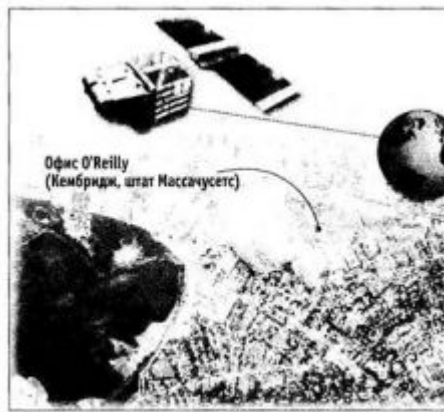
⁸³ Подробности программы рассекречивания могут быть найдены по адресу <http://edcwww.cr.usgs.gov/glis/hyper/guide/disp>. Примеры некоторых событий могут быть найдены по адресу <http://edcwww.cr.usgs.gov/dclass/dclass.html>.

Дальнейшее продвижение спутниковых изображений сдерживают две вещи. Первая – это политика. Спутниковые изображения высокого разрешения базируются на военной технологии. В течение многих лет разведывательные учреждения США всячески ограничивали доступ к этой технологии и препятствовали формальному разрешению на использование той же технологии в гражданских целях. Эту ситуацию изменили SPOT и IRS, функционировавшие за пределами США.

Старые привычки отмирают тяжело. Когда EOSAT/Space Imaging получили разрешение на запуск собственного спутника наблюдения с разрешающей способностью в 1 метр, они должны были подписать так называемое соглашение о «контроле затвора» [shutter control]. В любое время – предположительно во время военных действий – американское правительство могло закрыть затвор камеры EOSAT, перекрыв тем самым поток изображений. Конгресс США принял ограничения на спутниковые системы, в частности запретив продажу снимков высокого разрешения территории Израиля. Несмотря на то что система SPOT не попадала под юрисдикцию «контроля затвора» американского министерства обороны, она установила ограничения на доступ к изображениям в военное время: во время войны в Персидском заливе SPOT отказалась продавать изображения агентствам новостей, которые могли демаскировать перемещения войск на Аравийском полуострове, опасаясь, что иракский лидер Саддам Хусейн сможет увидеть эти фотографии и воспользоваться ими для корректировки своих планов.

Вторым ограничением является сама атмосфера Земли. Поскольку спутники используют большое увеличение, даже самые небольшие помехи в атмосфере, вызванные туманом, влажностью или тепловыми потоками играют огромную роль. Для получения чистых изображений требуется не только высокоточная оптика и сложная обработка данных, но и удача. «Существуют ли какие-либо теоретические ограничения, которые имеют практический смысл? Я бы сказал, что, вероятно, нет», – говорит Миллер из WorldSat, имеющий более чем 20-летний опыт в области гражданского применения спутниковых изображений. Миллер говорит также, что если смотреть на вещи реалистично, то мы никогда не сможем увидеть микроскопические объекты из космоса. Но, с другой стороны, постоянно появляются небезосновательные слухи о существовании сверхкачественных спутников наблюдения, которые «могут различить текст, написанный на сигаретной пачке... В прекрасный день, когда все условия способствуют этому, я, может быть, соглашусь, что вы сумеете это сделать. В общем, это в пределах технологических возможностей». Но, говоря практически, отмечает Миллер, нет смысла ввязываться в игру с поднятием разрешения: «Вряд ли вы когда-нибудь получите столь совершенные условия». Более того, разрешение гораздо менее важно, чем доступность и частота обновления изображений, т. е. возможность получить нужное изображение в нужный момент и возможность фотографировать определенный участок земного шара каждую неделю, каждый день или каждый час.

Онлайновые службы, продающие фотоинформацию со спутников, наиболее явственно иллюстрируют важность частоты обновления информации. Например, Microsoft TerraServer позволяет вам просматривать спутниковые изображения высокого разрешения (до 1,5 метра) практически любого места на планете. Все, что вам нужно, – это указать широту и долготу места. Пространственный охват просто превосходен: TerraServer охватывает большую часть земной поверхности. К сожалению, подводит временной фактор. Например, в августе 1999 года я запросил спутниковую фотографию моего квартала в Кембридже.



Вид на офис О'Рейли в Кембридже

Эта спутниковая фотография Кембриджа, штат Массачусетс, сделана советским разведывательным спутником в 1989 году, продана через SPIN-2 и загружена через Интернет с Microsoft TerraServer за \$13,95. На этой картинке, имеющей разрешение приблизительно 1,2 метра на пиксель, хорошо различимы строения, дороги, железнодорожные пути и большое белое пятно, на месте которого теперь вырос парк. Несмотря на то, что всего одна фотография высокого разрешения вроде этой является гораздо менее затратной альтернативой наземным исследованиям, истинная ценность спутниковых изображений проявляется, когда организация имеет доступ к нескольким изображениям, сделанным через несколько дней, недель или лет. Такие высококачественные изображения, доступные через Интернет, меняют в сознании людей понимание приватности во время нахождения вне помещений. [Изображение любезно предоставлено Aerial Images, Inc.]

Достаточно уверенно TerraServer выдал фотографию, сделанную спутником-шпионом еще во времена СССР. Но, увы, снимок был сделан 30 июня 1989 года. Кембридж подвергся значительным изменениям за последние десять лет, но высококачественная фотография Кембриджа, которую я заказал в Интернете за 13 долларов 95 центов, не отражала этих изменений.

Поскольку мы не стоим на месте, влияние спутниковых изображений на общество происходит в результате их комбинирования с дополнительной информацией и сложной обработкой, а не простой печати красивых фотографий для эстетического удовольствия. Привкус такого будущего мы почувствовали весной 1997 года, когда Госдепартамент США использовал спутниковую информацию, чтобы подтвердить сомнение в возможностях израильских поселенцев на Западном берегу реки Иордан и для вмешательства во внутреннюю политику этой страны. Госдепартамент заявил, что, согласно данным спутникового наблюдения, 26 % построенного еврейскими поселенцами жилья на оккупированном Западном берегу пустует, то же самое можно сказать про 56 % жилья в секторе Газа. «Нет необходимости расширять поселения, поскольку все поселенцы могут быть размещены в уже существующих помещениях», – сообщил *New York Times* неназванный представитель Госдепартамента. Эти цифры были получены путем простого сравнения данных дневного наблюдения, дающего сведения о местоположении домов, с данными ночного наблюдения в инфракрасном диапазоне, показывающего какие дома на самом деле отапливаются.

Сочетание глобального спутникового наблюдения, долговременных банков данных изображений и коммерческой доступности этой информации меняет наше представление о том, что значит пребывать на открытом воздухе. Находитесь ли вы на вершине Эвереста, плывете ли на плоту посреди Тихого океана, тайно ли хороните жертв резни или просто строите без разрешения бассейн позади дома – сегодня вы можете быть в абсолютном одиночестве, не считая глаз, постоянно наблюдающих за вами сверху.

Глаза на земле

Гораздо проще не запускать спутник-шпион, а установить камеру видеонаблюдения на столбе. Двадцать лет назад большинство людей рассматривали видеокамеры как непрошеное вторжение в их личную жизнь. Но сегодня мы все больше привыкаем к ним. Сегодня видеокамеры постоянно присутствуют в окружающем нас мире. Они установлены в магазинах, на аллеях, офисных зданиях, на улицах и даже внутри наших собственных домов. И их очень сложно обнаружить. Камеры больше не похожи на квадратную коробку с объективом с одной стороны и пучком кабелей – с другой. В наши дни большинство видеокамер устанавливается под куполом из дымчатого пластика. Существует новое поколение видеокамер, размер которых сравним с коробкой спичек. Их можно запрятать куда угодно.

Я помню, впервые столкнулся с камерами видеонаблюдения в банках и ночных магазинах в 1970-е годы в предместьях Филадельфии, где я рос. Мне не очень нравилось, что меня записывают на видеопленку каждый раз, когда я предъявляю к оплате чек или покупаю содовую, но я понимал, зачем здесь нужны эти камеры: история нашей страны богата ограблениями банков и ночных магазинов. Разумным доводом было то, что наличие этих камер давало некоторую защиту банковским кассирам и служащим ночных магазинов: даже если их убьют во время ограбления, видеозапись поможет идентифицировать и, я надеялся, привлечь преступника к ответственности. Я был уверен, что будь я служащим ночного магазина, я был бы за видеонаблюдение, несмотря на то что не менее важную роль видеонаблюдение играет в предотвращении злоупотреблений со стороны персонала.

Когда банки стали устанавливать банкоматы, вполне естественно, что и их оснастили камерами наблюдения. Когда я впервые увидел банкомат в 1979 году, мне подумалось, что камера «защищает» эту бронированную машину. И только годы спустя, когда мне довелось снимать деньги в банкомате на пустынной улице среди ночи, я понял, что камера установлена для моей безопасности.

Когда я учился на младших курсах МТИ, институт заключил договор с двумя банками на установку пары банкоматов в середине «Бесконечного коридора» [Infinite Corridor], основной пешеходной магистрали института. Это создало проблему: несмотря на то что банкоматы были необходимы институту, администрация не хотела, чтобы видеокамеры записывали каждого студента, направляющегося на занятия мимо этих банкоматов. После переговоров между банками и администрацией института камеры были наклонены таким образом, чтобы не захватывать весь проход, а на стену была нанесена надпись, извещающая, что территория находится под наблюдением.

Однако постоянное видеонаблюдение делает нас нечувствительными к нему. Несколько лет спустя камеры были возвращены «в нужную» позицию, предупредительная надпись со стены исчезла после очередной покраски и никогда больше не появлялась. Несмотря на то что теперь камеры нарушают политику МТИ в отношении видеонаблюдения: политика не допускает видеонаблюдение, когда в этом нет необходимости, и запрещает производить его без предупреждения – похоже, никого это не заботит. Одна из причин кроется в том, что это не входит ни в чьи обязанности: политика не имеет механизма реализации.

В начале 1990-х годов в городах Южной Англии стали устанавливаться камеры наружного наблюдения, присоединенные к постоянно работающим магнитофонам. Их назначение было простым: борьба с преступностью. Предполагалось, что камеры будут работать на эту цель двумя взаимодополняющими способами: записывая ограбления и уличные преступления, они создают доказательство, которое может быть позднее использовано во время следствия и судопроизводства. А поскольку камеры установлены совершенно открыто и их трудно не заметить, они должны производить сдерживающий эффект.

Одна община за другой стремились избавиться от эфемерного счастья, заключающегося в приватности ежедневных событий, происходящих в общественных местах, и заменить его постоянной видеозаписью.

В 1993 году двое детей в возрасте 10 и 11 лет увели 4-летнего мальчика по имени Джейми Балджер [Jamie Bulger] с торговой аллеи в Северной Англии. Установленные на аллее камеры безопасности записали, как старшие мальчики тащат Джейми через парковку к расположенным неподалеку железнодорожным путям, где они убили его. Видеокамера не смогла предотвратить преступление, но запись послужила доказательством для обвинения мальчиков в убийстве.

«Видеонаблюдение – очень популярное занятие сегодня в Великобритании, – говорил мне в 1998 году Джон Берджес [John Burgess], служащий отдела информации американского посольства в Лондоне. – Местные власти предписывают использовать камеры видеонаблюдения в районах с высоким уровнем преступности, и это дает хороший эффект. Например, в Cardiff City Center зафиксировано снижение уровня преступности на 13,4 %».⁸⁴ Согласно данным, опубликованным в журнале *New Scientist*, в Ньюкастле дела 1000 из 1800 задержанных при помощи системы видеонаблюдения были переданы в суд; 993 признали себя виновными, вина остальных была доказана.⁸⁵

По данным английской наблюдательной группы Privacy International, Великобритания тратит сегодня от 150 до 300 миллионов фунтов стерлингов (225–450 миллионов долларов) в год... на видеонаблюдение, включая около 300 тысяч камер, охватывающих торговые зоны, жилые массивы, автомобильные парковки и общественные места в огромном числе городов и других населенных пунктов. «...»...CCTV[p27] очень быстро стали неотъемлемой частью политики контроля над преступностью, социальной теории управления и общественного сознания. Полиция и политики преподносят эти системы как основное средство борьбы с городскими беспорядками. Без преувеличения можно сказать, что в Великобритании эта технология оказала на развитие политики правоохранительных органов большее влияние, чем любая технологическая инициатива за последние два десятилетия.⁸⁶

Камеры наружного наблюдения пришли сегодня и в США. В 1996 году в центре Балтимора были установлены оплаченные частным бизнесом камеры наблюдения. Пилотный проект включал 16 высококачественных камер, которые могли фиксировать лица людей, бронированный киоск и линейку видеомониторов. Брайан Льюбарт [Brian Lewbart], менеджер по связям с общественностью Downtown Partnership of Baltimore, признал, что центр Балтимора не является районом с высоким уровнем преступности, на самом деле он «относительно безопасен». По словам Льюбарта, действительная цель установки камер заключалась не в том, чтобы сделать район безопаснее, а в том, чтобы «общественность чувствовала себя более комфортно вследствие присутствия системы наблюдения, установленной для ее защиты».⁸⁷

После того как полицейское управление анонсировало план по установке видеокамер, многие люди стали протестовать. Но они воспротивились не видеонаблюдению за центром города, а тому, что система видеонаблюдения не была установлена там, где действительно происходят преступления, – в жилом массиве, характеризующемся высоким уровнем преступности, который находился в дюжине кварталов к северу от центра города.

⁸⁴ Из личной переписки (электронная почта), 11 апреля 1997.

⁸⁵ *News Scientist*, 12 апреля 1997 года, р. 4.

p27

Closed Circuit Television – система замкнутого телевидения, не связанного с широкоэмитерным телевидением по воздуху или по кабельной системе; общепринятое сокращение для систем охранного телевидения и видеонаблюдения.

⁸⁶ Privacy International, «Video Surveillance». См.: [http:// www.privacy.org/pi/issues/cctv/](http://www.privacy.org/pi/issues/cctv/).

⁸⁷ Интервью автору, 21 февраля 1996.

«Размещение в жилых районах еще более спорно, – говорит Сэм Рингольд [Sam Ringgold], директор полицейского управления Балтимора по общественным делам. – От домовладельцев поступило всего несколько обещаний установить камеры в жилых районах с высоким уровнем преступности. Это невозможно сделать, пока работа камер не будет протестирована в центре города в течение достаточного срока. Это также невозможно сделать без повсеместной поддержки соседних районов».⁸⁸

Фактически балтиморский проект был непродуманным. Несмотря на то что люди больше опасаются преступлений в ночное время, а не днем, камеры не были оборудованы системами ночного видения. Это были обычные серийные камеры, а не специализированные устройства высокого разрешения, применяемые в системах безопасности. Хотя камеры, возможно, и могли быть использованы для определения роста, пола и цвета кожи правонарушителя, было бы глупо полагать, что полученные видеоизображения можно действительно использовать для опознания кого-либо. Так какой цели они служили на самом деле? Как сказал Льюбарт, камеры стояли, чтобы люди чувствовали себя хорошо.

Но даже такие «успокоительные» камеры могут оказать огромную помощь. В апреле 1995 года, когда в Оклахоме был произведен взрыв в Alfred P. Murrah Federal Building, запись камеры видеонаблюдения находящегося недалеко жилого дома помогла полиции быстро установить, что бомба находилась в грузовике Ryder. Полиция обзвонила все агентства, сдававшие в прокат Ryder'bi, и вскоре получила описание внешности предполагаемых преступников. Это было реальное подтверждение больших возможностей видеонаблюдения.

Камера внешнего наблюдения

Камеры наружного наблюдения, такие как эта, установленная снаружи станции подземки Park Street в Бостоне, все более широко распространяются и становятся частью городского ландшафта. Камеры используются для мониторинга транспортных потоков, держат под присмотром входящих и выходящих из зданий людей и помогают полиции бороться с уличными преступлениями. Мировым лидером в использовании камер наблюдения является Великобритания, на территории которой установлено более 300 тысяч таких камер и почти нет ограничений на их использование. [Фотография любезно предоставлена Симеоном Гарфинкелем]



Несмотря на случайное разоблачение, большинство записанных камерами наблюдения изображений навсегда пропадают на магнитной пленке. Кстати, эта сложность поиска

⁸⁸ Интервью автору, 21 февраля 1996.

приносит обществу скрытую выгоду: за исключением некоторых первоклассных случаев, таких как размещение камеры в примерочной, просто очень сложно получить «горячие» кадры. Слишком огромен объем скучного материала, который необходимо просматривать. По крайней мере до тех пор, пока просмотром и поиском интересных фрагментов не займутся компьютеры.

Видеонаблюдение для всех остальных

Для высоких технологий естественна тенденция постепенно переходить от избранных в массы. В свое время вслед за правительствами компьютеры стали использоваться в бизнесе, а затем пришли в каждый дом. То же самое произошло и с системами видеонаблюдения. Пять лет назад разве что студенты колледжа или закоренелые холостяки устанавливали скрытые камеры для записи своих походов на пленку. Сегодня системы видеонаблюдения широко распространены на рынке: один из новомодных аксессуаров для родителей, имеющих маленьких детей – Safety 1st Day 'N Night TV Monitor System, – домашняя система видеонаблюдения стоимостью 179 долларов, состоящая из переносной видеокамеры и беспроводного приемного экрана. Монитор получает сигнал от камеры сквозь стены, этажные перекрытия и даже в соседнем здании! Продукт укомплектован «современной инфракрасной» системой ночного видения, позволяющей получать «ясное и четкое изображение как при свете дня, так и в темноте».

Хотя система разработана для того, чтобы родители могли приглядывать за спящим малышом, менеджер по продажам Boston Baby сказала мне, что большинство родителей интересуются возможностью приглядывать за няней. Они подключают приемное устройство к видеомагнитофону в спальне, закрывают ее на ключ, а камеру незаметно размещают на книжной полке в общей комнате.

Американские потребители приобрели в 1998 году видеокамер на 2,4 миллиарда долларов; всего в магазины было отгружено 3,83 миллиона видеокамер.⁸⁹ Эти дешевые камеры стали играть роль средств массовой информации и полиции, позволяя рядовым гражданам записывать на видеопленку доказательства в реальных условиях в своих кварталах. Скрытно сделанные видеозаписи могут влиять на общественный порядок и менять течение национальных событий, ярким подтверждением чего является позорная домашняя видеозапись избиения Родни Кинга [Rodney King] полицией Лос-Анджелеса.

В конечном счете более существенным, чем снижение стоимости и широкая продажа систем видеонаблюдения, стало изменение выдаваемого камерой видеосигнала. Камеры прошлых лет имели выход в формате Национального комитета по телевизионным стандартам [National television Standards Committee, NTSC], аналогового видеосигнала, хорошо подходящего для мониторов CCTV и записи на видеопленку. Современные камеры выдают цифровой сигнал, который легко можно ввести в домашний компьютер. После помещения в компьютер, изображениями можно манипулировать и сохранять их, как и любой другой вид цифровой информации. Цифровые камеры выпускают на свободу информацию, которая до настоящего времени томила на миллионах миль видеопленки, и делают эти изображения доступными.

Камера Connectix QuickCam была первой цифровой видеокамерой, заполнившей рынок домашних пользователей. Похожую на Пластиковый теннисный мяч с хвостиком, QuickCam можно было подсоединить к любому настольному или переносному компьютеру. QuickCam поставлялась с маленьким треугольным основанием, позволявшим установить ее на мониторе компьютера; на ней имелось также отверстие для прикрепления к стандартному штативу. Достаточно было присоединить ее к компьютеру, запустить программу, и вы получали свою собственную миниатюрную видеостудию. Вместо видеопленки система

⁸⁹ Consumer Electronic Manufacturing Association, Arlington VA.

использовала жесткий диск компьютера; для сохранения одной минуты видеозаписи требовалось около 6 мегабайт дискового пространства. Другим фактором, способствовавшим ее популярности, была ее приемлемая цена, снизившаяся с 200 до 99, а затем и до 79 долларов всего за три года с момента выпуска.

QuickCam мгновенно стала популярной. Миллионы пользователей компьютеров получили дешевую и простую возможность иметь на компьютере статические изображения и видеофрагменты.

Когда я купил QuickCam, первая вещь, которую я сделал, – снял экскурсию по своему дому и послал видеозапись по электронной почте другу в Калифорнию, который никогда не видел моего дома. Конечно, я мог сделать это и с обычной видеокамерой, но тогда мне пришлось бы посылать кассету, а ему искать телевизор и видеомагнитофон для ее просмотра. Благодаря цифровой QuickCam видеоизображение просто отправилось через Интернет с моего компьютера на компьютер приятеля.

Вскоре мы с женой нашли еще одно применение для QuickCam. Мы решили узнать, чем занимаются в наше отсутствие наши кошки, поэтому однажды в воскресенье мы оставили QuickCam включенной, а сами отправились позавтракать. Программное обеспечение Connectix имеет специальный режим обзорной записи: вместо обычных 10 или 15 кадров в секунду компьютер программируется на запись одного кадра в секунду или даже одного кадра в 15 секунд. Это позволило нам записать целый час всего на 6 мегабайтах дискового пространства и просмотреть часовую запись за несколько минут.

Мы узнали, что кошки живут своей собственной жизнью. Просматривая запись нашей самодельной системы наблюдения, мы увидели их запрыгивающими на стол в гостиную. Мы видели их спящими на этом столе. Мы видели, как они чешут когти об обивку мебели. Мы видели, как они читают наши книги, роются в ящиках стола, копируют номера кредитных карт с чеков в мусорной корзине, заказывают по почте корм для кошек Gourmet, а потом хулиганят по телефону, звоня соседской собаке. А что мы могли ожидать? Они же кошки в конце концов.

Однажды мы с Бет попробовали продать нашу квартиру в Кембридже и в ближайшее воскресенье устроили день открытых дверей. Агент по продаже попросила нас покинуть дом в полдень и возвратиться приблизительно в 15 часов. Она обещала обо всем позаботиться. Мы уже так поступали до этого дважды, и каждый раз агент давала нам скучный и неподробный отчет о двух-трех парах, осмотревших наш дом. На этот раз мы решили выяснить для себя, в чем же дело, и оставили QuickCam включенной, не сообщая об этом агенту по продажам, конечно. Мы просто включили компьютер, настроили его на запись, как это было в случае с нашими кошками, и выключили монитор. Это было так просто сделать! Мы узнали, что агент позволяла людям ходить по дому без сопровождения, в то время как она сама сидела в гостиной и читала книжку. После этого мы решили не устраивать больше дней открытых дверей.

Web-камера

Гораздо интереснее, когда вы делаете изображения с цифровой видеокамеры доступными через Интернет в реальном времени. Внезапно камера превращается из простого средства видеонаблюдения в потенциальные глаза и уши миллионов людей на планете.

Первая интернет-видеокамера была установлена в 1991 году в компьютерной лаборатории Кембриджского университета и показывала кофейник в «Троянской комнате» [Trojan Room Coffee Pot]. Пятнадцать аспирантов пользовались одним кофейником, расположенным на втором этаже лаборатории, называемой «Троянская комната». Кофейник был удобен для аспирантов, работающих на втором этаже. Проблема заключалась в том, что аспиранты на других этажах не знали, когда будет готов кофе. Конечно, они были слишком заняты (и немного ленивы), чтобы пойти на второй этаж, включить кофейник и подождать, пока кофе приготовится. Они хотели знать, когда *кто-нибудь другой* в здании возьмет на

себя тяжкий труд включить кофейник, чтобы после быстренько налететь и насладиться кофе.

Аспиранты нашли старую видеокамеру и вспомогательный компьютер с устройством ввода видеосигнала. Пол Джардецки [Paul Jartzky] написал программу, которая получала изображение с устройства ввода видеосигнала каждые несколько секунд. Квентин Стаффорд-Фрейзер [Quentin Stafford-Fraser] написал другую программу под названием XCoffee,^[p28] которая связывалась с программой Джардецки по сети и выводила изображение кофейника на экран компьютера. «Картинка обновлялась всего лишь три раза в минуту, но это было неплохо, так как кофейник наполнялся довольно медленно; она была также черно-белой, что тоже было достаточно», – писал Стаффорд-Фрейзер на web-странице, посвященной проекту.

Кофейник стал приобретать некоторое количество поклонников по всему миру. Боб Меткалф [Bob Metcalf] написал о нем в выпуске *Comm Week* от 27 января 1992 года. Как он сообщал, копию XCoffee загрузили 600 человек, которые теперь тоже могли наблюдать кофейник. Но программа работала только на рабочих станциях под управлением UNIX, что несколько ограничило ее распространение. Когда вспомогательный компьютер внезапно вышел из строя, аспиранты Дэниэль Гордон [Daniel Gordon] и Мартин Джонсон [Martin Johnson] возродили систему на новом оборудовании и поместили изображение кофейника непосредственно на свою web-страницу.⁹⁰

Это привело к существенным изменениям. До расцвета Всемирной паутины, единственным способом увидеть кофейник в «Троянской комнате» было загрузить программу XCoffee и запустить ее. Поскольку программа имела только одну функцию, то сомнительно, что результат оправдывал затраченные усилия. Другая проблема была в том, что XCoffee могла работать только на некоторых типах рабочих станций UNIX. Но помещение изображения на web-страницу привело к тому, что любой обладатель web-браузера мог просмотреть его путем простого щелчка мышью на ссылке. Web-браузер не нуждался в специальной модификации для показа изображения: с точки зрения браузера, нет никакой разницы между изображением кофейника и фотографией президента США на web-странице Белого дома.

Работа Гордона принесла результат: согласно сообщению BBC, 11 ноября 1994 года более 150 тысяч человек активировали ссылку на кофейник в «Троянской комнате», с момента первого появления изображения во Всемирной паутине. Это было рождением web-камер.

В течение следующих двух лет web-камеры стали распространяться по всему миру. Одна из первых web-камер, установленная OpenMarket в Кембридже, штат Массачусетс, показывала панораму Бостона. C|Net, комбинируя трансляцию по сетям кабельного телевидения и web-сайт, установила web-камеру, позволявшую посетителям сайта подглядывать за тем, что творится в телевизионных студиях компании. Farm.net, интернет-провайдер из Нью-Гемпшира, установил «цыплячью камеру», которая была направлена на клетку с цыплятами. Была и обманная «туалетная» камера, которая постоянно показывала изображение туалета. Люди заходили на сайт в надежде поймать кого-нибудь «на горшке». А потом появилась JenniCam, камера, установленная в спальне и домашнем кабинете ее владельца – web-дизайнера-эксгибициониста. Вы можете бесплатно увидеть Дженифер Рингли [Jennifer Ringley] по адресу www.jennicam.org с частотой обновления 20 минут или с частотой обновления каждые 2 минуты за абонентскую плату 15 долларов в год.

В 1994 году журналист BBC Майкл Айзексон [Michael Isaacson] взял у Дэниэля Гордона интервью о камере в «Троянской комнате». Перед началом интервью Гордон сидел

p28

Обычно с приставкой «X» именуют программы, разработанные для функционирования в X-Window – графической среде, распространенной в UNIX-подобных операционных системах.

⁹⁰ Домашняя страница Trojan Room Coffee Pot находится по адресу <http://www.cl.cam.ac.uk/cgi-bin/xvccoffee>.

за своей клавиатурой и что-то печатал. «Все, что мне нужно сделать, это нажать на кнопку „кофеварка“... и в конечном счете... я получу картинку на экране моей рабочей станции... и, похоже, кто-то уже выпил весь кофе. Так что, я полагаю, мне придется сделать его самому».

Репортер ВВС был в некотором недоумении. Он спросил Гордона: «Может быть, надо было сделать картинку покрупнее, чтобы Вы могли увидеть, кто выпил кофе?»

«Да, но я думаю мы должны защитить виновных», – ответил аспирант.

JenniCam

Дженифер Рингли живет под наблюдением. Находясь в своей квартире в Вашингтоне, федеральный округ Колумбия, она спит, просыпается, ест и работает под неусыпным взглядом нескольких видеокамер, постоянно транслирующих поток изображений во Всемирную паутину. Изображение обновляется каждые 20 минут и доступно бесплатно. Да, здесь присутствуют обнаженная натура и секс, хотя это не является целью создания этого сайта. Это часть жизни Рингли. Хотя официально она зарабатывает на жизнь web-дизайном, тысячи людей платят абонентскую плату в размере 15 долларов в год, чтобы получить улучшенный доступ – изображение в этом случае обновляется каждые 2 минуты, вместо 20. [Фото любезно предоставлено JenniCam]

Фактически, оставляя изображение маленьким, Гордон и его коллеги делали гораздо больше, чем просто «защиту виновных». Сопrotивляясь искушению превратить устройство мониторинга кофеварки в систему видеонаблюдения общего назначения, они защищали общественное устройство своего сообщества. Запись лиц «кофейных воришек» положила бы конец этой практике, но она также разрушила бы и дух товарищества, который был создан частично благодаря общественной кофеварке.



От Web-камеры к камере-одежде [p29]

Web-сайт Вашингтонского транспортного управления [Washington State Department of Transportation, WSDOT] показывает информацию о текущей загруженности магистралей вокруг озера Вашингтон. Идея заключается в предоставлении водителям возможности получить информацию о пробках, чтобы попытаться избежать их. Отображаемая на сайте

p29

В оригинале присутствует игра слов, так как слова webcam (web-камера) и wearcam (камера-одежда) близки по звучанию.

информация собирается с магнитных рамок, встроенных в покрытие магистралей и с более чем 200 отдельных видеокамер, установленных по всей системе магистралей. В 1996 году видеопоток с 45 из этих камер направлялся непосредственно на web-сервер WSDOT, позволяя любому пользователю Интернета посмотреть через их объективы.

WSDOT установило видеокамеры и магнитные рамки на магистралах еще после постройки в 1960-е годы Interstate 5, рассказывает инженер транспортного управления Махрок Арефи [Mahrokh Arefi].⁹¹ Но до появления Всемирной паутины не было простого способа сделать эту информацию общедоступной. Сегодня все изменилось.

Значительная часть этих камер подключена сегодня к большому видеокоммутатору в принадлежащем WSDOT Центре управления движением Северо-западного региона на севере Сиэтла. Заполняющие стены Центра видеомониторы позволяют инженерам быстро локализовать проблемы с движением и информировать о них общественность при помощи сообщений об обстановке на дорогах. Центр также может включить специальные светофоры, ограничивающие приток новых автомашин на магистраль.

Многие камеры имеют индивидуальное управление: их можно наклонить, повернуть, изменить увеличение, позволяя обслуживающему персоналу Центра управления движением вести подробное наблюдение за дорогой. Поток видеоинформации дублируется в полицию штата. Изображение с камер, установленных в тоннеле, также записывается на видеокассеты. Основное предназначение записи, по словам Арефи, в том, чтобы представить доказательство в случае, если служащий WSDOT будет ранен или сбит машиной.

Парадоксально, но как только появилась возможность сделать изображения с камер наблюдения более широкодоступными, WSDOT приняло решение сделать их менее полезными. Предоставив видеопоток в распоряжение телевизионных станций Сиэтла, WSDOT проинструктировала операторов не делать увеличение отдельных машин, особенно ставших участниками дорожного происшествия. Доступность видеоизображения через Интернет лишь подтвердило правильность этого решения. WSDOT не хочет, чтобы жители Вашингтона думали, что за ними следят. В размещенных на сайте ответах на часто задаваемые вопросы любопытным поясняется, что камеры имеют недостаточное разрешение, чтобы прочесть номер машины и что, несмотря на предоставление видеоинформации вашингтонской дорожно-патрульной службе, «она не используется для записи в интересах правоохранительных органов».⁹²

Аналогично, говорит Арефи, были удалены видеомэгнитофоны. Очевидно, они никогда не использовались в юридической практике. Видео пленка является потенциальным подтверждением ответственности WSDOT в случае, если водитель попал в аварию по вине управления.

Там, где правительства ступают с опаской, обычные граждане уверенно движутся вперед. Как только средства видеоконтроля стали широко доступны, граждане начали активно их использовать, подтверждая аксиому, что солнечный свет – лучшее средство обеззараживания. В мае 1997 года Мартин Майноу [Martin Minow] поместил в *RISK Digest* сообщение о том, что норвежская газета *Nettavisen* сообщала о web-камере, установленной у входа в бордель.⁹³ Такая камера не нарушает норвежское законодательство до тех пор, пока номера машин и личности людей, попавших в поле ее зрения, не разглашаются, заявлялось в статье.

⁹¹ Интервью автору, май 1997.

⁹² Часто задаваемые вопросы: <http://www.wsdot.wa.gov/regions/northwest/NWFLOW/camera/camfaq.htm>, 9 апреля 1997.

⁹³ Martin Minow, «Норвежская камера наблюдения», *RISK Digest* 19:13. Доступно в Интернете по адресу <http://catless.ncl.ac.uk/Risks/19.13.html#subj8.1>.

В Сан-Франциско независимый видеопродюсер, чья студия находилась на сложном пересечении улиц, устал наблюдать, как машины проезжают на красный свет на перекрестке 11-й улицы и Хоуворд и попадают в аварию. Он установил резервную видеокамеру на постоянную запись происходящего на перекрестке. Теперь всякий раз, когда он наблюдает столкновение, особенно если вред нанесен пешеходу, он спускается вниз и предлагает пострадавшему копию видеозаписи.⁹⁴

Кульминацией распространения систем видеонаблюдения стала камера-одежда, новое поколение видеокамер, которую человек носит на теле и использует для непрерывной передачи видеоизображения своего окружения. Многие писатели-фантасты писали о такой технологии. В романе «Лавина» [*Snow Crash*] Нил Стивенсон [Neal Stiphenson] изобразил людей-«горгулий», которые записывали все, что видели вокруг, и загружали эту информацию в огромный банк данных Центральной разведывательной корпорации, рассчитывая, что она кому-нибудь понадобится и за нее заплатят. В книге «Земля» [*Earth*] Дэвид Брин [David Brin] пророчит появление видеоочков True-Vue,^[p30] записывающих все, что видит их владелец, и передающих информацию на расстояние как мобильная система видеонаблюдения.

Мобильные видеокамеры с радиоканалом уже не являются предметом научной фантастики: они вполне доступны сегодня. В бытность свою аспирантом лаборатории сред Массачусетского технологического института в начале 1980-х Стив Манн [Steve Mann] начал носить видеокамеру, смонтированную на его голове. Камера была присоединена к радиопередатчику, посылавшему изображение на web-сервер, где картинка отображалась под заголовком «Посмотрите, что я вижу сквозь мои очки прямо сейчас (или во время последней передачи)».

Тогда же Манн поместил на свою шляпу маленькую карточку, содержащую следующее предупреждение.

Для вашей защиты видеозапись Вас и Вашего окружения может быть
передана и сохранена в удаленном месте.
ВСЕ ПРЕСТУПНЫЕ ДЕЙСТВИЯ НЕ ОСТАНУТСЯ
БЕЗНАКАЗАННЫМИ!!!

Видеокамера причиняла Манну массу неудобств в магазинах, банках и других организациях, чьи правила запрещают посетителям вести фото- и видеосъемку. Контроль над средствами наблюдения – способ поддерживать власть. Власть, которой магазины не спешат делиться с клиентами.

Возня вокруг выключателя питания

Энтузиасты видеонаблюдения, такие как Брин и Манн, считали, что со временем видеокамер будет все больше и больше. А в мире, заполненном видеокамерами, утверждали они, у нас всего два варианта: либо камеры целиком и полностью находятся под контролем правительства и бизнеса, либо они свободны и доступны для использования каждым.

Эволюция ходячей web-камеры Стива Манна

⁹⁴ *All Things Considered*, National Public Radio, 12 мая 1997.



Оборудованный видеокамерой на батарейках, переносным компьютером и устройством беспроводного подключения к Интернету, Стив Манн является чей web-камерой, или камерой-одеждой, как он сам предпочитает ее называть. Стив Манн, сегодня профессор электротехнического факультета университета Торонто, за последние десять лет носил несколько разных в своего электронного приспособления. «Око за око – это справедливо», – утверждает Манн, имевший серьезные проблемы с торговцами вроде MIT имеющими установленные повсюду камеры наблюдения, но запрещающих своим клиентам вести съемку в своих магазинах. Большинство исследовательских работ Манна связано с программным управлением движением камеры, например технологии восстановления дополнительной информации, увеличения разрешения, построения большого изображения путем комбинирования нескольких маленьких. [Фото любезно предоставлено Стивом Манном]

Но, к сожалению, этот утопичный анализ антиутопичного будущего не учитывал простых экономических соображений. Даже при постоянном снижении цен кто-то должен платить за все эти технологические новинки. И именно люди, платящие по счетам, будут определять, куда именно будут направлены камеры. Результаты эксперимента в Великобритании подтверждают это: видеокамеры не одинаково смотрят на разные сообщества и на разных индивидуумов.

В 1997 году Центр криминологии и уголовного права [Centre for Criminology and Criminal Justice] Тульского университета в Великобритании изучил 888 зафиксированных системой видеонаблюдения случаев, когда оператор мог управлять движением камеры или картинкой на мониторе. В результате исследования было установлено, что камеры «систематически и непропорционально» фокусируются на молодых мужчинах с черным цветом кожи, «не потому, что они стали участниками преступления или нарушения порядка, а „без очевидных причин“», кроме их возраста и расовой принадлежности.⁹⁵ Исследователи также установили, что 10 % женщин были сняты камерой исключительно по «вуайеристским» причинам, а 40 % попавших под мониторинг людей были выбраны лишь по причине их расовой и этнической принадлежности. В отчете говорится:

Камера неравномерно обращает свой взор на прохожих, она фокусируется на тех, кто вследствие стереотипности мышления определяется как потенциально опасный, либо из-за внешнего вида и поведения выбирается оператором как нереспектабельный. В результате этого молодежь, особенно социально и экономически неустроенная, становится субъектом авторитарного вмешательства и общественной неприязни. Вместо обеспечения социальной справедливости путем снижения насилия, CCTV-системы через усиление разделительной и дискриминационной политики просто станут средством несправедливости.

Генеральный директор Privacy International Саймон Дэвис [Simon Davies] на слушаниях в палате лордов в 1997 году по вопросу воздействия постоянного видеонаблюдения заявил:

Во-первых, я глубоко уверен, что непредвзятость этой технологии показная, непроверенная и основывается в значительной степени на эмоциональных соображениях. Заявления о влиянии CCTV-систем на уровень и состав

⁹⁵ Clive Norris and Garry Armstrong, «The Unforgiving Eye: CCTV Surveillance in Public Space», Centre for Criminology and Criminal Justice, University of Hull, Hull HU6 7RX, U.K. Цитируется по «Prejudice Drives CCTV Targets», KDIS Online, 24 октября 1997. Доступно в Интернете по адресу <http://merlin.legend.org.uk/~brs/archive/stories97/Suspects.html>.

преступлений часто преувеличены и упрощены. Например, преступления на почве ревности, преступления, связанные с наркотиками и алкоголем, и действия профессиональных преступников редко предотвращаются камерами. Вообще говоря, технология очень слабо влияет на снижение числа «спонтанных» преступлений.

Во-вторых, основное влияние этой технологии на поведение людей касается больше общественного порядка, чем противоправных действий. Практически большинство систем видеонаблюдения борются с «антисоциальным поведением», включая оставление мусора, справление малой нужды в парках, курение малолетних, нарушение правил дорожного движения, надписи на стенах, драки, обструкцию, пьянство, непристойное поведение и обман счетчиков на парковках. Конечно, найдутся аргументы, что именно на эти цели ориентирована данная технология, но слишком малая часть общественности ассоциирует CCTV-системы с такими проступками.

Наконец, я уверен, что данной технологии присущ целый ряд отрицательных моментов, о которых не сообщается. Я лично могу засвидетельствовать, что операторы постоянно дискриминируют людей из-за своих личных предубеждений по расовой принадлежности, возрасту, классовой принадлежности и сексуальным предпочтениям. Результаты проведенного недавно Тульским университетом исследования подтверждают эту точку зрения. Несколько высококлассных случаев неправильного использования этой технологии и полученных изображений внесли свой вклад в склонение общественного мнения к поддержке технологии. CCTV-системы являются также ключевым фактором, вызвавшим целый ряд изменений в деятельности полиции. Эти изменения, включая смещение практики с упреждающей на реагирующую, еще не были адекватно изучены и оценены.⁹⁶

В своей речи Дэвис высказал определенные возражения против компьютеризованного распознавания лица, миниатюрных видеокамер, разработанных для скрытного наблюдения, и высокочувствительных камер, таких как Forward Looking Infrared Radar, которые могут видеть в темноте, а в некоторых случаях и сквозь стены.

Повсеместное одобрение технологий видеонаблюдения не является неизбежным. Даже использование миниатюрных камер может регулироваться, если общество захочет этого.

Несмотря на то что видеонаблюдение невозможно полностью уничтожить, строгие наказания вкупе с давлением общественности будут еще одним шагом на длинном пути минимизации этой практики. Например, Мартин Майноу сообщал в *RISK Digest*, что видеокамера, установленная в одном из шведских ресторанов, была принудительно отключена шведским Агентством по защите информации [Data Protection Agency]. В Канаде визит члена Комиссии по обеспечению приватности Британской Колумбии в новую публичную библиотеку в Ванкувере привел к тому, что объем видеонаблюдения был существенно снижен, а общественность стала информироваться о производимом наблюдении.

Вернемся к Великобритании. Саймон Дэвис предложил несколько простых мер регулирования использования данной технологии, включая следующие:

- позволить местным органам контролировать установку камер видеонаблюдения в городе;
- расширить британское законодательство в области защиты данных, чтобы органы по защите данных «напрямую извещались об установке и запуске систем»;
- установить минимальные требования к подготовке операторов камер наблюдения;
- запретить продажу или трансляцию изображений из систем наблюдения.

Эти рекомендации могут также неплохо работать и в Соединенных Штатах. Без этих

⁹⁶ Simon Davies, «Summary of Oral Evidence of Simon Davies», 23 октября 1997. Доступно в Интернете по адресу http://www.privacy.org/pi/issues/cctv/lords_testimony.html.

рекомендаций наше общество рискует сделать видеонаблюдение свободно доступным для всех.

Что это было?

Звук кардинально отличается от света. На физическом уровне свет состоит из частиц, называемых *фотонами*, которые перемещаются сквозь пространство. В отличие от света, звук представляет собой волны давления, распространяющиеся в газе, твердом веществе или жидкости. Свет существует вне среды, звук без среды существовать не может. Это ключевое различие имеет большое практическое значение. Звук записать гораздо проще, чем изображение, но очень сложно это сделать на расстоянии. Это происходит потому, что световые волны распространяются по прямой линии, а звуковые – рассеиваются и отражаются.

Чтобы проверить эту разницу на практике, отправьтесь в парк в теплый солнечный день. При помощи небольшой подзорной трубы вы сможете наблюдать за маленьким семейным пикником в четверти мили от вас. Вы сможете разглядеть, что семья ест и насколько хорошо ведут себя дети. Но если вы захотите подслушать беседу, вам, очевидно, придется подкрасться и установить скрытый микрофон. Фоновые шумы в сочетании с тем фактом, что звуковые волны быстро затухают при распространении, обеспечивают нам некоторую степень «акустической приватности» даже в общественных местах.

Неудивительно, что большинство методик акустического наблюдения подразумевают в той или иной степени физическое вмешательство. Иногда такое вмешательство чрезвычайно трудно обнаружить. В 1946 году советские школьники подарили американскому послу в СССР Авереллу Гарриману [Averell Harriman] вырезанный из дерева большой герб Соединенных Штатов. Посол был так растроган, что повесил этот герб в своем кабинете в здании посольства в Москве. Но он не знал одной вещи: герб был с «начинкой». Шесть лет спустя агенты спецслужбы обнаружили, что внутри подарка находились скрытый микрофон и антенна. Направляя на устройство высокочастотный сигнал [\[p31\]](#) советская разведка могла прослушивать все переговоры посла.

В 1966 году сенатор Эдвард Лонг [Edvard V. Long] в своей книге «Захватчики: вторжение в личную жизнь правительств и бизнеса» [*The Intruders: The Invasion of Privacy by Government and Industry*] выразил негодование по поводу широкого спектра доступного современного подслушивающего оборудования. Возглавляя подкомитет сената по вопросам неприкосновенности частной жизни, Лонг одним из первых мог ознакомиться с самым передовым подслушивающим оборудованием. Для обеспечения жучками вечеринки имелись миниатюрные микрофоны с передатчиком, камуфлированные под оливку на палочке; они могли передавать сигнал на приемник, расположенный в квартале от этого места. Для прослушивания жилой комнаты существовал так называемый spike mike, монтируемый на конце дротика. Устройство выстреливалось из винтовки с расстояния в четверть мили, и, воткнувшись в подоконник, оно начинало передавать все, что слышало.

Лонг также установил, что эти технологии использовались всеми без разбора: правительственными агентствами, например Управлением по контролю за пищевыми продуктами и лекарственными препаратами США, бизнесменами и даже просто любопытными людьми. В конечном счете в результате повышенного внимания Капитолийского холма к этому вопросу были приняты ограничения на использование средств электронной разведки, ставшие в 1968 году частью законодательного акта – Omnibus Crime Control and Safe Streets Act. [\[p32\]](#)

p31

В отечественной литературе этот метод обозначают термином «высокочастотное навязывание».

p32

Сводный закон о контроле над преступностью и обеспечении безопасности на улицах. Первый

Сегодня достижения в области цифровой обработки сигналов делают физическое присутствие для установки жучков менее важным. Широко известно, что разговор в современном офисном здании может быть перехвачен при помощи лазерного луча, который, отразившись от окна помещения, будет промодулирован звуковыми волнами. Разведывательные трюки, вроде использованного советской разведкой против американского посла, работают и сегодня. Но современная техника позволяет получать полезный радиосигнал, отражающийся от металлических объектов уже находящихся в помещении, не привлекая младших школьников для вручения вашей жертве резного американского орла.

Технологии подслушивания широко доступны на массовом рынке. Например, в феврале 1997 года *New York Times Magazine* опубликовал рекламу о распродаже PowerVox IV, мощного направленного микрофона стоимостью 39 долларов 95 центов: «Поместите PowerVox IV в карман рубашки и к вашему изумлению вы обнаружите, что можете слышать шепот на расстоянии 15 метров, звук упавшей булавки на расстоянии около 3 метров и даже разобрать, о чем говорят люди в соседней комнате».

Что действительно нужно, так это не принятие новых законов, а лишь обеспечение исполнения уже написанных. Простые люди, бизнес и правительство должны усвоить, что подслушивание незаконно и аморально.

Когда в 1994 году в Ванкувере открылась новая публичная библиотека, ее посетители не предупреждались, что все их действия контролируются 34 видеокамерами и большим количеством скрытых микрофонов. Основные зоны, подвергаемые жесткому контролю, – входы, выходы и зоны возле детских ванн комнат. Системы акустического контроля разработаны таким образом, чтобы услышать крик человека, подвергшегося нападению на автостоянке, или инвалида, который может упасть в санузел. Идея сама по себе хорошая, кроме того факта, что общественность не предупреждается о наличии системы контроля.

Дешевые подслушивающие устройства

Оборудование для подслушивания дешево, легкодоступно и неподконтрольно. На рекламном листке в настоящее время уже несуществующей компании Sheffield Electronic Company представлен миниатюрный FM-передатчик, имеющий размер втрое меньше 9-вольтовой батарейки, питающей его. Скрытно установленное в доме или машине, такое устройство может в течение недели и более передавать сигнал, который можно принять на расстоянии более 300 метров. Другая модификация получала питание от телефонной линии. [Рекламный листок предоставлен Sheffield Electronic Company]



Уже скоро появятся принципиально новые типы аудиомониторинга, которые не укладываются в существующие рамки. Это широкомасштабный мониторинг, сочетающий телекоммуникации с процессом обработки данных для обнаружения, определения местоположения, классификации и постоянной записи любых событий, считающихся подозрительными.

В 1993 году городок Редвуд-Сити, штат Калифорния, понял, что имеется проблема с оружием. «Люди стреляли в воздух в сторону других людей. Группы людей разъезжали на машинах и стреляли в дорожные знаки. Некоторые люди разряжали оружие на внутренних дворах [и] внутри домов», – рассказывает Уорд Хэйтер [Ward Hayter], заместитель уполномоченного по связям со СМИ городской полиции.⁹⁷

Некоторые люди, услышав выстрелы, вызывали полицию, но никто из граждан не мог точно сказать, откуда была стрельба. Городские власти решили прекратить это и поручили доктору Роберту Шоуэну [Robert Showen] из Trilon Technology сконструировать детектор и локатор выстрелов.

Три года спустя прототип системы стоимостью 25 тысяч долларов был готов к внедрению. Система состояла из восьми микрофонов, размещенных в полуторамильной зоне. Микрофоны были установлены на зданиях и высоких точках. К каждому микрофону вела выделенная телефонная линия. Микрофон улавливал окружающие его шумы и посылал звуковую информацию в полицейское управление, где звуки анализировались рабочей станцией Sun Microsystems. Компьютер осуществлял цифровую фильтрацию звука и определял, не является ли он звуком выстрела. Если он считал, что это выстрел, то фиксировал точное время, когда звук был услышан каждым микрофоном, и использовал эту информацию для расчета точки выстрела. Через 45 секунд система показывала место выстрела на карте города. После этого полиция посылала туда патрульную машину, задолго до того, как кто-нибудь позвонит 911.

«Система имела точность определения выстрела 60–70 % и могла определить его местонахождение с точностью 10–20 метров», – говорит Хэйтер. Часто система слышала и локализовывала выстрелы, произведенные внутри домов и других строений. Хэйтер сказал также, что «один или два случая задержания связаны с выстрелами», которые обнаружила система. Но основная отдача от системы заключалась, по его утверждению, в сдерживающем факторе: «Она предотвратила большое количество выстрелов в нашем сообществе», – заявил он вполне уверенно, хотя и не смог представить каких-либо статистических данных в подтверждение своего утверждения.

⁹⁷ Интервью автору, 9 мая 1997.

В 1967 году Верховный суд США по делу «Кац против США»⁹⁸ определил, что полиция не может устанавливать микрофон для осуществления прослушивания разговора по общественному телефону без специального постановления. Но детектор выстрелов не прослушивал определенный разговор: он слушал то, что свободно доступно для прослушивания каждому. Более того, он не производил записи разговоров. Учитывая эти ограничения, система не попадает под определение Верховного суда 1967 года.

Несмотря на это, сама идея установки полицией микрофонов по всему городу для обнаружения криминальных действий чем-то напоминает «1984» Джорджа Оруэлла. Я спросил Хэйтера, не протестовали ли люди по поводу нарушения их приватности. «Мы не получили ни одного заявления по поводу нарушения права на неприкосновенность частной жизни», – ответил он. Для начала, сказал он, у полиции просто не было возможности увеличить уровень громкости сигнала от микрофонов, чтобы прослушивать разговоры на улицах. «Вы не смогли бы ничего понять, – говорит Хайтер. – Это просто телефонная линия, идущая к микрофону-датчику... Для того чтобы имело место какое-либо нарушение приватности, надо было бы подняться на здание и вести разговор непосредственно перед микрофоном... Прослушивание разговоров не было целью создания системы».

Но другая названная им причина, по которой никто не жаловался на нарушение приватности, более существенна: «Большинство датчиков расположено на зданиях, и они себя никак не обозначают: широкая публика просто не знает, где они находятся».

Систематическое научное наблюдение

Получение изображений со спутника, наземные видеокамеры и микрофоны, конечно, самые очевидные инструменты для наблюдения, но они не единственны в своем роде. Все шире для наблюдения начинают использоваться высокоточные научные методы.

Международные соглашения, направленные на ограничение и сокращение вооружения, неизменно влекут за собой усиление мониторинга нашей планеты. Один из хороших примеров – многостороннее соглашение о запрещении ядерных испытаний, подписанное 24 сентября 1996 года в ООН президентом Клинтоном. Это соглашение, являющееся результатом 40-летней борьбы за запрет испытаний ядерного оружия, подразумевает создание сложнейшей международной системы мониторинга для отслеживания на планете небольших ядерных взрывов, которые были бы нарушением соглашения.

Система мониторинга включает в себя основную и вспомогательную сейсмические сети, сеть мониторинга радионуклеотидов, гидроакустическую сеть, инфразвуковую сеть и инспектирование ядерных объектов. Сейсмическая сеть разработана для обнаружения взрывов, которые вызывают рукотворные «землетрясения» силой 4,25 балла и выше по шкале Рихтера, и способна указать его местонахождение с точностью до 1000 квадратных километров (окружность радиусом 18 километров). Для сравнения: испытание относительно небольшого 10-килотонного ядерного заряда, произведенное в Китае 29 июля 1996 года, вызвало колебания силой 5,2 балла.⁹⁹

Кто будет обеспечивать работоспособность сети? Ученые, которые уже осуществляют мониторинг Земли с другими целями.

Объединенный институт сейсмологических исследований [The Incorporated Research Institution for Seismology, IRIS] называет себя «университетским исследовательским консорциумом, созданным для исследования внутренней структуры Земли путем сбора и распространения сейсмографических данных». IRIS располагает сетью из более чем 50

⁹⁸ *Katz v. U. S.*, 389 U.S. 347 (1967).

⁹⁹ «CTBT... At last!», Incorporated Research Institution for Seismology, IRIS Newsletter, vol. XV, no. 3, Fall 1996, p. 1–3.

расположенных по всему миру сейсмологических станций и финансируется Национальным научным фондом США [United States National Science Foundation] и Центром научных исследований Военно-воздушных сил [Air Force Office of Scientific Research]. Организованный в 1984 году 26 университетами, к 1997 году IRIS стал некоммерческим консорциумом, членами которого являются более 90 учреждений.

Члены IRIS знают, что их сеть имеет двойное назначение: научное и военное. Информационные письма этой организации содержат статьи о сотрясениях земной поверхности, имеющих как естественную природу, так и искусственное происхождение. Это ученые с определенной миссией.

Весной 1995 года IRIS получил необычный запрос из Сената США. Террористическая организация Аум Синрике 20 марта выпустила нервно-паралитический газ зарин в токийском метро, в результате погибло 12 человек, а более 5 тысяч получили отравление. В результате последующего расследования было установлено, что секта имеет своих последователей и в западной Австралии.

Постоянно действующий подкомитет сената по расследованиям интересовало событие, имевшее место в западной Австралии 28 мая 1993 года. В тот вечер, в 23 часа по местному времени, станция мониторинга зафиксировала «толчок силой 3,6 балла на глубине 1 километр». Находившаяся неподалеку группа местных геологоразведчиков рассказывала о «похожем на звезду объекте на горизонте». Объект набрал скорость подобно самолету и исчез. Затем разведчики увидели внезапную сильную вспышку и услышали звук взрыва, длившийся несколько секунд. «Несколько человек позвонили в обсерваторию Mundaring и сообщили о свистящем объекте, похожем на шаровую молнию, наблюдаемом низко над горизонтом».¹⁰⁰

Два года спустя местные газеты сообщали, что Аум Синрике пыталась провести обогащение урана на атомной станции Баньяварн [Banjawarn] к северу от места взрыва. Что же произошло? Испытывала ли секта ракеты с ядерными зарядами? Был ли это НЛО? Или это был неудачный взрыв при производстве горных работ? Сенатор Сэм Нан [Sam Nunn] хотел получить ответы.

К счастью, инцидент был зафиксирован станцией глобальной сейсмографической сети IRIS, находящейся в 650 километрах в северо-восточной Австралии. Проанализировав «загадочное событие» 28 мая и сравнив его с данными локального землетрясения 4 сентября 1994 года и проведенного во время горных работ взрыва 28 января 1995 года, сотрудники IRIS Кристел Хеннет [Christel B. Hennet] и Грегори ван дер Винк [Gregory van der Vink] установили, что странное событие не являлось ни тем ни другим. Они сообщили, что, вероятнее всего, имело место столкновение с поверхностью Земли железного метеорита диаметром приблизительно три метра, при детонации которого высвободилась энергия порядка двух килотонн. По данным ученых, вероятность столкновения с таким метеоритом – приблизительно один раз в шесть лет.

Более чем через два года после подозрительного события в западной Австралии, ученые из Вашингтона, федеральный округ Колумбия, смогли изучить записи станции мониторинга и с твердой уверенностью сказать, что взрыв не был результатом испытания ядерной бомбы японской террористической сектой «Судного дня». Глобальный инструмент и библиотека работали.

Мир един, нравится нам это или нет

В течение многих лет защитники окружающей среды твердили, что все мы живем в

¹⁰⁰ Christel B. Hennet (IRIS), Gregory van der Vink (IRIS), Danny Harvey (University of Colorado), and Christopher Chyba (Princeton University), «IRIS Assists Senate in Investigation of International Terrorist gGroup», *IRIS Newsletter*, Fall 1996, p. 13–15.

огромном едином мире: все, что кто-то делает, влияет и на всех остальных. Если смотреть через призму времени, это замечание становится все более верным. С момента изобретения фотографии прошло более 150 лет, а мы все еще только подходим к осознанию того, что мир вокруг нас может быть зафиксирован с постоянно увеличивающимся количеством подробностей.

Выбор, перед которым мы стоим, не сводится только к всепроникающим системам мониторинга, управляемым учреждениями и системами мониторинга, управляемым учреждениями и всем населением. Имеется и третий вариант: создать правила, определяющие порядок установки систем мониторинга и использования полученной информации. Мы отклоняем этот вариант на свой страх и риск.

6

Знать свое будущее

Делали ли вы аборт, когда Вам было 15 лет?

Несколько лет назад, когда в Вашей семейной жизни была особенно тяжелая полоса, согласно нашим записям, Вы лечились от заболевания, передающегося половым путем, которого Ваша жена не имела. Знает ли она об этом?

Этот одинокий ребенок в госпитале штата, страдающий синдромом Дауна, Ваш? Почему Вы не навещаете его чаще?

Я рассказал Дженис о головных болях, которые мучают Вас на работе. Она сказала, что, когда вы были детьми, ваш отец бил вас головой о стену. Вы не думаете, что у вас повреждение мозга?

Большинство американцев считает, что медицинская документация является наиболее критичной частью персональной информации, которая у них есть. Медицинские карты – вехи нашего прошлого. Они хранят семейные секреты. Они раздевают нас догола, как перед подготовкой к хирургической операции. Они напоминают нам о вещах, которые мы хотели бы забыть и которые никогда не раскрыли бы посторонним.

В то же время медицинские карты – окно в наше будущее. Они не идеальные предсказатели, если быть точным, – абсолютно здоровый человек может быть сбит грузовиком на улице, – но многие болезни и болезненные состояния развиваются по предсказуемому пути. Люди с нарушенной проходимостью коронарных артерий имеют тенденцию к развитию сердечного приступа; диабетики, не имеющие возможности контролировать уровень сахара в крови, рискуют ослепнуть; люди с хронической депрессией имеют склонность к суицидальным попыткам. Генетические данные могут рассказать еще больше.

Но медицинские карты говорят о временном здоровье столь же подробно, сколь и о хронических заболеваниях. В нашем неточном мире точное знание веса, кровяного давления и уровня холестерина здорового человека создает ощущение предсказуемости. Врач не может точно сказать, что вы доживете до 92 лет, но статистика говорит, что ваши шансы на это равны 35 %. Страховые компании используют эту информацию для установки процентных ставок. Компании могут использовать эти данные при принятии решения, кого следует обучать и продвигать на ответственные позиции.

Нет большего пробела

Медицинская документация является также одним из самых сложных для защиты видов персональной информации. В то время как реальные бумаги или электронные файлы могут быть защищены при помощи замков и паролей, отдельные факты из этой документации могут быть легко раскрыты в результате преступных действий, с целью наживы или даже по случайности.

Рассмотрим случай, произошедший в Пафкипси, штат Нью-Йорк, с молодой женщиной, попавшей в автомобильную аварию со своим женихом в 1982 году. Они были доставлены в Vassar Brothers Hospital, где женщина рожала тайком от всех год назад. Когда женщину регистрировали, дежурный поднял из больничного компьютера ее записи. «О, вы родили малыша год назад», – сказал дежурный в присутствии женщины и ее жениха.¹⁰¹ Это была объяснимая оплошность, но она раскрыла миру персональную информацию.

С гораздо более серьезным нарушением приватности пришлось столкнуться в том же году члену палаты представителей Нидии Веласкес [Nydia Velazquez]. Три недели спустя после того, как Веласкес одержала победу на предвыборном собрании Демократической партии в Нью-Йорке, ей позвонил ПитХэмилл [Pete Hamill], редактор *New York Post*. Из показаний Веласкес Судебному комитету сената в 1994 году:

Он сказал мне, что накануне вечером в *Post* пришел анонимный факс с моей картой из St. Claire Hospital. Из этих документов следовало, что я обратилась год назад в этот госпиталь за оказанием медицинской помощи после суицидальной попытки. Он сказал мне, что и другие газеты города получили эту информацию, и что *NewYorkPost* собирается опубликовать передовицу на следующий день. Утечка моих данных произошла с единственной целью, чтобы помешать моему избранию в палату представителей путем дискредитации меня в глазах моих избирателей. Очень мало людей знали об этой ситуации, и я приняла решение не сообщать об этом моей семье. Я хотела, чтобы они помнили меня только задорной, счастливой и сильной. Мои 80-летние родители не поняли этого. Они до сих пор не понимают. Когда мне стало ясно, что эта информация будет опубликована в газете и я не имею возможности это остановить, я почувствовала себя оскорбленной. Я доверяла системе, а она предала меня.¹⁰²

Нидия Веласкес

Через три недели после того, как Нидия Веласкес победила на выборах в палату представителей от Демократической партии штата Нью-Йорк, кто-то из госпиталя St. Claire Hospital отправил по факсу в адрес газеты *NewYorkPost* медицинскую карту Веласкес. Карта содержала информацию о медицинской помощи, полученной Веласкес в госпитале после суицидальной попытки – попытки, произошедшей за несколько лет до выборов. [Фото любезно предоставлено Нидией Веласкес]



Что больше всего беспокоит, так это то, что, по всей вероятности, не было нарушено ни

¹⁰¹ Dr. George Way, New York, NY, процитировано Scott Winokur, «Nowhere to Hide», *San Francisco Examiner*, 7-12 октября 1984, p. 13. Опубликовано: Robert Ellis Smith and Eric Siegel, *War Stories: Accounts of Person Victimized by Invasion of Privacy* (опубликовано *Privacy Journal*, PO BOX 28577, Providence, RI 02908. 401-274-7861, 1990).

¹⁰² Testimony of U.S. Representative Nydia Veldzquez to the Senate Judiciary Committee, 1994. См.: Ann Cavoukian and Don Tapscott, *Who Knows? Safeguarding Your Privacy in a Networked World* (Toronto: Random House of Canada, 1995, p. 103).

одного закона, когда записи Веласкес были отправлены по факсу. Врач мог быть подвергнут дисциплинарному взысканию или лишиться лицензии за нарушение права пациента на конфиденциальность. Согласно установленным в штате требованиям, отдел регистрации госпиталя «должен обеспечивать конфиденциальность карт пациентов» и может лишиться аккредитации в случае нарушения конфиденциальности, говорит Дональд Мой [Donald Moy] из Совета медицинского общества штата Нью-Йорк.¹⁰³ Но очень мало законов (местных или уровня штата) считают криминалом несанкционированное опубликование медицинских карт самих по себе. Секретарь или охранник, который имеет возможность проникнуть в помещение, где хранятся карты и отправить их по факсу, нарушает внутренние правила госпиталя, но маловероятно, что при этом он совершает уголовное деяние.

«Многие люди думают, что обнародовать медицинскую документацию незаконно. Но они не знают, что таких законов не существует», – говорит издатель *The Privacy Journal* Роберт Эллис Смит [Robert Ellis Smith]. «Возможно, они имеют ввиду, что разглашение может повлечь за собой санкции этического характера в отношении врача или что жертва может подать иск по факту нарушения приватности. Попросите людей, утверждающих это [что медицинские карты защищены законом], процитировать закон. Мой опыт подсказывает, что ни в одной другой области нет такого разрыва в части защиты приватности между ожиданиями людей и реальным положением дел, как в медицинских данных».¹⁰⁴

В 1995 году 43 американских штата не имели законов, устанавливающих ответственность за разглашение медицинских данных.¹⁰⁵ На федеральном уровне также не существует законов, устанавливающих ответственность за незаконное разглашение медицинских данных. Потребность в таких законах очевидна, поскольку случаи несанкционированного разглашения распространены очень широко. Согласно исследованию Health Information Privacy Survey (опрос об обеспечении приватности в отношении информации о состоянии здоровья), проведенного Louis Harris and Associates и Аланом Уэстином, «27 % респондентов (представляющих 50 миллионов взрослых) заявили о своей уверенности, что организации или отдельные лица, имеющие доступ к их персональной медицинской информации раскрывают ее ненадлежащим образом. 31 % этих респондентов (представляющих 8 % всего населения и 14 миллионов американцев) сообщили, что в результате таких разглашений им был причинен вред или беспокойство».¹⁰⁶ Исследование также показало, что в первую очередь всю серьезность проблемы с обеспечением приватности медицинских карт осознают люди «на переднем крае» – врачи и медсестры.

«Многие пациенты были бы немало удивлены, узнав какое количество организаций получает информацию о состоянии их здоровья: поставщик, страховщик, фармацевт, организации здравоохранения штата, возможно, даже работодатель, компания по страхованию жизни или маркетинговые фирмы, – говорит Пол Клэйтон [Paul D. Clayton], возглавляющий Комитет по обеспечению приватности и безопасности в здравоохранении Государственного совета по исследованиям [National Research Council's Committee on Healthcare Privacy and Security]. – Совместное использование информации в здравоохранении ничем не регулируется и вызывает серьезное беспокойство в равной мере у защитников

¹⁰³ Интервью автору, 25 июля 1997.

¹⁰⁴ Из личной переписки (электронная почта), 24 июля 1997.

¹⁰⁵ Cavoukian and Tapscott, *Who Knows?* p. 98.

¹⁰⁶ Harris-Equifax, *Health Information Privacy Survey*. Проведено для Equifax фирмой Louis Harris and Associates в сотрудничестве с доктором Аланом Уэстином из Колумбийского университета. Study No. 934009, Louis Harris and Associates. New York, NY, 1993.

личных свобод и у пациентов, поскольку зачастую этот процесс происходит без разрешения пациентов и даже их информирования». ¹⁰⁷

Несмотря на раскрытие информации о попытке самоубийства, Веласкес выиграла выборы. Но Томми Робинсон [Tommy Robinson] не оказался столь удачлив. В 1990 году конгрессмен Робинсон был кандидатом на пост губернатора штата Арканзас от Республиканской партии, конкурируя с Биллом Клинтоном. Страховщик «слил» в прессу информацию, что Робинсон имеет проблемы с алкоголем. Как оказалось, диагноз был ошибочным. Невзирая на это, проигрыш Робинсона обусловлен частично этой утечкой информации. Это событие в корне изменило будущие события национального масштаба, поскольку Билл Клинтон имел возможность использовать пост губернатора для осуществления удачной предвыборной кампании на пост президента США. ¹⁰⁸ Кажущаяся сложной задача защиты медицинских карт в офисе врача или госпитале блекнет при более широком взгляде на проблему. В нашем обществе существует огромное и постоянно увеличивающееся количество других типов медицинской информации, которая, будучи раскрытой, может принести не меньше вреда, чем разглашение диагноза. Счета на оплату лечения направляются страховым компаниям и другим организациям, оплачивающим лечение пациента. Результаты анализов и подробные расшифровки счетов направляются пациентам. Фармацевты знают, какие лекарства выписаны пациенту. Когда человек покупает лекарства, продающиеся без рецепта, регистрационная лента кассового аппарата также становится одним из видов медицинских документов. Существует широкий ассортимент наборов для определения в домашних условиях уровня сахара в крови, овуляции, беременности и индикации приема наркотиков. Новое поколение генетических тестов стремительно набирает популярность. Эти тесты во многих случаях можно провести тайком от человека, не получая его разрешения. Эта информация может быть использована, как и многие другие вещи, в маркетинговых целях. Metromail, по сообщениям, имеет медицинскую базу данных, называемую Patient Select, содержащую 15 миллионов имен. «Затратив примерно 30 центов за имя, крупные фармацевтические компании имеют возможность напрямую предлагать свою продукцию страдающим от ангины, диабета или артрита», – сообщает Амитай Этциони [Amitai Etzioni] в статье, опубликованной в *Consumer Report*. ¹⁰⁹

Сказка о медицинских картах

Глядя со стороны, Дэниэль выглядел идеальной кандидатурой на пост вице-президента. Проработав в компании семь лет, он дважды менял должности, улучшил работу подразделения и стал старшим директором. Но однажды вечером босс Даниэля обнаружила в его медицинском шкафчике пузырек с лекарством (она искала аспирин). Несколько телефонных звонков позволили выяснить, что это лекарство используется для снижения повышенного артериального давления и что Даниэль страдает этим заболеванием уже 15 лет. Врач компании сказал, что люди с подобным заболеванием живут от 5 до 30 лет, но каждый случай индивидуален. Когда пришло время ежегодной аттестации, Даниэль получил прибавку к жалованию, но его не стали продвигать по служебной лестнице. В конце концов зачем парню дополнительные стрессы? И зачем предлагать человеку занять одну из высших

¹⁰⁷ Пресс-релиз, National Research Council, 5 марта 1997.

¹⁰⁸ Janlori Goldman, «Regarding the Confidentiality of Health Records», statement before the US House of Representatives Government Operations Subcommittee on Information, Justice, Transportation and Agriculture, 4 ноября 1993.

¹⁰⁹ «Who's Reading Your Medical Records?», *Consumer Reports*, октябрь 1994, p. 628–632. Прочитировано по: Etzioni, *Limits of Privacy*, p. 147.

руководящих должностей в компании, если его может не стать в ближайшие 10 лет?

Когда-то давным-давно медицинские карты имели сугубо специальную цель: они представляли подробную запись всех обращений человека в медицинские учреждения, чтобы будущие обращения имели больше шансов принести положительный результат. Люди были заинтересованы в корректности медицинских карт.

Сегодня медицинские карты играют более широкую роль, не ограничиваясь лишь здравоохранением. Они используются работодателями и страховыми компаниями для принятия решения при найме на работу и страховании. Они используются госпиталями и религиозными организациями для ходатайства о дотациях. Даже маркетинговые фирмы скупают медицинские карты в поисках коммерческой выгоды. Если раньше у людей был стимул следить, чтобы их медицинские карты были полными, точными и своевременными, то сейчас многие чувствуют необходимость их разделения, чтобы в случае неизбежного разглашения ущерб был минимален.

Когда-то медицинские карты были почти священны. Сегодня обычное дело, когда медицинские карты разыскиваются и используются в судебных процессах для дискредитации свидетелей, особенно в делах об изнасиловании. Медицинские данные политиков и преступников публикуются в прессе без их разрешения. Забавно, но все возрастающая медицинская грамотность населения делает ущерб от публикации персональной медицинской информации более существенным. Медицина – комплексная и очень специфичная наука, с большим числом правил и гораздо большим числом индивидуальных исключений. В неопытных руках история болезни человека часто становится средством подтверждения предубеждений или наклеивания ярлыков.

В особенной степени подвержена угрозам конфиденциальность психотерапевтических записей, говорит доктор Дениз Нагель [Dr. Denise Nagel], исполнительный директор Национальной коалиции по правам пациентов [National Coalition for Patient Rights]. Адвокаты, НМО, страховые компании и другие постоянно требуют доступ к психотерапевтическим записям, и, если это произойдет, опасности будет подвергнута вся национальная система душевного здоровья.¹¹⁰

«Готовность человека поделиться критичной, зачастую щекотливой информацией зависит от гарантий сохранения ее в тайне. Это база доверия во взаимоотношениях», – говорит Нагель. Восстановление после многих видов душевных травм и заболеваний требует, чтобы обсуждаемые во время терапевтических сеансов вопросы оставались в секрете. В 1995 году Верховный суд США принял такое же решение в деле *Jaffe v. Redmond*. Нагель отмечает, что суд счел разговоры между пациентом и лицензированным социальным работником или врачом, даже не имеющим лицензии на медицинскую деятельность, защищенными и поэтому не может требовать от свидетеля разглашения их содержания, за исключением случаев, когда интересы дела явно перевешивают интересы пациента по сохранению приватности. «Качественное здравоохранение зиждется на безусловном требовании конфиденциальности и доверия, и это доверие не должно быть легко разрушено», – констатировал суд.

Однако эта документация часто используется адвокатами обвиняемых в изнасиловании. Адвокаты обычно угрожают представить эти документы на открытом судебном заседании, чтобы подорвать доверие к обвинителям их подзащитного, если жертва не снимет обвинения.

Такой подход защитников сам по себе может быть преступным или по крайней мере неэтичным, но это обычная практика во многих делах об изнасиловании. Например, жертва изнасилования могла в юности иметь фантазии на тему быть изнасилованной; теперь она ощущает себя глубоко растрепанной и не может смириться с фактом, что это наконец произошло с ней в реальности. Жертве могла понадобиться многомесячная терапия, чтобы

¹¹⁰ Лекция на Privacy Summit Conference, 1995.

смириться с осознанием этого, а она вынуждена выслушивать в суде теорию адвоката защиты о том, что женщина сама каким-либо образом поощряла нападающего и была добровольным участником процесса.

Между тем родители все чаще требуют получить доступ к психотерапевтическим записям людей, контактирующих с их детьми. В Западной Виргинии родители потребовали ознакомить их с медицинской картой водителя школьного автобуса, который отпускал странные замечания, когда вез детей. Школьный управляющий провел расследование и сказал, что водитель проходил лечение и его состояние не представляет угрозы детям. Но родители настаивали, и в 1986 году Верховный суд штата принял их сторону, заявив, что они имеют право ознакомиться с полной историей болезни водителя, включая записи, касающиеся его душевного здоровья.¹¹¹

Приватность – обязанность вашего врача

Плакат на стене в моем местном госпитале гласит «Пожалуйста, уважайте конфиденциальность пациентов». Он имеет очень глубокий смысл. Госпитали и другие медицинские учреждения зависят от способности персонала хранить секреты пациентов. Врачи, медсестры, клерки и даже санитары – все имеют доступ к сугубо конфиденциальной информации. Госпиталь, который попытается оградить своих служащих от контактов с критичной информацией о пациентах, очень быстро перестанет выполнять свои функции.

К счастью, в большинстве случаев это доверие обосновано. Я никогда не встречал врача или другого медицинского работника, который бы не относился со всей серьезностью и ответственностью к соблюдению врачебной тайны. Обеспечение конфиденциальности пациента – одна из важнейших основ профессии медика. Она исходит от клятвы Гиппократова, которая, в частности, гласит: «Что бы при лечении – а также и без лечения – я ни увидел или ни услышал касательно жизни людской из того, что не следует разглашать, я умолчу о том, считая подобные вещи тайной».

Сохранение конфиденциальности пациента осложняется тем фактом, что при обычном визите в госпиталь в доступе к карточке пациента нуждаются от 50 до 75 человек. Сохранение секрета возможно только общими усилиями, для разглашения же достаточно одной «паршивой овцы». Многие госпитали временно нанимают на работу вспомогательных сотрудников, не прошедших обучения по вопросам медицинской этики или имеющих лишь минимальные представления об этой сфере. Другие медицинские учреждения проводят сокращения, которые вызывают в бывших служащих обиду на работодателя. Как мы убедились в случаях с Нидией Веласкес и Томми Робинсоном, небрежный или подкупленный сотрудник может легко разрушить врачебную тайну.

В последние 50 лет военные разведывательные ведомства и крупные корпорации занимались разработкой технологий предотвращения хищений конфиденциальной информации и выяснения источников утечки. Каждому выдавалась персональная копия материалов. Фотокопирование регистрировалось. При входе и выходе с режимного объекта личные вещи людей подвергались досмотру. Эти технологии просто невозможно применять в здравоохранении. И в большинстве случаев этого и не требуется.

Но утечка информации происходит – и это касается не только людей, баллотирующихся на какой-либо пост. После начала эпидемии СПИДа один за другим происходят случаи, когда человек теряет страховку или работу, если открывается, что он инфицирован ВИЧ. В 1989 году ФБР не заключило контракт с врачом, который выполнил все предварительные требования Бюро, сдал экзамен по физической подготовке в Сан-Франциско, но было установлено, что у него СПИД. В начале 1990-х в Солт-Лейк-Сити

¹¹¹ *Morgantown Dominion Post*, Morgantown WV, 13 ноября 1989, p. 1; *Privacy Journal* victim file. Опубликовано в *War Stories*.

производитель витаминов уволил Кима Олреда [Kim All red] после положительного теста на производные марихуаны в прописанном ему лекарстве Marinol; когда компания узнала, что он принимает лекарство от СПИДа, она отказалась принять его обратно на работу. В 1987 году в Принстонском медицинском центре практикующий хирург по имени Уильям Беринджер [William Behringer] был диагностирован в своем собственном учреждении, где ему был поставлен диагноз СПИД. «В течение нескольких часов после этого он получил множество звонков от доброжелателей, которые, очевидно, знали о его ситуации. Большинство звонивших были его коллеги из медицинского центра. После этого стали звонить пациенты. Вскоре госпиталь отстранил его от хирургической практики. Суд установил, что нарушение конфиденциальности произошло по вине госпиталя», – читаем мы в отчете «Военные истории II», опубликованном в *Privacy Journal*.¹¹²

Эти истории показывают и другой аспект дилеммы приватности медицинской информации. Вам не надо делать фотокопии чьей-нибудь истории болезни, чтобы нарушить его медицинскую приватность, – достаточно утечки декларативного заявления вроде «Нидия Веласкес пыталась покончить жизнь самоубийством» или «доктор Уильям Беринджер болен СПИДом». И конечно, как показывает случай с Томми Робинсоном, утверждение не обязательно должно быть истинным, достаточно, чтобы оно было правдоподобным.

Когда в 1993 году я начал встречаться с моей будущей женой, мы решили пройти обследование на СПИД в городском госпитале Бостона. Эта клиника – одна из нескольких в городе, специализирующаяся на анонимном тестировании. Медсестра, которая брала у меня кровь на анализ, не знала, кто я, и не требовала от меня никакой идентификации. Она дала мне контрольный номер, чтобы я мог получить результаты. Но когда мы с женой пришли неделю спустя за результатами, одна из женщин-добровольцев, работавших в клинике, узнала меня, так как мы вместе учились в МТИ. Запрещает ли закон такому добровольцу рассказывать людям, что он видел меня в клинике? Что относительно других людей, оказавшихся в приемной, которые могли узнать меня?

Это одна из проблем, вызванных специализацией. Цель анонимного тестирования на СПИД заключается в том, чтобы позволить людям провести анализ, не оставляя при этом записей. Но создание специальных мест для анонимного оказания определенных медицинских услуг приводит к тому, что приватность личности зависит от ее последующей анонимности. Если в клинике анонимно оказывается целый ряд медицинских услуг, то простое узнавание человека на входе не приводит к полному разглашению медицинской тайны человека. Кризисные центры для жертв изнасилования и клиники по производству абортов («женские клиники») имеют аналогичную проблему. Одним из решений является реинтеграция этих услуг в обычную медицинскую практику.

Многие люди имеют обратную точку зрения. Они считают, что лучший способ решить неподъемную проблему медицинской приватности – это просто уничтожить ее: раскрыть файлы и банки данных, сделав медицинские карты свободно доступными для всех. Дэвид Брин, автор «Прозрачного общества», большой сторонник этой точки зрения. Я даже сам верил в это одно время; прозрачность просто изящна. Я считал, что раз каждый из нас имеет какие-либо медицинские проблемы, то лучший способ смыть пятно позора с болезней – выставить их на всеобщее обозрение.

Но проблема с открытием доступа к медицинским картам заключается в том, что у каждого свой организм. Кто-то страдает диабетом, кто-то астмой, кто-то имеет наследственные генетические заболевания. Некоторые имеют небольшие шизофренические отклонения, контролируемые медикаментозными средствами. Некоторые по-настоящему здоровы. Открытие для публичного доступа историй болезни всех и каждого подвергнет людей опасности дискриминации или личных нападков, для которых всегда найдется повод. Одна из целей обеспечения приватности в обществе заключается в защите каждого из нас от

¹¹² Опубликовано в *War Stories II*, p. 58.

различных социальных проблем, которые мы еще не изжили.

Даже если какое-нибудь футуристическое просвещенное общество сумеет уважительно относиться к болезням, в отличие от нас, существует еще одна причина, по которой мы все равно должны соблюдать приватность пациента. Люди, которые сумели справиться со своей физической или душевной болезнью, заслуживают того, чтобы в повседневной жизни различные доброжелатели не напоминали им постоянно об этом. И, как я уже говорил ранее, гарантии конфиденциальности психотерапевтической документации являются неременным условием для успешного лечения душевных болезней.

Люди заслуживают того, чтобы контролировать свои медицинские вопросы и приватность своих медицинских карт. Врачи и медсестры понимают это, но медицинские учреждения не заботятся об этом.

Приватность не является обязанностью вашей страховой компании

В то время как местный госпиталь озабочен постоянным напоминанием своим служащим о необходимости уважать конфиденциальность пациентов, страховая компания озабочена постоянным напоминаем *мне*, что конфиденциальность не совместима с их манерой ведения бизнеса.

Как и большинству американцев, чтобы обеспечить оплату посещений врача из моей страховки, мне необходимо заполнить специальное заявление. Внизу этой формы имеется небольшой контракт, который стирает остатки странных представлений, которые я мог иметь о приватности. Контракт имеет форму соглашения. Он гласит:

Я предоставляю право любому врачу, госпиталю или иному медицинскому учреждению, страховой компании или другой организации, учреждению или физическому лицу, располагающему данными или информацией обо мне, моих иждивенцах или состоянии нашего здоровья, сообщать по первому требованию CNA/[p33] или ее полномочных представителей полностью или частично эту информацию. Фотокопия данного разрешения обладает такой же юридической силой, как и оригинал.

Я не юрист, но и не надо быть юристом, чтобы понять, что означает это соглашение. В качестве предварительного условия оплаты страховой компанией суммы в 50 долларов за мой визит к врачу и 14 долларов за антибиотики, я даю право любому предоставлять всю медицинскую информацию обо мне кому угодно. Это полное разрешение охватывает *все* документы: школьные, налоговые и банковские. Оно также охватывает и те конфузские любовные письма, которые я писал моей девятнадцатилетней подружке. Это разрешение является неопределенным, у него нет даты окончания или определенного срока действия.

Некоторые люди думают, что позволения, изложенные в подобных формах, никогда не используются на практике. Они справедливо полагают, что страховая компания может разве что позвонить врачу для уточнения диагноза или получения дополнительных подтверждений об оказании услуг, но они сомневаются, что страховая компания захочет получить всю информацию. В конце концов, у нее нет обусловленных требованиями бизнеса причин делать это. Здоровые рассуждения, не правда ли?

Проблема такого подхода на основе здравого смысла заключается в том, что он неправильный. Эта форма разрешения означает именно то, что в ней написано. «Любые записи» означает именно *любые* записи. «Вся информация» действительно означает, что ничего не остается за рамками этого понятия. Такое полное разрешение позволяет страховой компании вылавливать любые персональные данные, которые она захочет.

«Бланк заявления составлен именно таким образом, чтобы мы могли получить необходимую нам информацию для обнаружения мошенничества, – говорит пресс-секретарь CNA Роджер Моррис [Roger Morris]. – Нашей целью является не накопление информации о людях, а попытка защитить интересы держателей наших страховых полисов».¹¹³ Такие широкие полномочия позволяют страховой компании проводить расследования в случае подозрения в мошенничестве без риска быть обвиненной во вторжении в личную жизнь. Такая экономия для компании в конечном счете отражается на гораздо более низких страховых премиях для всех, говорит Моррис. Конечно, снижение потерь компании отражается и на повышении ее доходов.

Медицинские страховые фирмы говорят, что мы не должны беспокоиться, предоставляя им критичную информацию. «В страховой индустрии хорошо поставлена работа с информацией, что позволяет сохранять конфиденциальность. Мы чтим и соблюдаем все писанные законы», – уверяет пресс-секретарь Американской ассоциации медицинского страхования [Health Insurance Association of America] Ричард Курш [Richard Coorsh].

Но американская общественность считает по-другому. Согласно проведенному в 1993 году совместному исследованию Harris и Equifax по вопросам обеспечения приватности в здравоохранении, 15 % столкнувшихся с нарушением их медицинской конфиденциальности – а это 7,5 миллиона человек, – говорили о том, что нарушение произошло по вине страховой компании.

Человек, придерживающийся обратного мнения, – профессор университета имени Джорджа Вашингтона, автор «Пределов приватности» [*The Limits of Privacy*], Амитаи Этциони. В своей книге, в которой, вообще говоря, достаточно критично относится к приватности, Этциони, однако, подтверждает важность приватности медицинских данных. И реальная угроза приватности медицинских данных исходит не от правительства, а от бизнеса.

В попытке понять мотивацию, стоящую за упомянутой выше разрешительной формой, я обратился в Albert H. Wohlers & Co., расположенной в Иллинойсе компании, выдавшей мне страховой полис CNA. Я потратил час, продираясь через цепочку клерков, обрабатывающих жалобы, и инспекторов, пока наконец меня не перенаправили в кабинет Джеймса Малика [James Malik], который, как я был уверен, сможет ответить на мои вопросы. Но когда я попал в офис мистера Малика, его секретарь проинформировала меня, что я не могу поговорить с ним. Я спросил его должность, она не могла назвать ее мне. Я спросил ее имя, но она не смогла сказать мне даже этого. Она сказала, что, если у меня есть вопрос, я должен представить его в письменном виде. После чего положила трубку.

Обращение, с которым я столкнулся в Albert H. Wohlers & Co., является симптомом закоренелой проблемы индустрии медицинского страхования США. Здравоохранение – сверхъестественное сочетание денег и медицины; оно играет по правилам компаний-миллиардеров. Неважно, насколько странными и произвольными кажутся эти правила, но это – правила. Если вы хотите получить страховку, посетить своего врача или оплатить визит в госпиталь, вы должны играть по этим правилам. А поскольку страховые компании сохраняют деньги, когда теряют заявления клиентов, то они имеют финансовый стимул плохо обращаться с клиентами. Все это правда, поскольку люди, оплачивающие счета страховых компаний, это не те люди, которые пользуются их услугами.

Мы должны также опасаться немедицинского использования медицинских данных, предупреждает Этциони, который цитирует неопубликованное исследование 1996 года, согласно которому «35 % компаний, входящих в список Fortune 500, подтверждают, что используют медицинские данные при принятии решения о приеме на работу».¹¹⁴ Самый

¹¹³ Интервью автору, 25 июля 1997.

¹¹⁴ David F. Linowes, «A Research Survey of Privacy in the Workplace», неопубликованная работа, University of Illinois at Urbana-Champaign, апрель 1996.

распространенный путь получения работодателем этой информации – через страховые компании или схемы корпоративного страхования, т. е. когда полис выдается профессиональной страховой компанией, но выплаты производит корпорация. (Такие схемы чрезвычайно популярны, поскольку позволяют ущемлять права работников, не нарушая закон.) Один из случаев, приводимых Этциони, произошел со служащим транспортного управления Юго-Восточной Пенсильвании [Southeastern Pennsylvania Transit Authority, SEPTA], лечившимся от СПИДа. SEPTA узнало о лечении, когда получило запрос о возмещении расходов нанею, и информация была передана руководителю этого человека.¹¹⁵

Уже внимательно прочитав параграф с разрешением в моем заявлении о страховании, я совершил нечто из ряда вон выходящее. Большинство людей не читают внимательно документы, которые подписывают в своей повседневной жизни, – документы кабальные. Эти документы и стоящие за ними политики создают и укрепляют чувство бессилия. Это ловушки, расставленные системой на потребителя. У нас нет возможности обсуждать условия или предложить свой вариант. Единственное, что нам остается, – подписывать.¹¹⁶

Никто не знает о MIB [p34]

Работая над диссертацией на тему политики в области приватности в корпоративной Америке в Гарвардской школе бизнеса Джефф Смит [Jeff Smith] опросил более тысячи человек по различным аспектам приватности и провел подробные интервью с несколькими десятками. Один из ключевых вопросов, которые он задавал, был следующий: знают ли люди о существовании компании под названием «Медицинское информационное бюро»? То, что он узнал, не было сюрпризом:

Только один человек из опрошенных знал о существовании MIB, хотя почти все, кроме двух человек, застраховали свою жизнь и прошли через процесс подписания. Это говорит о том, что люди читают договор о страховании невнимательно, поскольку уведомление о MIB точно туда включено. Однако этот недостаток понимания указывает также на неадекватность процедуры уведомления.¹¹⁷

Я спросил свою жену, знает ли она, что такое Медицинское информационное бюро. Она сказала, что нет. Тогда я показал ей договор медицинского страхования, который она подписала около двух лет назад. Он включал следующие абзацы:

Я ПРЕДОСТАВЛЯЮ ПРАВО любому врачу, медицинскому работнику, госпиталю, клинике, другому медицинскому или относящемуся к медицине

¹¹⁵ Etzioni, *The Limits of Privacy*, p. 145.

¹¹⁶ Договоры медицинского страхования не единственные бланки, которые люди не читают. Когда мы с женой покупали наш первый дом, нас заставили прочитать огромное количество документов перед подписанием. Наш адвокат попросил нас взять подписанные документы домой и почитать их на досуге: чтение их в процессе подписания растянуло бы часовую процедуру до 3–4 часов. Очень мало людей читают напечатанные мелким шрифтом соглашения об использовании кредитных карт, и почти никто не читал свод правил пользования толщиной с пару телефонных справочников, на который ссылается соглашение. И практически никто не читает узенькое лицензионное соглашение к компьютерным программам, несмотря на то что они выражают согласие с условиями соглашения, используя эти компьютерные программы.

p34

Медицинское информационное бюро [Medical Information Bureau, MIB] В оригинале присутствует игра слов: MIB также является сокращением от «Men In Black» – «Люди в черном».

¹¹⁷ Smith, *Managing Privacy*, p. 143.

учреждению, MIB, Inc., агентству по сбору информации о потребителях [consumer reporting agency], страховой или перестраховывающей компании или работодателю, располагающему определенной информацией *обо мне или моих иждивенцах*, передавать всю или часть этой информации John Alden Life Insurance Company или ее полномочным представителям. Виды информации, которую я позволяю раскрывать, включают: (1) физическое состояние, (2) историю болезни, (3) профессию, (4) возраст, (5) занятость и (6) личные характеристики. Это разрешение включает информацию о (1) наркотиках, (2) алкоголизме, (3) душевных заболеваниях или (4) инфекционных заболеваниях.

Я СОГЛАСЕН с тем, что информация, полученная в соответствии с этим позволением, будет использована JOHN ALDEN LIFE INSURANCE COMPANY для определения права на выгодоприобретение. Я ТАКЖЕ ПОЗВОЛЯЮ JOHN ALDEN LIFE INSURANCE COMPANY передавать любую полученную информацию перестраховывающей компании, MIB, а также любым другим физическим и юридическим лицам, осуществляющим законную деятельность по оказанию услуг в связи с моим обращением, заявлением, или в других установленных законом случаях, либо по моему будущему позволению.

«Есть ли твоя подпись на этом бланке?», – спросил я ее. «Да», – ответила она. После чего прочитала бланк договора еще раз. Она по-прежнему не имела никакого представления, что такое MIB, кроме как, что это, возможно, какой-то центр обмена медицинской информацией.

Фактически MIB хранит в своих компьютерах информацию о людях. А именно каждый раз, когда вы сообщаете о состоянии здоровья в страховом заявлении, все, начиная от проблем с сердцем и до рака кожи, должно быть сообщено в MIB. Когда в следующий раз вы обратитесь за страховкой, ваша «новая» страховая компания запросит в MIB ваш файл и просмотрит ваши предыдущие обращения.

Теоретически MIB создано для того, чтобы предотвратить случаи, когда люди, имеющие серьезные проблемы со здоровьем (и которым неоднократно отказывали в страховании), вдруг «забудут» указать эту информацию в страховом заявлении и застрахуют свою жизнь и здоровье по льготным тарифам, предназначенным для практически здоровых людей. MIB помогает «сохранять стоимость страховки страховым компаниям и их клиентам, предотвращая потери, которые могут произойти в результате мошенничества или умышленного сокрытия информации», – говорит президент MIB Нейл Дэй [Neil Day].¹¹⁸

MIB не создавалась как медицинский «черный список». Страховщикам официально запрещено использовать информацию, хранящуюся в файлах MIB, в качестве основания для отказа в страховании. Им разрешено лишь использовать эту информацию для проведения будущего расследования. По крайней мере, так сказано в правилах.

MIB, созданному в 1902 году как профессиональное некоммерческое объединение, принадлежит сегодня около 750 страховым компаниям. Файлы MIB не содержат медицинских данных, результатов анализов или рентгенологических исследований. Вместо этого досье каждого человека содержит несколько кодов, которые описывают диагнозы, поставленные данному человеку. Они могут означать диабет, проблемы с сердечной деятельностью и употребление наркотиков. Некоторые коды очень подробны. Например, Джефф Смит установил, что для СПИДа у MIB имеется пять кодов:

- связанные со СПИДом состояния [AIDS-related complex or condition, ARC] или синдром приобретенного иммунодефицита (СПИД);
- необъяснимое появление кандидозного стоматита, других условно-патогенных инфекций, потери веса, общего хронического увеличения лимфатических узлов, постоянного жара или диареи;
- ненормальные результаты исследования Т-лимфоцитов;

¹¹⁸ Интервью автору, 29 июля 1997.

- ненормальные результаты анализа крови, для которых нет отдельного кода;
- наличие двух и более различных типов антител, указывающих на присутствие вируса HTLV-III; [p35] этот код более не используется.¹¹⁹

Не все коды МІВ являются медицинскими, отмечает Смит. Например, у МІВ есть пять кодов, указывающих на небезопасный образ жизни, включая «информацию о небезопасном вождении, опасные виды спорта или увлечение авиацией».¹²⁰ Эти коды соответствуют вопросам, которые задает большинство страховых компаний.

Таким образом, МІВ является официальным страховым агентством по сбору сплетен и слухов. МІВ заботится о том, чтобы в случае, когда одна страховая компания отказалась застраховать жизнь человека по медицинским основаниям, все другие страховые компании знали о его болезни и также отказали ему. МІВ стало объектом постоянных споров с 1970-х годов, когда стало известно о его существовании. Корнем этих споров была склонность организации к секретности. В течение многих лет страховые компании консультировались в МІВ, не ставя своих клиентов в известность об этих файлах. МІВ не упомянуто ни в одной книге, посвященной проблемам потребителей или обеспечению их приватности. Даже номера телефонов МІВ отсутствовали в общедоступных справочниках. Секретность продолжается и сегодня, разве что в меньшей степени: МІВ не разглашает список используемых им кодов.

Дэй объясняет:

Общий смысл создания списка кодов заключается в обеспечении конфиденциальности. Отчеты МІВ очень короткие. Это небольшой лист бумаги, содержащий в среднем 2–3 кода. Обычно коды состоят из трех цифр – 321, иногда дополняются буквами – 321XYZ. Базисом обеспечения конфиденциальности является доступность списка кодов для использования только специально уполномоченными лицами в страховых компаниях и никому больше.

Сохранение в секрете таблицы соответствия между кодами и диагнозами/состояниями, которые они обозначают, в некоторой степени обеспечивает приватность. Но засекречивание списка диагнозов не дает дополнительной приватности. Скажем так: разве пострадала конфиденциальность какого-либо пациента оттого, что я сообщил о существовании пяти упомянутых выше кодов, относящихся к СПИДу? Засекречивая не только сами коды, но и словесное описание их значений, МІВ само создает предпосылки для нападков на него с претензиями, что файлы содержат не только медицинскую информацию. В прошлом, говорит издатель журнала *Privacy Journal* Роберт Смит [Robert Smith], МІВ имело коды для обозначения «сексуальных девиаций» и «странного поведения». Дэй не согласился с этим, но, поскольку МІВ не разглашает список диагнозов/состояний, для которых у него имеются коды, нет возможности установить истину.

Существуют разногласия и по поводу точности хранимой в файлах МІВ информации. «Закон о точной отчетности по кредитам» не распространяется на медицинские данные, но МІВ добровольно согласилось выполнять его требования после проверки его в 1983 году Федеральной комиссией по торговле. С тех пор МІВ ежегодно получает около 15 тысяч запросов от людей, говорит Дэй. От 250 до 300 человек оспаривают содержимое наших отчетов, говорит он. В общем, «97 % клиентов, получивших отчеты МІВ [в 1996 году], признали собранную о них МІВ информацию точной», – говорится в рекламной публикации

p35

Human T-cell Leukemia Virus – вирус лейкемии Т-лимфоцитов человека, СПИД.

¹¹⁹ Smith, *Managing Privacy*, p. 58.

¹²⁰ Ibid., p. 33.

компании.

Но если вы окажетесь среди этих 300 пациентов, вы можете остаться без медицинской страховки. В 1990 году группа по исследованию общественных интересов штата Массачусетс [Massachusetts Public Interest Research Group, MASSPIRG] провела изучение деятельности МИБ и обнаружила большое количество случаев, когда в результате ошибки в записях МИБ людям было отказано в получении медицинской страховки. В одном случае, рассказывает адвокат MASSPIRG Джош Кратка [Josh Kratka], мужчина из штата Массачусетс сообщил своей страховой компании, что он был алкоголиком, но потом справился с проблемой, уже несколько лет ведет трезвый образ жизни и регулярно посещает занятия группы анонимных алкоголиков. Страховая компания проигнорировала его пояснения и отослала в МИБ код «опасное для здоровья злоупотребление алкоголем». Следующая компания, в которой этот человек хотел оформить страховку, получила из бюро информации «злоупотребление алкоголем» и повысила для него страховую ставку на 25 %.¹²¹

В другом случае бюрократическая ошибка привела к тому, что в записях МИБ об одной женщине появилась информация, будто она – носитель вируса СПИДа. MASSPIRG установила, что «лишь только после чрезвычайного вмешательства комиссии штата по урегулированию [state regulatory board]» – так как женщина работала врачом – записи были исправлены.

МИБ заявляет, что, если по результатам представленного им отчета кому-то было отказано в страховании, это указывает на неправильное использование отчета. Компания подчеркивает, что отчеты МИБ базируются только на информации, предоставляемой при заключении договора страхования, а не на информации из заявлений о выплате страховых. Но эта отговорка звучит несерьезно в свете имеющегося в заявлении пункта, дающего страховой компании право сообщать МИБ информацию из него.

«Рекомендации МИБ понятны, но только серия проверок деятельности компаний, оказывающих услуги по страхованию жизни и здоровья, независимыми аудиторами может дать ответ о реальном состоянии дел, – говорит Джефф Смит. – Насколько мне известно, таких проверок силами независимых от страховой индустрии исследователей не проводилось».

Принуждение врачей ко лжи

Конечно, страховые компании получают информацию из различных источников, включая информационную систему страхования по нетрудоспособности [Disability Insurance Record System, DIRS] и указатель заявлений о выплате страховки [Health Claim Index]. Сам факт того, что страховым компаниям законно позволено отказывать клиентам в страховании жизни и здоровья на основании состояния их здоровья, ставит врачей под жесткий прессинг. С одной стороны, профессиональные соображения и закон требуют от врача вести точные записи о своих пациентах и предоставлять в счетах правдивую информацию. С другой стороны, врач знает, что, если он будет до конца честен при постановке диагнозов, это может привести к появлению в медицинских данных его пациентов информации, которая может помешать им в будущем заключить договор страхования. Даже в отсутствие письменного диагноза большую часть информации, которую хочет знать страховая компания, можно автоматически получить из платежных кодов.

«Страховые компании накапливают потрясающее количество информации, – говорит доктор Питер Тарши-Хорноч [Dr. Peter Tarczy-Hornoch], возглавляющий большое количество проектов по дистанционной медицине в медицинском центре Вашингтонского

¹²¹ Garfinkel, Simson, L., «From Database to Blacklist: Computer Records Let Employers and Landlords Discriminate Against Unsuspecting Applicants», *Christian Science Monitor*, 1 августа 1990, p. 12.

университета. – Эти данные не являются „крутой сексуальной информацией“, это данные типа „Какими заболеваниями страдала ваша бабушка? Госпитализировали ли вас по поводу проблем с алкоголем и наркотиками? Страдаете ли вы заболеваниями, требующими дорогого лечения и получали ли вы уже такую помощь?“ Они не особенно заботятся о точности. Это скрытый процесс. 90 % точности вполне достаточно для большинства этих материалов»¹²²

Девяносто процентов точности вполне достаточно медицинской страховой компании для принятия решения продать вам страховку или отклонить ваше заявление. 90 % точности вполне достаточно для принятия решения, как высоко можно задрать страховые ставки для вас или вашей компании, когда придет время их пересмотра. 90 % точности вполне достаточно для систематического исключения людей, в первую очередь нуждающихся в медицинском страховании. Но что, если вы попадете в те самые невезучие 10 %, которым будет отказано в страховке или предложены более высокие ставки, несмотря на то что с вами все в порядке? Лучшее, что вы можете сделать, это попытаться найти другую страховую компанию в надежде, что ошибочная информация о вас не попала в МІВ.

Столкнувшись с этой дилеммой, многие врачи выбирают ложь. Вместо постановки действительного диагноза или кода оплаты, они используют близкие по стоимости оплаты коды, не имеющие социального клейма и далеко идущих последствий для страхования. Например, говорит Тарши-Хорноч, врач может использовать код «расстройство адаптации» [adjustment disorder] вместо «депрессия».

Медицинские работники называют эти альтернативные диагнозы *суррогатами*. Законность этой практики под вопросом, ведь это разновидность подлога; в конечном счете нет статистических данных о распространенности этого явления. Очевидно одно: суррогаты создают разновидность игры в кошки-мышки между врачами и страховщиками, в которой страховые компании постоянно пытаются выловить «модные» суррогаты, а врачи выдумывают новые. Игра усложняется тем, что разные врачи в различных уголках страны используют различные суррогаты, и тем, что некоторое количество людей действительно страдает этими заболеваниями, а не более страшными, для замены которых служат суррогаты.

Мы с женой столкнулись с конкретным проявлением эффекта суррогатов в 1994 году, когда Бет заключала договор медицинского страхования. Страховая компания выдала ей бланк, который должен был заполнить ее врач. Когда она принесла заполненный бланк, ей было отказано в страховании.

Причина отказа, как мы узнали позже, заключалась в том, что врач Бет сообщил страховой компании, что при осмотре он диагностировал у нее «общее беспокойство» [generalized anxiety]. У нее была серьезная причина для волнений – она проходила осмотр за три недели до нашей свадьбы! Но проблема была в том, что другой врач в нашем районе использовал диагноз «общее беспокойство» в качестве суррогата для пациента с депрессией, получавшего лечение антидепрессантами. Понятно, что страховая компания не имела желания связываться с таким потенциально дорогостоящим клиентом, как моя жена. В конце концов страховые компании всего лишь зарабатывают деньги на страховании здоровья.

В августе 1996 года президент Клинтон подписал «Закон об отчетности и безопасности медицинского страхования» [Health Insurance Portability and Accountability Act]. Согласно этому закону, американским страховым компаниям запрещено исключать новых сотрудников, по причине имеющих у них заболеваний, из схем группового медицинского страхования их работодателей. Но дальше этого закон не пошел. Компании обязаны предоставлять страховое покрытие по имеющимся заболеваниям, но они могут это делать по астрономическим процентным ставкам. Они также могут не продлевать договор группового медицинского страхования с компанией, если один из новых сотрудников имеет заболевание, требующее дорогостоящего лечения. Это может не касаться таких компаний,

¹²² Интервью автору, 26 мая 1997.

как IBM или Еххон, но станет решающим фактором для малого бизнеса. Закон защищает лишь служащих, меняющих одну программу медицинского страхования на другую, но он не охватывает людей, самостоятельно занимающихся бизнесом, и людей, самостоятельно оплачивающих свою страховку, поскольку их работодатель не включает медицинское страхование в социальный пакет для своих работников. Наконец, закон совсем не затрагивает вопросы страхования жизни, вся история которого связана с дискриминационным использованием медицинских данных. В конце концов, именно компании, осуществляющие страхование жизни, находились в первых рядах создателей МІВ.

Право на самого себя

На пороге XXI века кажется невозможной ситуация, когда человеку отказывают в доступе к своим собственным медицинским данным. Действительно, 96 % американцев считают право на получение копии собственных медицинских данных важным, а 84 % – «очень важным».¹²³ И все же у многих американцев этого права нет.

Согласно опубликованной *Privacy Journal* выборке из законов, касающихся приватности, изданных штатами и на федеральном уровне, только 23 штата предоставляют пациентам право на ознакомление с их собственными историями болезни (см. перечень).¹²⁴ Однако, несмотря на эти законы, даже граждане этих штатов сталкиваются иногда с тем, что врачи не дают доступа к медицинским картам.

Согласно проведенному в 1993 году Harris-Equifax опросу, большинство американцев (87 %) полагают, что они «знают все» или «имеют общее представление, но не в курсе подробностей» о содержании своих медицинских карт. Приблизительно лишь один американец из четырех когда-либо интересовался содержанием своих медицинских карт. Только 92 % изъявившим желание это сделать, была предоставлена возможность получить копию. Среди тех, кому было отказано в этом фундаментальном праве, 31 % получили ответ, что их карты не могут найти; запрос 25 %, представляющих четыре миллиона американцев, был просто отклонен без объяснения причин.

Штаты, в которых пациентам предоставлено право на ознакомление со своими медицинскими картами

Аризона Невада

Виргиния Нью-Йорк

Висконсин Огайо

Гавайи (закон распространяется лишь на госпитали)

Джорджия

Иллинойс Орегон

Индиана (закон лишь поощряет открытый доступ)

Калифорния

Канзас Род-Айленд

(только психотерапевтические) (закон распространяется лишь на госпитали)

Теннесси

Колорадо Коннектикут Флорида

Луизиана (частичный доступ) Юта

Массачусетс (записи предоставляются адвокату пациента, но не самому пациенту)

Мэриленд (частичный доступ)

Что может разрешить эту проблему? Ложь. Скажите вашему врачу, что вы переезжаете и что копия вашей медицинской карты должна быть выслана врачу в другом штате. Конечно,

¹²³ Harris-Equifax, *Health Information Privacy Survey*, 1993.

¹²⁴ *Privacy Journal's Compilation of State and Federal Privacy Laws* (Providence: *Privacy Journal*, 1997).

вместо того чтобы называть имя какого-нибудь врача, назовите имя своего старого институтского друга, которого вы заранее предупредили и который в курсе дела. На моей практике такая уловка всегда срабатывала.

За рубежом аналогичные проблемы стоят не менее остро. Например, в Германии люди не просто не имеют права доступа к своим медицинским картам, там существует традиция скрывать диагноз «рак» и другие болезни, имеющие дурную славу в обществе, отзольного, а в некоторых случаях и от его семьи. В настоящее время в Германии создается национальный реестр раковых больных. Многих усилий требует внедрение в рамках этой системы сложных криптографических алгоритмов для сокрытия имен людей, информация о которых введена в реестр. Но криптография в данном случае применяется не для обеспечения анонимности людей и обеспечения их приватности, цель прямо противоположна: криптографические средства внедряются, чтобы раковые больные не смогли случайно узнать свой диагноз.¹²⁵

Лишение людей права на доступ к своим собственным медицинским картам неверно изначально. Уже двадцать пять лет назад разработчики «Кодекса о справедливом использовании информации» понимали, что не должно существовать записей о человеке, которые он не имел бы возможности проверить и скорректировать. Удивительно, но даже в странах с прогрессивной системой защиты личной свободы подобная практика продолжает существовать.

По иронии судьбы, повышенная доступность к своим картам для пациентов является следствием недостаточной приватности медицинской документации сегодня. Покуда врачи послушно посылают медицинские карты страховым компаниям и другим врачам, практически невозможно уберечь эти карты от рук определенных пациентов. Фактически сочетание движения за права пациентов, увеличения гибкости медицинского страхования и тенденции к самостоятельному обеспечению себя работой приведет в конечном счете к тому, что люди получат расширенный доступ к своим медицинским картам в грядущие годы. Но использование отсутствия конфиденциальности медицинских данных – порочный путь обеспечения прав пациентов.

Право на ваше прошлое

Одной специфичной группе американцев уже в течение более чем 60 лет систематически отказывается в доступе к медицинским данным, историям болезни и семейным записям. Личности этих американцев захвачены государством, запечатаны и заменены новыми, поддельными записями. Эти американцы выглядят так же, как и все остальные; многие даже не подозревают о своем секрете. Эти скрытые жертвы – те, кто был усыновлен.

Записи об усыновлении засекречиваются в Соединенных Штатах с 1930-х годов. Засекречивая эти записи, социальные реформаторы надеялись, что они одновременно смогут устранить негативное отношение как к биологической матери, имеющей «незаконнорожденного» ребенка, так и к принявшей его паре, не сумевшей завести своего. Особенную важность секретность информации об усыновлении приобрела в годы Второй мировой войны, когда много незаконнорожденных детей появлялось у женщин, чьи мужья воевали в Европе и Азии.

После формализации процесса усыновления, оказывающие эту услугу учреждения обнаружили, что секретность увеличивает степень их контроля как над биологическими родителями, так и над приемными. Наконец, гарантия тайны усыновления «очень привлекательна для приемных родителей – ребенок будет вашим, биологическая семья полностью вне игры, – говорит Эбигейл Ловит [Abigail Lovett], вице-президент

¹²⁵ J. Michaelis, M. Miller, K. Pommerening and I. Schmidtman «A New Concept to Ensure Data Privacy and Data Security in Cancer Registries», Medinfo 1995; X pt 1:661–665.

Американского конгресса по усыновлению [American Adoption Congress], организации, борющейся за реформирование законодательства по усыновлению в национальном масштабе. – Все считают, что это будет лучшим способом ведения дел». ¹²⁶

Засекречивание и рассекречивание информации об усыновлении – чрезвычайно сложный вопрос, неизменно включающий проблему аборт, родительских прав и прав ребенка. Некоммерческая организация Национальный совет по усыновлению [National Council for Adoption, NCFA] утверждает, что закрытие записей – в интересах обеспечения приватности всех вовлеченных сторон. Соккрытие имени настоящей матери усыновленного ребенка защищает ее от того, что когда-нибудь он вернется в ее жизнь. Ребенок также защищен, продолжает NCFA, от ситуации, когда мать изменит свое решение и решит вернуть ребенка. NCFA говорит также, что, если закон не будет требовать засекречивания записей, многие будущие матери предпочтут сделать аборт, чтобы избавиться от нежелательного ребенка, вместо того чтобы родить его и отдать на усыновление.

Но постоянно увеличивающееся количество усыновленных, ставших взрослыми, говорят, что тайна усыновления нарушает их неотъемлемое право знать свою личность, свое прошлое, свои медицинские данные и свою наследственность. Они настаивают, что биологические родители не имеют права поворачиваться спиной к своим детям, так же как не имеют права плохо обращаться с детьми или убивать их.

В течение многих лет Шия Грим [Shea Grimm] страдала болями в спине. Врачи проводили различные анализы и исследования, но не могли найти причину. «Они относили это на мой сколиоз», – вспоминает она. ¹²⁷ У Грим были и другие беспокойства. Она боялась, что ей грозит ранняя смерть от рака груди. Она опасалась болезней сердца. Она ничего не знала о своей наследственности. Кто были ее предки? В отличие от многих усыновленных, она знала о факте своего усыновления. Но дальше – глухая стена.

С медицинской точки зрения, фундаментальная проблема тайны усыновления заключается в том, что, после того как все бумаги оформлены и записи засекречены, по-прежнему остается существенная генетическая связь между биологическими родителями и усыновленным ребенком. Неважно, что написано в новом свидетельстве о рождении, – усыновленный ребенок не может получить гены приемных родителей. Поскольку медицина все более осознает роль использования генетической и наследственной информации для диагностирования и лечения болезней, становится ясно, что изначальная фиктивность тайны усыновления не просто неверна, она опасна.

«Я всегда задавалась вопросом, поскольку меня удочерили, должны ли врачи обследовать меня более подробно. Я не располагала большим количеством информации», – сказала Грим.

Существовало несколько причин, по которым Грим решила начать поиски своей биологической матери, поиски, которые в конечном счете увенчались успехом. После этого стали появляться ответы на ее вопросы. Она узнала, что лишь на половину является американкой. «Примерно через две недели, после того как я нашла мою биологическую мать, я узнала, что она страдает недоразвитием межпозвоночных дисков. Это позволило мне снова обратиться к своему врачу и сказать: „У меня недоразвитие межпозвоночных дисков“». Более того, Грим узнала и способ лечения. «Моя биологическая мать посещала силовые тренировки, чтобы укрепить мышцы, как ей посоветовал врач, чтобы скомпенсировать слабость дисков. Я тоже стала это делать. Это стало моим большим хобби. Это полностью изменило мой мир».

Шесть лет спустя Грим сказала, что боли в спине «беспокоят ее очень редко». В качестве приятного дополнительного вознаграждения она больше не боится рака груди: «В

¹²⁶ Интервью автору, 24 июля 1997.

¹²⁷ Интервью автору, 24 июля 1997.

истории моей семьи никогда не встречалось это заболевание».

Грим занимает пост заместителя председателя по вопросам законодательства в Bastard Nation,^[p36] правозащитной группе, объединяющей людей, знающих о своем усыновлении, и борющейся за открытие записей об усыновлении в национальном масштабе. Суть этой борьбы, говорит Шия Грим, в установлении справедливости и защите прав личности на самоопределение. «Я была лишена информации, которая позволила бы мне установить мою национальную принадлежность. Я была лишена всех тех вещей, которые люди считают само собой разумеющимися, которые помогают вам при создании семьи».

Пресс-секретарь Национального совета по усыновлению Патрик Пертил [Patrick Purtill] соглашается с тем, что медицинские данные являются одной из самых сложных проблем, с которыми сталкиваются усыновленные. Пертил говорит, что суды сообщают приемным родителям об известных проблемах со здоровьем их нового ребенка. Но проблема заключается в том, что большинство женщин, отдающих детей на усыновление, являются подростками или им всего 20 с небольшим лет, в то время как большинство опасных для жизни проблем со здоровьем (которых должен опасаться и ребенок) проявляются у женщины лишь к 30–40 годам.¹²⁸

Однако NCFA остается противником рассекречивания информации об усыновлении. Пертил аргументирует это тем, что небольшое преимущество, которое дает усыновленным доступ к их медицинским данным, будет значительно перевешено снижением числа усыновлений, которое непременно последует за этим. Вопрос в том, что принесет больше пользы, говорит он. Одним из путей решения проблемы медицинских данных, по словам Пертила, являются так называемые *реестры взаимного согласия* [mutual consent registries], в которых биологические родители и усыновленные дети регистрируют свое желание встретиться. Если обе стороны зарегистрировались, запись рассекречивается.

«Они пытаются доказать, что реестры взаимного согласия решают наш вопрос, но уже умершие люди не могут в них зарегистрироваться, – говорит Эбигейл Ловит. – И зачастую [реестры] недостаточно финансируются и недостаточно доступны».

Реестры взаимного согласия напоминают игру в одни ворота. Для того чтобы эта схема работала, усыновленный должен зарегистрироваться, а это автоматически означает, *что он должен знать о своем усыновлении*. Многие усыновленные дети не знают этого простого факта своей биографии. «Около семи лет я вела группу поддержки, – рассказывает Ловит. – В мою группу пришел 50-летний мужчина, после того как на похоронах своей матери узнал, что он был усыновлен». Но почему вдруг эта новость появилась на свет? «Жадные родственники не хотели допускать его к наследству».

В другом случае, рассказывает Ловит, она встретила женщину, которая родила ребенка с серьезными физическими недостатками. В конечном счете у женщины не было другого выбора, кроме как передать ребенка на воспитание государству. С этого же времени она стала разыскивать ребенка, которого родила в юности. «Она действительно нашла своего первого ребенка, переданного [со схожими проблемами] на попечение государства, его никто не навещал и не хотел усыновлять», – рассказывает Ловит. Очевидно, приемная семья отказалась от него, когда проблемы впервые проявились. «Она никогда бы не решилась заводить второго ребенка, если бы знала об этом». Реестр взаимного согласия никогда бы не помог этой женщине, поскольку ее «государственный» ребенок не мог быть там зарегистрирован.

Усыновление является одним из самых жестоких «открытых» секретов нашего общества. В то время как сама Ловит в течение многих лет не обладала простой информацией о факте ее усыновления, большинство людей из ее окружения знали гораздо

p36

Дословно – «нация усыновленных» (англ.).

¹²⁸ Интервью автору, 24 июля 1997.

больше. «Сразу после того как моя приемная мать умерла, доктор, который принимал мои роды, зашел ко мне в магазин и обратился ко мне по имени», – рассказывает Ловит. Но он отказался дать Ловит информацию о ее настоящей личности:

Я выросла, зная, что меня удочерили. Я знала врача, который принимал роды у моей матери. В его офисе все знали мою историю. Персонал госпиталя знал мою историю. Адвокат и его сотрудники знали мою историю. Все в моем окружении знали мою историю. Они знали обо мне больше, чем я сама. Мне же было не позволено знать свою историю. Я не могла взглянуть на свои записи о рождении; я не могла взглянуть на свои судебные записи.

Брайсейс Гатто [Briseis Gatto], усыновленный в Нью-Йорке в начале 1960-х годов, описывает это так:

Все родственники знают об усыновлении, но не сам ребенок. Вы буквально растете в обществе, где все постоянно лгут вам. Вы не смеете говорить об этом из-за боязни, что ваши родители выпнут вас, поэтому вы сами становитесь лжецом, надеясь, что, если вы не будете показывать, кто вы на самом деле, вы не будете отвергнуты, причем не только вашими родителями, но и вашими родственниками. Когда я поделился этими соображениями с моим братом, который был усыновлен примерно в то же время, что и я, он подтвердил, что он тоже так или иначе рассматривал усыновление, как нечто, о чем абсолютно недопустимо говорить с родителями, хотя они никогда не говорили ему чего-либо в этом роде.¹²⁹

Одним из способов, которым такие организации, как NCFA, решали проблему открытия записей, было заявление об этом тех усыновленных, которые действительно желают воссоединения со своими биологическими родителями. Но эта методика противопоставляла права усыновленных праву на приватность, обещанному биологическим родителям, большинство которых, утверждает NCFA, рассматривают прошлую беременность как досадный инцидент, который они хотели бы забыть. Но усыновленные и их биологические родители вполне могут избежать отношений, в которые им не хотелось бы вступать. В конце концов, существуют законы, защищающие от домогательств и навязчивого поведения.

Организации вроде Bastard Nation утверждают, что воссоединение не является решением. «Большое количество людей ищет не семью, а всего лишь информацию. Существуют права, предоставленные каждому взрослому гражданину, которых вы, как усыновленный, лишены просто по причине вашего усыновленного статуса», – говорит Дамсель Плам [Damsel Plum], заместитель председателя по связям с прессой Bastard Nation.¹³⁰

«На пороге грядущего столетия мы должны понимать всю важность для нас генетической информации, – говорит Эбигейл Ловит. – Мы знаем, что рак груди имеет генетические корни. Если вы растете, зная, что в вашей семье были случаи рака груди, вы совершенно по-другому будете организовывать свое питание и образ жизни».

В конечном счете все возрастающая доступность онлайн-информации может разрешить эту полемику. На web-сайте Bastard Nation приведены подробные инструкции по поиску биологических родителей. Там же приведены ссылки на другие онлайн-источники информации, вроде списков номеров социального страхования умерших людей, генеалогических баз данных и традиционных поисковых систем Интернета.

¹²⁹ Интервью автору, 5 мая 1999 и 23 мая 1999.

¹³⁰ Интервью автору, 24 июля 1997.

«С точки зрения возможности людей найти друг друга Интернет вскоре сделает конфиденциальность шуткой, – соглашается Даун Смит-Плинер [Dawn Smith-Pliner], возглавляющий агентство по усыновлению в Вермонте. – Фактически мы уже используем [Сеть] с этой целью здесь, в агентстве. Если кто-то хочет найти кого-то достаточно сильно, он сможет сделать это онлайн».¹³¹ Но увы, чтобы использовать эти продвинутые поисковые методики, усыновленный по-прежнему должен знать имя, дату или место. И он по-прежнему должен знать сам факт того, что он усыновлен.

Смит-Плинер считает, что конец тайному усыновлению и открытие информации об усыновлении произойдут уже в ближайшие 20 лет: «Взрослые движутся к пониманию важности связи усыновленного со своей биологической семьей. Я думаю, это произойдет и в национальном масштабе».

Мы можем лишь надеяться.

Компьютеризованные истории болезни: перспективы

Здравоохранение внедряет компьютеры уже более 20 лет, но это медленный и болезненный процесс. Сегодня мы прошли лишь половину пути. Медицина достигла больших успехов в компьютеризации кодов оплаты счетов, результатов лабораторных исследований и составлении расписания для врачей. Сегодня можно оцифровывать результаты рентгенологических исследований. А в ближайшие годы будут оцифрованы рукописные записи врачей.

Конечной целью процесса компьютеризации является создание медицинского аналога безбумажного офиса – *компьютеризованных историй болезни*. Согласно концепции, они будут содержать полную медицинскую историю пациента, включая данные о прививках, визитах к врачу, детских болезнях и результатах ежегодного обследования. Записи будут включать информацию об оплате, напоминания о необходимости контрольных осмотров в будущем и примечания. Результаты рентгенологического исследования будут оцифровываться и храниться в истории болезни, так же как и результаты лабораторных исследований.

Стремление к компьютеризации информации о пациентах частично обусловлено необходимостью более эффективно обрабатывать большие объемы информации. Многим госпиталям закон запрещает уничтожать информацию о пациентах. В результате они тратят миллионы на хранение бумажных записей в специальных хранилищах. Эта же самая информация может быть оцифрована и сохранена в объеме всего лишь в нескольких кубических футов с использованием современных технологий хранения. Экономия на площадях для хранения в сочетании со снижением затрат на фотоматериалы и их обработку – одна из причин, по которой госпитали переходят на цифровые рентгенологические системы.

Переход на компьютерные истории болезни поднимает ряд очень сложных технических вопросов. Когда вы впервые приходите на осмотр к врачу, медицинская сестра или ассистент записывают ваше кровяное давление и пульс. Как эта информация должна попадать в компьютер? Каким образом должны оцифровываться записи врача? Когда врач назначает анализы или рентгенологическое исследование, он обычно выписывает направление на листочке бумаги – это быстрее, чем вводить его в компьютер. А когда вы приходите в лабораторию, там еще больше бумаги.

Многие из этих проблем решаются при помощи современных технологий в сочетании с новыми методиками ведения дел. Например, в госпитале, который я посетил в Сиэтле, врач надиктовывает свои записи на магнитофон. После этого они в электронном виде пересылаются в Индию, где имеется дешевая рабочая сила, а английский язык широко

¹³¹ Интервью автору, 24 июля 1997.

распространен. Сотрудники со специальной подготовкой прослушивают запись и набирают ее на компьютере, после чего текст отсылается обратно через компьютерные сети.

Производящая фотопленку японская компания Fuji тем временем разработала электронную пластину, чувствительную к рентгеновским лучам. Она может быть использована со стандартным рентгеновским оборудованием и обеспечивает непосредственную оцифровку рентгенограммы и пересылку ее в компьютер. Эта пластина стоит около тысячи долларов, но ее можно использовать многократно, что дает существенную экономию на фотоматериалах. А поскольку рентгенограммы оцифрованы, они могут храниться на магнитной ленте, что не требует дорогостоящего хранилища с климат-контролем.

Одним из факторов, повышающих стоимость медицинского обслуживания, является большое количество повторных анализов. Анализы повторяются по причине утери предыдущих результатов или потому, что пациент переходит в другое учреждение, а его записи не пересылаются. А 1997 году законодательская инициатива Кеннеди-Кассебаума о переносимости в здравоохранении [Kennedy-Kassebaum healthcare portability legislation] стала попыткой решить проблему повторных анализов путем принуждения медицинских учреждений к принятию универсального медицинского идентификационного номера [universal healthcare identification number]. Идея законопроекта была проста: если все медицинские учреждения и врачи будут использовать одни и те же идентификационные номера, то меньше шансов, что результаты анализов будут потеряны. Основным аргументом за принятие закона было «упрощение административных процедур». Однако его реализация была временно приостановлена конгрессом, в основном благодаря протестам групп защиты приватности.

Как только медицинские карты будут переведены в компьютерную форму, информация из них может быть использована в совершенно иных целях. Одной из простейших методик является сканирование новых записей в карте пациента при его явке и памятки с напоминанием о необходимости сдачи очередных анализов. Эти памятки напоминают, чтобы женщина сдала мазок Папаниколау (ПАП-мазок) и сняла маммограмму; проинформируют родителей о необходимости провести у детей анализ на содержание свинца; они даже могут напомнить взрослым о необходимости регулярного контроля кровяного давления и уровня холестерина. Напоминания формулируются на английском языке и печатаются на карточке пациента. Когда пациент обращается с заболеванием или приходит на профилактический осмотр, врач видит эти напоминания и во время приема назначает необходимые процедуры.

Когда специалист по информатизации в сфере медицины из Вашингтонского университета доктор Гарольд Голдберг [Dr. Harold Goldberg] впервые предложил идею памяток своим коллегам-врачам, они посмеялись над ней, заявив, что в состоянии запомнить, какие процедуры какому пациенту требуются. Но когда программа была реализована, произошло нечто удивительное: количество анализов, которые необходимо было сдать пациентам резко подскочило.

Сегодня такие напоминания являются стандартной практикой в медицинской индустрии. «Семнадцать различных контрольных исследований подтвердило, что напоминание врачу перед началом приема увеличивает вашу возможность [получить направление на необходимые анализы] на 70 %», – говорит Голдберг.¹³²

Компьютеризованные истории болезни: угрозы

Врачи не строят оптимистичных иллюзий относительно угроз, которые возникают в связи с компьютеризацией историй болезни. Согласно проведенному в 1993 году Harris-Equifax опросу, 74 % врачей считают, что компьютерные системы «почти наверняка

¹³² Интервью автору, 29 апреля 1997.

ослабят» сохранность медицинской тайны, напротив, 26 % считают, что компьютеры «могут обеспечить бо льшую конфиденциальность».

Проблема проистекает из различия между физической и электронной формой представления. Физической формой являются записи на бумажном носителе. Они могут существовать в данный момент времени лишь в одном месте. Чтобы отправить копию этих записей по факсу, человек должен иметь к ним физический доступ.

Основное преимущество электронных записей заключается в том, что ими легко манипулировать, но эта легкость двоякая. Маловероятно, что анализы крови в электронном виде будут утеряны. Это хорошо для пациентов, особенно тех, которые не любят, чтобы их лишний раз кололи иглой. Но равным образом компьютерное представление данных дает возможность любопытной медсестре или практиканту подойти к оставленному без присмотра терминалу, набрать имя человека и получить доступ к результатам анализов. А поскольку к компьютерному файлу можно получить доступ одновременно с сотен расположенных по всему госпиталю терминалов, задача контроля становится неимоверно сложной.

В отчете, опубликованном в 1997 году Национальным советом по исследованиям, выделено пять «уровней угроз» информации, хранимой в медицинских компьютерах.¹³³

1. *Инсайдеры (законные пользователи системы), которые совершают «невинные» ошибки, приводящие к случайному разглашению конфиденциальной информации.* Это могут быть такие простые ситуации, как посылка результатов лабораторного исследования по факсу на ошибочный номер или передача медсестрой записей одного пациента вместо другого.

2. *Инсайдеры, превышающие свои полномочия по доступу к информации.* Просмотр является распространенной проблемой во многих электронных системах хранения информации. В Налоговом управлении всегда существовала проблема любопытных служащих, просматривающих налоговую документацию, к которой они имели доступ. Было бы наивным полагать, что госпитали могут так или иначе избежать этой беды.

3. *Инсайдеры, которые осуществляют доступ к информации злоумышленно или с целью наживы.* Во время предвыборной кампании Демократической партии в 1992 году к одному моему знакомому патологоанатому из Beth Israel Hospital в Бостоне обратился представитель прессы, желавший получить доступ к медицинским данным кандидата Пола Цонгаса [Paul Tsongas]. Репортер предложил неплохие деньги, и менее этичный врач мог бы легко достать нужный файл, не оставив при этом следов.

4. *Физический нарушитель, получивший доступ к информации, не имея на то права.* Многие госпитали полагаются на физические меры обеспечения безопасности хранимой в компьютерах информации: терминалы размещаются в специальных помещениях или за стойками, куда должен иметь доступ только допущенный персонал. Но журналист мог просто надеть белый халат, фальшивую табличку с именем и получить доступ к данным Цонгаса без посторонней помощи.

5. *Обиженные служащие и внешние нарушители, такие как желающие отомстить пациенты или нарушители, планирующие несанкционированный доступ к информации, повреждение систем или прерывание операций.* Работающий в НМО врач рассказал мне о проблеме, с которой столкнулась его группа: один из служащих – они предполагали, кто именно, – проникал в компьютер, на котором хранилось расписание работы врачей, и удалял записи о назначенных визитах пациентов. В регистратуре думали, что данное время свободно и назначали его для других; в результате на прием одновременно являлось два или три пациента.

Существует большое количество методик, которые можно использовать для

¹³³ *Protecting Electronic Health Information*, Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, national Research Council (Washington, DC, 1997).

минимизации угрозы несанкционированного доступа. Например, в Beth Israel Hospital файлы некоторых пациентов помечены как *VIP*. Когда к этим файлам осуществляется доступ (с любой целью), имя осуществившего его сотрудника записывается в журнал; в обязанности специально назначенного человека входит регулярный аудит этих журналов для контроля того, что все попытки доступа законны.

Кто же должен быть отнесен к категории *VIP* ? В настоящее время госпиталь помечает файлы как *VIP*, если имеются достаточные основания полагать, что сотрудники госпиталя могут интересоваться информацией о данном человеке. Известные люди и политики являются первыми кандидатами на это.

Но служащие госпиталя и члены их семей также получают данный статус, чтобы сократить число обращений к информации со стороны любопытных (или имеющих самые добрые намерения) коллег. В идеале все, кто хочет получить *VIP*-статус, должны получать его. Но на практике Beth Israel Hospital не уведомляет пациентов, что они имеют на это право.

Некоторые компьютерные специалисты видят простое решение проблемы компьютеризованных историй болезни в использовании криптографических методов. Выдайте каждому копию его истории болезни, помещенную на смарт-карту. Для защиты от хищения карты сохраните копию медицинских записей где-нибудь еще и зашифруйте ее, чтобы исключить несанкционированный доступ.

Но врачей беспокоит такой технократический подход к решению проблемы с использованием криптографии. Они опасаются, что в экстренных случаях может оказаться невозможным расшифровать или даже найти медицинские записи человека. Большинство людей, аргументируют они, не желают умирать за свое право на приватность.

Другие угрозы

Компьютеризация подвергает приватность и другим рискам, которые только сейчас становятся очевидными. Вспомним услугу по расшифровке диктофонных записей в Индии. Что, если служащий индийской фирмы узнает имя пациента, чью запись он расшифровывает и решит продать эту информацию какой-нибудь бульварной газете в Америке? Даже если предположить, что расследование утечки информации выведет на этого служащего, трудно представить, какое адекватное наказание он может понести.

Но компьютеризация также дает возможность обеспечить пациентам повышенный уровень конфиденциальности. Служащий в Индии не нуждается в имени пациента, чью запись он расшифровывает, – вполне хватит цифрового кода. При этом, вместо того чтобы использовать в качестве кода номер социального страхования, надо брать случайное число, время, в которое пациент был на приеме, или другой код, сгенерированный госпиталем, пославшим аудиозапись на расшифровку. Обработываемая запись будет, по существу, анонимной, по крайней мере с точки зрения сотрудника в Индии.

Возможно, способность компьютеров обезличивать и скрывать информацию является причиной, по которой чуть больше половины (53 %) главных администраторов госпиталей считают, что компьютеры действительно обеспечат пациентам большую конфиденциальность. Среди руководителей страховых компаний этот процент больше – 61, по сравнению с 35 %, считающими, что компьютеры нарушают конфиденциальность.

В чем причина различия взглядов администраторов и врачей? Возможно, она кроется в том, что администраторы знают возможности информационных технологий, а врачи видят реальное положение вещей. Врачи также знают, что любая технология, затрудняющая доступ персонала госпиталя к медицинской информации, может стоить жизни пациенту. Даже простые обезличивающие коды повышают риск того, что записи двух пациентов могут случайно перепутаться, и это может повлечь тяжкие последствия. Хотели бы вы, чтобы вам оказывали помощь в палате интенсивной терапии, где компьютеры требуют от персонала введения имени и пароля для получения доступа к анализам?

Когда в медицинском центре Вашингтонского университета была внедрена компьютерная система доступа к медицинским данным, каждому врачу и медсестре были выданы имя и пароль. Система была спроектирована таким образом, чтобы каждое обращение персонала к информации протоколировалось в журналах. В системе даже был предусмотрен таймер неактивности, т. е., если кто-то покидал терминал, с которого он вошел в систему, через некоторое время таймер автоматически отключался. Проведенный месяц спустя анализ журналов показал, что единственным человеком, входящим в систему из одной палаты, был старший ординатор. Осмотр терминала показал, что имя и пароль этого врача были написаны на листочке и приклеены к терминалу, поэтому любой находившийся поблизости врач или медсестра могли при необходимости войти в систему под его именем.

Сегодня мы можем представить гораздо более простое и элегантное решение проблемы учета доступа к медицинской информации в учреждениях, вроде этого медицинского центра. Во-первых, обеспечить установку терминалов в защищенных местах, чтобы только авторизованный персонал мог получить доступ к записям пациентов. После чего установить над каждым терминалом небольшую видеокамеру, чтобы записывалось изображение человека, осуществившего доступ. Создание таких систем видеозаписи вполне возможно уже сегодня.

Переосмысление медицинского обслуживания и медицинского страхования

Большинство американцев считают записи в своих медицинских картах одной из самых критичных составляющих персональной информации. Но для медицинских объединений и страховых компаний медицинская документация всего лишь партитура для сложной игры в «музыкальные стулья». [p37] Страховая компания знает, что, если она будет ждать слишком долго, велик шанс того, что данный пациент будет перехвачен другой страховой компанией по причине того, что он или его компания изменили предпочтения, или он потерял работу, или потому, что достиг 65-летнего возраста и теперь попадает под программу Medicare – американскую социальную программу медицинского страхования для пожилых людей. Страховые компании с высокой текучестью клиентов не заинтересованы продвигать профилактическое медицинское обслуживание и закрывают глаза на ранние дешевые в лечении стадии многих заболеваний, надеясь, что когда болезни начнут прогрессировать, пациент уже будет вне их зоны финансовой ответственности.

Если говорить о новых контрактах, то эксперты страховых компаний используют медицинские данные так же, как букмекеры используют спортивные рейтинги, – в качестве оценочных карт при расчете прибыли. Фактически такая оценка является основной работой при страховании жизни и здоровья.

По сути, процесс экспертизы состоит в оценке соотношения прибыли от уплачиваемого клиентом страхового взноса и вероятных страховых выплат. Процесс нельзя отнести к точным наукам, но результаты тем точнее, чем больше информации соберет страховая компания. И почти не существует ограничений на то, какая информация может быть использована. Сегодня страховая компания считает, что человек с повышенным кровяным давлением или уровнем холестерина относится к группе повышенного риска и соответственно повышает для него страховые ставки; завтра страховая компания начнет изменять ставки ежемесячно, в зависимости от съеденного вами количества пищи.

Большинство описанных в этой главе проблем могут быть решены путем кардинального изменения системы оплаты медицинского страхования в Соединенных Штатах. Вместо того чтобы привязывать медицинское страхование к занятости (практика,

существующая со времени введения контроля над заработной платой и ценообразованием в 1940 году), медицинское страхование должно быть привязано к оседлости и гражданству. Простейший способ положить конец дискриминации в медицинском страховании заключается в принятии единой государственной системы медицинского страхования. Однако сделать это невозможно по причинам политическим, учитывая объем капитала, вращающегося в страховой индустрии, – индустрии, зарабатывающей деньги на азартной игре с жизнями здоровых и болезнями больных людей.

При отсутствии возможности глобальной реорганизации лучшим способом защиты потребителей является сочетание прозрачности и регулирования – *прозрачности* деятельности страховой индустрии для предотвращения наиболее вопиющих случаев нарушения приватности и *регулирования*, призванного защитить потребителя в его ежедневных отношениях с медицинскими учреждениями. Без кардинальной смены политики положение будет лишь ухудшаться.

7

Купите прямо сейчас!

Издатель *Privacy Journal* Роберт Эллис Смит встретился на конференции в Нью-Йорке с вице-президентом одной из крупнейших маркетинговых компаний Америки, человеком, который косвенно повинен в миллиардах непрошенных писем и почтовых карточек, каждую неделю заполняющих дома американцев. Поэтому Смит спросил вице-президента, что американцы могли бы сделать, чтобы остановить поток почтового мусора, с которым они сталкиваются каждый день.

«Такой вещи, как почтовый мусор не существует, есть лишь мусор у людей», – поправил вице-президент Смита, удивленного одновременно искренностью и грубостью ответа.

Заявление вице-президента абсолютно точно, если рассматривать его с позиции продавца. Все эти рекламные предложения в вашем почтовом ящике, телефонные звонки, отрывающие вас от обеда и постоянный «спам», засоряющий вашу электронную почту, являются мусором, если вас не интересует предлагаемый товар или услуга. Для вас это мусор. А для кого-нибудь другого это может быть золотой возможностью.

Давайте теперь попробуем посмотреть на ситуацию с другой стороны – глазами продавца. Если человек не интересуется предлагаемым продуктом или услугой, с точки зрения продавца, – он мусор. Ни один нормальный продавец не хочет рассылать почту, которая отправится в корзину не будучи вскрытой.

Самим фактом своего существования «мусорные потребители» приводят к затратам времени и денег продавца.

Хороший продавец знает, что бесполезно рекламировать собачью еду владельцам кошек. Но маркетинг не относится к точным наукам. Когда сектор экономики, в котором крутится не один миллиард долларов, начинает наполнять конверты и шлепать на них почтовые марки, определенное количество ошибок неизбежно. Хорошие продавцы не любят почтовый мусор, потому что знают – этот мусор непосредственно обращается в недополученную прибыль. Вместо того чтобы злиться на компании, которые вторгаются в вашу жизнь, вы должны чувствовать себя виноватыми перед ними.

Совершенно ясно, что и потребители и продавцы хотят одного – остановить поток почтового мусора и телефонных звонков. Но борьба идет за средства. Все больше потребителей борется за введение ограничений на агрессивную маркетинговую политику. Но маркетинговая индустрия выбирает другой подход. Она использует огромные хранилища персональной информации для оттачивания своих рекламных кампаний. Она использует методики обмана для вытягивания критичной информации о родителях и детях, так что все мы являемся мишенями с самого рождения. Она стремится к тому, чтобы каждая

поверхность и каждый момент времени был использован в рекламных целях, чтобы потребители никогда не упускали шанса быть хорошо проинформированными.

Вырвавшийся из-под контроля маркетинг превратился в кампанию, которая оплачивается корпорациями по безостановочному навязчивому преследованию. Эта кампания в конечном счете коснется каждого мужчины, женщины и ребенка на планете. Она должна быть остановлена.

Маркетинг и кризис познания

Через несколько недель после того, как я купил свой первый дом, я получил почтовую карточку от биржевого брокера из Бостона, предлагавшего мне связаться с ним, чтобы обсудить, куда я могу инвестировать сбережения. Несколько дней спустя я получил карточку от чистильщика каминов, предлагавшему мне назначить время для чистки трубы.

И брокер, и трубочист получили мое имя в Кембридже: информация о сделках с недвижимостью является общедоступной. Оба понесли некоторые затраты на эту маркетинговую акцию – в размере стоимости почтовой марки. И оба сработали впустую: после покупки дома у меня не было свободных денег для игры на бирже, а в моем доме не было камина, так что в нем нечего было чистить.

Эти рекламные предложения оставили у меня ощущение насилия. Просто посмотрев на мое имя, эти люди решили, что они узнали некоторую персональную информацию обо мне, и попытались использовать ее для манипулирования моим поведением. Фактически сделав неверные выводы на основе неполной информации, они так или иначе ухудшили ситуацию.

Определение целевой аудитории используется в бизнесе не одно десятилетие, но эта практика становится просто невыносимой, когда компании начинают использовать все большее количество персональной информации для повышения эффективности, нарушая нашу приватность и делая в этом процессе неизбежные ошибки.

Просто спросите Синди Роуэн [Cindy Rowan].

В сентябре 1995 года мать Синди Роуэн погибла в автомобильной аварии. «Она отличалась отменным здоровьем, и все испытали настоящий шок, когда это произошло, – рассказывала мне Синди в 1996 году. – После ее смерти я попросила пересылать ее почту мне домой» (в Фармингдейл, штат Нью-Джерси¹³⁴).

Заполнение уведомления о смене адреса запустило огромную рыночную машину, которую Роуэн даже не могла себе представить, машину, которую нечего и надеяться контролировать. Несмотря на гарантии в бланке (и политику правительства США), что информация о смене адреса будет использована только для перенаправления почты, очень скоро информация стала использоваться торговцами по продаже земли.

Местный супермаркет Фармингдейла прислал матери Роуэн приветственное письмо в связи с переездом и приложил купон на бесплатный апельсиновый сок. Флорист прислал ей 10 %-ный купон-скидку на покупку цветов. Даже дантист по новому месту жительства прислал карточку – конечно, проще осматривать зубы в Фармингдейле, чем ехать за 40 миль к старому дантисту.

Примерно в течение полугода после аварии Джейн Сейс [Jane Seiss], погибшая мать Роуэн, получала через почтовый ящик дочери больше корреспонденции, чем сама Роуэн. А почему нет? С точки зрения продавцов, Джейн Сейс имела очень перспективные характеристики. Находясь на пенсии в добром здравии (продавцы не запрограммировали свои компьютеры проверять некрологи), Сейс потенциально могла бы быть лояльным клиентом в течение многих лет. Со стороны компаний было бы глупо не связаться с ней!

Но в данном конкретном случае каждое письмо, посланное ее погибшей матери, причиняло Синди Роуэн боль. «Я устала от этого. Это очень злило меня, – говорит Роуэн. – Я

¹³⁴ Интервью автору, 22 февраля 1996.

думаю, что люди, покупающие эти списки, даже не задумываются о том, какое влияние это может оказать на кого-либо».

Американская почтовая служба обещает, что 42 миллиона запросов на смену адреса, которые она получает ежегодно, используются только для пересылки почты, но не для продажи продуктов. Примечание на бланке гласит:

ОБЕСПЕЧЕНИЕ ПРИВАТНОСТИ: Заполнение этого бланка является добровольным, но ваша почта не сможет быть перенаправлена без запроса. После заполнения ваш новый постоянный адрес будет предоставляться компаниям и отдельным гражданам, которые запросят его. Это будет возможно, *только если* проситель знает ваше имя и ваш старый адрес. Используйте форму 3576 для информирования корреспондентов и издателей о смене адреса. Утверждено 39 U.S.C. 404.

Но, как мы увидим, система, призванная защищать поток персональной информации, как и многие другие системы в бизнесе, оказалась порочной. Почтовая служба между тем имеет очень слабую позицию, чтобы протолкнуть реформы. Как я покажу далее в этой главе, Национальная программа смены адресов [National Change of Address Program] на самом деле поддерживается теми же компаниями, которые ежегодно рассылают десятки миллиардов порций «почтового мусора» сотням миллионов американских потребителей.

Информация о сделках с недвижимостью и записи о смене адреса – всего лишь два вида правительственных данных, неправомерно используемых для маркетинговых целей. Другой богатый источник информации – данные о регистрации транспортных средств. Бесспорный лидер в этой области The Polk Company, которая торгует персональной информацией со дня своего основания в 1870 году.

Первым продуктом Polk стал бизнес-справочник Мичигана, отсортированный по железнодорожным станциям. Цель создания этого справочника заключалась в том, чтобы облегчить покупателям, живущим рядом с одной станцией, совершение покупок рядом с другой станцией. Но вскоре компания обнаружила, что больше денег можно заработать, продавая информацию о жителях города торговцам, предлагающим товары на дому.¹³⁵ В XX веке Polk стала крупнейшим регистратором транспортных средств. Для автомобильной промышленности Polk использует эти данные при необходимости отыскать владельцев в случае отзыва партии машин по соображениям безопасности. Для всех остальных Polk комбинирует данные о марке и модели вашего автомобиля с данными переписи населения, чтобы дать продавцам информацию о ваших доходах, стиле жизни и предпочтениях в приобретении заданных товаров.

Люби меня, люби мои приобретения

К началу XXI века маркетинг все больше ориентируется на персональный подход. Продавцы больше не удовлетворяются толпой потенциальных клиентов, выловленных из списков рассылки или правительственных данных. Они агрессивно ищут персональную информацию и создают компьютерные системы для классификации индивидуальных клиентов.

Сегодня большинство супермаркетов оборудовано лазерными сканерами, которые считывают штрих-код с каждой покупки и записывают его в компьютерный банк данных. Когда вы передаете служащему платежную карточку, вы фактически даете ему идентификационную карту, которая помечает покупки вашим именем. Продавцы используют эту информацию для составления подробных портретов покупателей.

Компании сами толком не знают, что им делать со всей этой информацией. Планы, о

¹³⁵ Westin, *Databanks in a Free Society*, p. 156.

которых они сообщают, невообразимо мягкие и невинные – вплоть до адресной рассылки купонов на Pepsi-Cola постоянным потребителям Coca-Cola. «Мы будем использовать это [портрет покупателя] для определения наших лучших клиентов, чтобы затем стимулировать их делать больше покупок в нашем магазине путем предоставления дисконтов, скидок и других подобных вещей», – говорит Норманн Цанг [Norman Tsang], директор по маркетингу Star Market в Бостоне.¹³⁶



Клиентская карточка супермаркета

Большинство супермаркетов в Соединенных Штатах имеют сегодня клиентские программы. Разработанные специально для постоянных покупателей, эти программы дают клиентам скидку за подробное отслеживание всех покупок. Владельцы супермаркетов используют эту информацию в различных целях, таких как смена дизайна магазина, ценообразование и маркетинг. Но ничто не ограничивает то, как супермаркет может использовать данную информацию. Известен прецедент, когда покупатель поскользнулся и упал в торговом зале, затем выступил с иском против супермаркета, который, в свою очередь, пригрозил обнародовать информацию о том, что истец часто покупает алкогольные напитки, чтобы подпортить ему репутацию в суде. [Фото любезно предоставлено Крисом Рейли (Chris Reilley), Reilley Design]

Но фактически данные по транзакциям – просто золотое дно. Изучая привычки отдельных покупателей в течение недель и месяцев, комбинируя их с технологиями индивидуального маркетинга, магазин может узнать, какой эффект оказывают рекламные акции на определенных посетителей. Star Market может экспериментально определить, требуется ему выпускать 10-центовые или 50-центовые купоны-скидки для стимулирования определенных категорий покупателей на совершение покупок. Он может точно установить, какие купоны приводят к увеличению продаж, а какие – нет. После этого они могут выборочно посылать купоны именно тем клиентам, которых купоны заставили сделать покупку, и не давать скидку всем подряд. Информация на уровне транзакций превращает искусство маркетинга в многовариантный научный эксперимент, в котором клиенты супермаркета выступают в роли лабораторных крыс.

Но супермаркеты могут пойти гораздо дальше, чем обычные психометрические исследования. Согласно мартовскому номеру 1999 года *Privacy Journal*, многие делают это уже сегодня:

Американское управление по борьбе с наркотиками уже запросило доступ к информации о постоянных покупателях Smith's Food & Drug Centers в Аризоне. Роберт Ривера [Robert Rivera] из Лос-Анджелеса рассказывал, что когда он повредил ногу после падения в супермаркете Vons и предъявил ему иск по этому поводу, администрация супермаркета просмотрела записи о его покупках и заявила, что использует для защиты на судебном процессе тот факт, что он покупал много ликера, и мог получить травму еще до

¹³⁶ Интервью автору, 20 февраля 1996.

падения в супермаркете.

Владелец Lees Supermarket в Вестпорте, штат Массачусетс, говорит, что использует эту информацию для определения покупательных привычек своих постоянных клиентов с тем, чтобы идти навстречу их нуждам.¹³⁷

Владельцы супермаркетов могут перепродавать эту информацию по своему усмотрению. Сегодня большинство данных о продажах имеют маркетинговое значение. Например Absolut Vodka может приобретать списки товаров, покупаемых вместе с водкой, для использования этой информации в будущих рекламных кампаниях Absolut, которые часто используют рекламу нескольких брендов одновременно. Но завтра эта информация легко может быть предоставлена страховым компаниям, медицинским организациям и даже правительственным следователям. Другое применение этой информации – научные исследования в области здоровья и диетологии. Информация на уровне транзакций дает возможность бизнесу и правительству обыскивать ваш дом и изучать вашу жизнь во всех подробностях, не получая на то разрешения и не переступая порог вашего дома. Не едите ли вы слишком много говядины или жирного мороженого? Не превышают ли ваши расходы уровень ваших доходов? Ваш кассовый чек расскажет об этом.

Наши тела, наши доллары

В 1995 году я получил письмо с просьбой о пожертвовании денег от одного из крупнейших госпиталей Бостона – Beth Israel Hospital. Случайно это или нет, но незадолго до этого я обращался в этот госпиталь. Я написал письмо руководителю госпиталя с жалобой на то, что он использует карты пациентов для сбора средств. Директор ежегодного фонда госпиталя Холли Глик [Holly Glick] написала в ответ:

Я думаю, вы согласны, что для таких учреждений, как Beth Israel Hospital, очень важно заниматься сбором средств организованным путем. Подразумевается в том числе и периодическая рассылка запросов практически всем людям, которые были когда-либо нашими пациентами, конечно, за исключением случаев, когда они умерли или есть другие причины не обращаться к ним.

Подобные запросы не являются непродуктивными, и, поскольку деньги идут на благое дело, такая практика будет продолжаться. Безусловно, такие просьбы вызывают неловкость, однако очень важно не рассматривать эти запросы как что-то личное, но как часть общих усилий по обеспечению финансирования услуг для тех, кто не может их оплачивать, и академической деятельности нашего учреждения, которая оплачивается лишь частично.¹³⁸

Холли Глик может думать, что такая практика ее госпиталя правильна, но, согласно проведенному в 1993 году Harris-Equifax опросу,¹³⁹ 66 % американцев считает, что «неприемлемо» использовать регистрационные записи госпиталя для сбора средств.

Маркетинговая кампания госпиталя Beth Israel этически уязвима, если рассматривать ее с позиций приватности, поскольку госпиталь рассылает просьбы о помощи не случайным людям, а лишь своим бывшим пациентам. Когда человек получает такое письмо, сам по себе конверт уже разглашает информацию о том, что данный человек был пациентом госпиталя. И этот конверт может повлечь ужасные последствия для человека, пытающегося скрыть сам факт получения им медицинской помощи, например для женщины, сделавшей аборт или

¹³⁷ *Privacy Journal*, март 1999, p. 5.

¹³⁸ Из личной переписки, 1995.

¹³⁹ Harris-Equifax, *Health Information Privacy Survey*, 1993, p. 4.

избитой своим мужем, которой угрожают новые побои в случае, если он узнает, что она обращалась за помощью. Последователю учения «христианской науки» такое письмо может доставить особое беспокойство, поскольку эта религия негативно относится к медицинской практике, считая ее недопустимым вмешательством в дела Бога. В феврале 1997 года Лойс Ратерфорд [Lois Rutherford] получила письмо с просьбой о финансовой помощи, адресованное ее мужу, который проходил лечение от рака в госпитале Alberta (Эдмонтон, Канада). «Больше всего меня огорчило то, что он умер именно в этом госпитале», – сказала она.¹⁴⁰

Даже аптечные записи используются сегодня для маркетинга. Одна из крупнейших компаний в этой области, National Data Corporation, покупает подробную информацию о выписанных рецептах почти у 30 тысяч аптек по всей стране. Данные обрабатываются и продаются фармацевтическим компаниям, которые могут сравнить, как продаются в различных регионах их препараты по сравнению с конкурентами. Эта информация обобщается и используется отделами продаж для лоббирования определенных препаратов среди врачей. Фармацевтические компании также проводят рекламные акции, направленные непосредственно на потребителей, поскольку знают, что врачи с большей охотой выписывают препарат, который просит пациент.

Продажа самым юным потребителям

Даже детей стали использовать в маркетинговых целях. Через телевидение и рекламу в школах, создавая ориентированные на детей сайты в Интернете, продавцы нашли эффективный способ обходить родителей. Например, в начале 1990-х, владельцы 900-й серии номеров [p38](#) запустили рекламу, приглашавшую детей позвонить по этим номерам, где они могли услышать предварительно записанные голоса персонажей мультфильмов, а их родители получали в результате счета на кругленькие суммы. Такая практика стала незаконной после принятия в 1992 году Telephone Disclosure and Dispute Resolution Act, [p39](#) после чего многие продавцы переключились на Интернет, как новую ничем не регулируемую среду, где можно использовать детей.

«Онлайновые технологии позволяют продавцам отслеживать модель поведения детей: какие сайты они посещают и как долго на них задерживаются», – сказал в июле 1997 года специальный уполномоченный Федеральной комиссии по торговле Роско Старек [Roscoe B. Starek]:

Используя вопросники – зачастую в виде регистрационных форм, которые должны быть заполнены для получения доступа к сайту или необходимы для участия в розыгрыше приза, – владелец сайта может собрать очень ценную маркетинговую информацию. Вся эта информация помогает продавцам с минимальными затратами находить новых потребителей и может позволить компаниям очень точно работать с клиентами в соответствии с их индивидуальными интересами.¹⁴¹

¹⁴⁰ Smith, *War Stories II*, p. 17.

[p38](#)

Номера телефонов, используемые для предоставления платных услуг.

[p39](#)

Закон о «раскрытии» (т. е. явном описании) услуги, оказываемой по телефону, и разрешении споров. Закон защищает как компании, предоставляющие платные услуги по телефону (от не желающих платить клиентов), так и потребителей. В частности, он предписывает точно информировать потребителя о платности услуги, стоимости единицы времени услуги и предполагаемой продолжительности услуги (разговора), а также необходимости получения разрешения на пользование услугой от родителей абонентов, не достигших 18 лет.

¹⁴¹ «The ABCs at the FTC: Marketing and Advertising to Children», Summary of Prepared Remarks of Commissioner Roscoe B. Starek III, Federal Trade Commission, Advertising and Promotion Law 1997, Minnesota

И это происходит, говорит Старек, несмотря на то что «97 % родителей, чьи дети пользуются Интернетом, считают, что web-сайты не должны накапливать информацию об именах и адресах детей, а также продавать или предоставлять ее во временное пользование третьим лицам». Даже когда компания гарантирует, что идентифицирующая личность информация не будет никому передаваться, 72 % родителей все равно против такой практики.

Родителям почти невозможно составить обоснованное мнение о том, кто запрашивает информацию об их детях: не существует простого способа отличить законный web-сайт от жульнического. Более подходящей альтернативой является государственное регулирование индустрии, установка стандартов надлежащего поведения и наказание компаний, переступивших черту.

Например, в 1996 году Федеральная комиссия по торговле начала расследование деятельности web-сайта под названием KidsCom.¹⁴² Этот сайт содержал привлекательную графику и бесплатные игры, но, для того чтобы поиграть, дети должны были зарегистрироваться. Регистрация была не простым делом: необходимо было заполнить сложную форму, в которой указывались возраст, дата рождения, пол, состав семьи, любимое телевизионное шоу, любимый коммерческий телеканал, любимая музыкальная группа, хобби, способ доступа в Интернет, корректный адрес электронной почты, адрес электронной почты родителей или опекунов, обычный почтовый адрес, скорость соединения с Интернетом и планы будущей карьеры. В целом ситуация вызвала большой резонанс в прессе: защитники прав потребителей говорили, что KidsCom использовал детей, которые не могли самостоятельно принять обоснованное решение о сообщении персональной информации. Владельцы сайта утверждали, что они задавали эти вопросы детям, чтобы вовлечь их в электронную программу дружбы по переписке и представлять им индивидуально подобранное содержание. После длившегося год расследования KidsCom добровольно изменил свою политику, создал консультативный родительский совет и принял кодекс приватности.

Примерно в то же время, когда шло расследование деятельности KidsCom, компания The Walt Disney Company запустила web-сайт стоимостью не один миллион долларов, единственной целью создания которого было продвижение продуктов компании и сбор маркетинговой информации. В отличие от KidsCom, Disney не принял жесткой политики в отношении разглашения имен и личностей детей. Напротив, «политика приватности», опубликованная на сайте в 1996 году, гласила:

«Предоставленная во время регистрации информация может быть использована для маркетинговых и рекламных целей компанией The Walt Disney Company, а также совместно с другими компаниями, по выбору The Walt Disney Company».¹⁴³

Но потом произошло нечто очень важное: конгресс Соединенных Штатов принял закон, который однозначно признавал незаконными самые ужасные злоупотребления компаний типа KidsCom и Disney. Принятый в 1998 году «Закон о защите конфиденциальности детей в Интернете» [Children's Online Privacy Protection Act] требовал от web-сайтов четкого указания, какую информацию они собирают от детей до 13 лет и в каких целях она будет использоваться. Закон также требовал от web-сайтов получения

Institute of Legal Education, 25 июля, 1997. Доступно в Интернете по адресу <http://www.ftc.gov/speeches/starek/minnfin.htm>.

¹⁴² Адрес KidsCom в Интернете <http://www.kidscom.com>.

¹⁴³ Адрес Disney в Интернете <http://www.disney.com>.

«подтвержденного разрешения родителей», т. е. принятия «разумных усилий» для подтверждения того, что передача детьми любой информации разрешена родителями.

После того как закон был принят, FTC приняла меры против компании GeoCities, предоставляющей услуги хостинга, и Liberty Financial Companies, владеющей web-сайтом «Юный инвестор» [Young Investor], за неподчинение требованиям законодательства. Тем временем Disney и другие сайты в значительной степени изменили свою тактику. Действия FTC доказали, что одного лишь закона без установления соответствующего контроля, недостаточно для защиты приватности. Но действия FTC доказали также и то, что без закона вообще невозможно установить какой-либо контроль. Несмотря на то что использование детей в маркетинговых целях остается сегодня серьезной социальной проблемой, положение дел с этим законом лучше, чем было без него.

Добавь звук

Использование детей в маркетинге лишь одна из многих попыток компаний «добавить звук» за последнее время. Такая практика идет рука об руку с другой тенденцией, наметившейся в маркетинге, – попыткой коренным образом увеличить количество рекламы в окружающем нас мире:

- бросьте монетку в телефон-автомат и, до того как он соединит вас, вы, скорее всего, услышите краткий анонс, содержащий имя владельца этого автомата: «Спасибо, за то, что вы воспользовались телефоном Bell Atlantic»;
- купите тур в Massachusetts Turnpike и вы обнаружите на счете рекламу поставщика канцелярских скрепок;
- по крайней мере одна компания экспериментирует с купонами, печатающимися на выдаваемых банкоматом чеках; не только потому, что такая реклама увеличивает объем продаж, это еще позволяет магазинам идентифицировать покупателей, рассчитывающихся наличными, и накапливать ценную демографическую информацию о них;
- сегодня рекламу можно вставить посредством компьютерного монтажа при показе спортивных соревнований в ограждение площадок и на газон.

Любое устройство, оснащенное дисплеем, потенциально может стать рекламной машиной. Microsoft первая пошла по этой дороге в 1997 году, когда выпустила вызвавший много споров Internet Explorer 4. Одной из новинок программы стал «активный рабочий стол» [active desktop], помещавший рекламу непосредственно на дисплей пользовательского компьютера. Аналогично экраны сотовых телефонов и пейджеров все чаще несут небольшую рекламу в виде фирменных знаков.

Все эти маркетинговые возможности объединяет одно: реклама все чаще ориентируется на одного человека. Такой индивидуальный подход востребован индивидуальным подходом к торговле, который в любом случае ведет к повышению спроса на персональную информацию.

Они нацелены прямо на вас: Процесс прямого маркетинга

Каким образом супермаркет, флорист и дантист получили имя матери Синди Роуэн первыми? Хотя мы не можем узнать этого точно, скорее всего, они получили эту информацию от одной из компаний, поддерживающих правительственную программу смены адресов.

Когда вы заполняете карточку смены адреса, она пересылается в процессинговый центр, где вводится в компьютер, после чего информация становится доступной крупнейшим фирмам, занимающимся прямым маркетингом. Договорные отношения запрещают этим фирмам непосредственно использовать эту базу данных для прямого маркетинга, говорит Уэйн Орбки [Wayne Orbke], представитель американской почтовой службы, занимающийся

надзором за контрагентами программы.¹⁴⁴ Но фирмам разрешено использовать эту информацию для обновления собственных баз данных – собственно, в этом и заключается цель программы. Разрешая маркетинговым компаниям поддерживать свои банки данных в актуальном состоянии, почтовая служба снижает свои расходы по доставке миллиардов писем по старым адресам, пересылая их на новый адрес.

Но поскольку продавцы уже владеют информацией, чрезвычайно трудно избежать некоторых злоупотреблений, на предотвращение которых направлено государственное регулирование. Рассмотрим компанию Metromail, с годовым объемом продаж, превышающим 250 миллионов долларов, которая была приобретена компанией Experian в апреле 1998 года. Metromail была одним из крупнейших контрагентов национальной программы смены адресов. Компания внимательно контролирует свои списки рассылки до и после изменений, вносимые из файлов программы смены адресов. Она вычленяет изменившиеся адреса и включает их в специальные списки, называемые «списки новоселов» [New Movers file]. Затем Metromail продает *именно этот* список бизнесменам в районе нового места жительства человека.

Фактически Metromail хвастается своим мастерством манипулирования информацией. Реклама компании гласит:

Списки новоселов от Metromail идеально подходят для компаний, занимающихся обстановкой, оборудованием и модернизацией домов, предоставляющих междугородную связь, банковских/инвестиционных проектов, включая кредитные карты. Они также являются прекрасной возможностью для использования при организации подписки на газеты и журналы, а также каталогизаторами, ищущими средство борьбы с истощением списков.¹⁴⁵

В 1996 году базовая цена «списка новоселов» от Metromail составляла 60 долларов за тысячу имен. За дополнительные 10 долларов компания может получить от Metromail отфильтрованный список, в который попадут лишь фамилии семей, переехавших на расстояние более 50 миль; возможно, именно этой услугой и воспользовался дантист из Фармингдейла, приславший приглашение погибшей матери Синди Роуэн. В конце концов, зачем тратить деньги, рассылая приглашения людям, переехавшим на соседнюю улицу?

Регистрационная карточка продукта

Многие продукты поставляются с регистрационной карточкой. Юридически, основное предназначение этих карточек заключается в помощи производителям при отзыве продукта. Но компании зачастую наполняют свои регистрационные карточки вопросами, единственная цель которых – построение более точных маркетинговых баз данных. С какой еще целью компания, производящая соковыжималки, может интересоваться годовым доходом вашей семьи? [Фото любезно предоставлено Крисом Рейли, Reilley Design]

¹⁴⁴ Интервью автору, 22 февраля 1996.

¹⁴⁵ Реклама в *DM News*, февраль 1996.

Сегодня Metromail является частью компании Experian с оборотом 1,5 миллиарда долларов, основная деятельность которой заключается в отслеживании персональной информации. Комбинируя информацию об адресах, кредитах и коммерческую информацию, Experian может оказать бизнесменам помощь в нахождении новых клиентов, более эффективном взаимодействии с ними и более эффективно отсеивать клиентов, представляющих кредитный риск, чем это было раньше.

Сочетание кредитной информации с услугами по прямым продажам позволяет Experian предлагать самый широкий спектр информационных услуг по всему миру. В следующей таблице приведены примеры большого числа предлагаемых компанией информационных продуктов.¹⁴⁶

Услуга – Описание

Analytical and consulting services – Предоставление американским компаниям услуг по более эффективному использованию уже имеющейся у них информации

AutoCredit – Используется при выдаче ссуд на транспортные средства и при заключении договоров по их аренде

Bankruptcy – Компьютерная модель, которая может предсказать банкротство

Bullseye Report – Используется для корректировки информации, ошибочно представленной Experian

Business Credit Extract – Поиск новых клиентов в коммерческой базе данных

Business Credit Prescreen – Поиск в списках почтовой рассылки людей, исправно оплачивающих свои счета

Business Owner Profile – Выборка единоличных владельцев предприятий

Business Profile – Предоставление кредитного отчета предприятия

Collection Report – Отслеживание клиентов, не оплачивающих счета

CollectScore – Оценка неоплаченных счетов с указанием наиболее вероятного плательщика

Connect Check – Предоставление подтверждающих идентификаторов для борьбы с «кражей личности»

Consortium databases – Каталог баз данных покупателей и подписчиков журналов

Credit Profile report – Предоставление кредитного отчета по потребителю

Credit Decision Expert – Ранжирование кредитных отчетов

CU Decision Expert – Предоставление услуги по автоматизированному принятию решения о предоставлении займа для кредитных объединений

Demographics Band – Подтверждение личности людей, не занесенных в кредитные банки данных

Employment Insight report – Предварительный отбор претендентов для работодателя

Experian Segmentation Systems – Группировка имеющихся или перспективных клиентов в зависимости от образа жизни, привычек, материального

¹⁴⁶ Источник: американский каталог продуктов и услуг Experian. Доступен в Инетрнете по адресу http://www.experian.com/catalog_us/index.html.

благополучия и других показателей

Experian Quest – Предоставление автоматизированных методов, позволяющих компаниям лучше взаимодействовать с существующими клиентами

FACS+ – Извещение об адресах с высоким уровнем риска или нерезидентных

Fair, Isaac – Предоставление моделирования потребительских кредитов

Flood certification services – Идентификация уязвимых свойств

ID Profile – Поиск новых клиентов, не занесенных в кредитные базы данных

INSOURCE – Дополнение списков рассылки демографической информацией, данными о собственности, списками транспортных средств, результатами опросов и др.

Intelliscore – Предварительная оценка кредитных рисков для составления рейтинга кредитоспособности малого бизнеса

Lettershop – Предоставление услуги по массовой почтовой рассылке

List Link™ – Предоставление объемных списков потребителей с предоставлением прямого доступа к национальной базе потребителей Experian.

List processing services – Предоставление комплексных услуг по индивидуальному маркетингу, начиная со сбора имен и заканчивая печатью и рассылкой предложений. Услуги включают «санацию адресов» [Address Hygiene] для исключения почтовых отправок, которые невозможно доставить еще до их отсылки, обработку по реестру национальной программы смены адресов, корректировку адресов и автоматическое выявление повторяющихся адресов.

List rental fulfillment and maintenance – Experian может оказывать помощь организациям, которые хотят предоставлять информацию из своих баз данных за плату, опционально «обогащая» ее информацией из своих баз данных

Market Share – Выпускаемая на CD-ROM система поиска новых клиентов с такими же характеристиками, как у существующих.

National Risk Model – Профилирование существующих счетов и определение степени риска

Platelink – Предоставление информации о потребителе по номеру автомобиля

Point-of-Sale Analyst – Анализ кредитов и клиентов по кассовым счетам

Postal optimization – Обеспечивает самые низкие почтовые расходы

Prescreen – Используется для формирования предложений предварительно оформленных кредитных карт

Profile Summary – Анализ кредитной истории клиента

Property Link – Предоставление подробной информации об имеющейся у клиента собственности

Prospect Locator Series – Выпускаемая на CD-ROM система формирования списков адресов и телефонов для использования в прямых или телефонных продажах

RecoveryScore – Ранжирование просроченных счетов по возможности их восстановления

Revenue Opportunity Indicator – Ранжирование выбранных клиентов по потенциальному доходу

Segmentation systems – Сегментирование клиентов

Signal – Предупреждение о счетах с наметившимися проблемами

Skip Locator – Отслеживание клиентов, уклоняющихся от оплаты счетов

Smart Quest – Идентификация клиентов с наиболее высокими потенциалами прибыли и риска

Vehicle Financing Solution – Предварительный отбор для агентств по аренде автомобилей

Vehicle Ownership Tracking System – Отслеживание смены владельцев автомобиля

Правительственные архивы являются лишь одним из многих источников информации. Возьмите любой экземпляр еженедельной газеты индустрии прямых продаж *DM News* и вы

увидите рекламу, предлагающую обработанные списки с сортировкой людей по микродемографическим группам: «испаноязычные семьи с детьми», «респектабельные мужчины», «американцы азиатского происхождения, заказывающие товары по почте» и тому подобное.

Нью-йоркская компания Kleid страстно желает продать вам фамилии подписчиков таких престижных журналов, как *Architectural Digest* (средний доход семьи, СДС – 82 100 долларов), *New Yorker* (СДС – 71 100 долларов) или *Vanity Fair* (СДС – 99 400 долларов). Ищете новобрачных? Response Media Products из Атланты может продать вам список из 132 761 имен женщин, совершавших покупки в свадебном салоне за последние 12 месяцев. Списки стоят 80 долларов за тысячу имен, что является средней ценой на этом рынке. Списки могут быть использованы как самостоятельно, так и в сочетании с другой информацией для проведения высокоточных маркетинговых кампаний.

Многие американцы до глубины души оскорблены этой торговлей. Но индустрия парирует любые нападки стандартными оправданиями, используемыми уже более 30 лет. Первое это то, что мы живем в свободной стране, и рекламодатели также имеют права на свободу. Как сказал в 1972 году один торговец: «Поскольку каждый может просто выбросить непрошеную почту, он не подвергается принуждению ни в какой форме, и его гражданские свободы не нарушаются».¹⁴⁷

В качестве второго оправдания приводится аргумент, что неважно, что потребители думают о продаже имен, главное – они довольны результатом. «Более 98 миллионов американцев совершают покупки не выходя из дома и им нравится свобода получения предложений в соответствии с их интересами», – говорит Конни Хитли [Connie Heatly], старший вице-президент Ассоциации прямого маркетинга [Direct Marketing Association, DMA].¹⁴⁸ В качестве дополнительного доказательства DMA приводит информацию о том, что за последний год методом прямого маркетинга потребителям было продано товаров на сумму 240 миллиардов долларов. Конечно, говорит DMA, если потребители реагируют на предложения не столь благосклонно, компании перестают их использовать.

Под прицелом криминала

К сожалению, проблема не ограничивается только лишь Ассоциацией прямого маркетинга. Продаваемая персональная информация используется для телемаркетинговых мошенничеств, объем которых, согласно данным Федеральной комиссии по торговле, составляет 40 миллиардов долларов в год. Жулики часто покупают имена, номера телефонов и адреса так же, как законопослушные предприниматели. После этого они используют персональную информацию, чтобы тем или иным способом заставить людей расстаться со своими деньгами.

Мошенничества все больше приобретают интернациональный характер. Хильда Ханна [Hilda Hanna], гражданка США, начала получать телефонные звонки из Квебека в 1996 году. Звонивший сказал, что она была введена в тотализатор и выиграла джекпот в размере 945 тысяч долларов. Но есть одна загвоздка: чтобы получить эти деньги, она должна выслать 19 тысяч долларов для уплаты канадских налогов и таможенных платежей. Считая, что деньги уже у нее в кармане, Ханна заняла указанную сумму по своей кредитной карте. Но выигрыш от тотализатора так никогда и не пришел. Вместо этого она получила другой телефонный звонок, и ей сообщили, что она выиграла второй приз (128 тысяч долларов) и должна выслать дополнительно 4 тысячи долларов для его получения. После этого ей позвонили и в третий раз.

¹⁴⁷ Westin, *Databanks in a Free Society*, p. 163.

¹⁴⁸ Интервью автору, 14 февраля 1995.

«Все выглядело вполне законно, – рассказывала Ханна корреспонденту *Washington Post*. – Они продолжали просить денег... и мое сердце говорило мне: не делай этого больше... Но я склонна верить людям, а они говорили, что я получу [денежный приз], до того как [платеж] уйдет с моей кредитной карты. Я полагаю, что я слишком доверчива. Мне 71 год, и я должна была знать [жизнь] лучше». ¹⁴⁹

Канада привлекает заезжих мошенников, потому что телемаркетинговые мошенничества преследуются там относительно слабо, а наказания не такие суровые, как в США. Более того, «работая» только с американскими потребителями, гастролеры могут избежать риска судебного преследования со стороны местных властей. Именно по этой причине, говорят представители канадских властей, в Канаде постоянно действуют десятки схем мошенничества «на расстоянии».

Печально, но эта международная проблема становится все серьезнее в связи с падением цен на международные звонки и перемещением большинства подобных мошенничеств в Интернет.

Исключения не работают

Вернемся к Ассоциации прямого маркетинга. Конни Ламатто [Connie LaMatto] утверждает, что индустрия прямых продаж разработала специальную систему в помощь тем «редким» людям, которые не хотят получать предложения. Это так называемая Служба почтовых предпочтений [Mail Preference Service] – поддерживаемый DMA список людей, заявивших, что они не хотят получать предложения по почте. Просто пошлите в адрес DMA карточку с просьбой удалить вас из маркетинговых списков и вы будете избавлены от всей непрошеной почты. DMA поддерживает подобный же список под названием Служба телефонных предпочтений [Telephone Preference Service], цель которого – положить конец непрошеным предложениям по телефону.

Внутри индустрии прямых продаж Службу почтовых предпочтений называют «базой исключений». Идея состоит в том, что торговые компании не хотят тратить деньги, посылая предложения людям, не желающим их получать; гораздо дешевле *отсечь* их имена заранее, пока почта еще не отослана. Но исключения не работают для большинства потребителей. И вот почему:

- многие потребители просто не знают о существовании списков исключений. Другие потребители слышали об этих списках, но не знают, как в них попасть;
- каждый раз, когда вы переезжаете, вам необходимо вновь добавлять себя в этот список. Это происходит потому, что компании, производящие почтовые рассылки, используют информацию национальной программы по смене адресов для корректировки своих данных, а DMA – нет;
- списки работают по принципу «все или ничего». В результате многие потребители сомневаются, добавлять ли себя в эти списки, поскольку опасаются, что могут пропустить какое-нибудь заманчивое предложение;
- имя удаляется из списка по прошествии пяти лет;
- закон не требует от занимающихся почтовой рассылкой компаний использовать эти списки, поэтому многие этого просто не делают.

Проведенный в 1996 году обзор законодательства по защите информации и текущая деятельность профессора Пола Шварца [Paul Schwartz] с юридического факультета при университете штата Арканзас и профессора Джоэля Рейденберга [Joel Reidenberg] с юридического факультета в Фордхэyme показывают, что только 53 % членов DMA используют Службу почтовых предпочтений для ограничения своих почтовых рассылок!

¹⁴⁹ Howard Schneider, «Telemarketing Scams based in Canada Increasingly Target U.S. Residents», *The Washington Post*, 24 августа 1997, p. A21.

(Так было до октября 1999 года, пока DMA не стала требовать от своих членов обязательного использования этого сервиса; пока еще рано судить, каковы результаты изменения политики организации.) «В любом случае большинство американцев просто не знают о возможности исключения имен из списков. Это незнание отражает либо неэффективность, либо неисполнительность даже тех членов DMA, которые заявляют об использовании этого сервиса».¹⁵⁰ Далее в исследовании сказано:

Внутренние процедуры компаний не предусматривают каких-либо возмещений людям в случае, если имело место нарушение политики компании. В отличие от финансовых или телекоммуникационных услуг, для служащих, нарушающих кодекс компании, кажется, не предусмотрено никаких строгих внутренних санкций.¹⁵¹

Поскольку списки исключений являются добровольными и поскольку законом не предусмотрено санкций за посылку почты людям, поместившим себя в списки исключений, будет или нет компания использовать Службу почтовых предпочтений, – остается на ее усмотрение. На практике компании вроде Experian взимают со своих клиентов плату за каждое использование списков исключений для удаления фамилий из списков рассылки, что еще больше снижает шанс использования этого сервиса.

Несмотря на эти трудности, размер списков исключений постоянно растет – от 988 тысяч человек в 1989 году до 3,2 миллиона человек в 1995-м и 3,9 миллиона в 1999-м. Этот скачок произошел из-за повышения гласности благодаря активистам приватности и Интернету, что позволило людям более просто находить потребительскую информацию и обмениваться ею, не ограничиваясь традиционными информационными каналами.

Однако, с точки зрения этики, сама идея «исключения» порочна. Потребители не должны просить продавцов не слать им почту. Более правильным является «включение», а не «исключение». Компании должны воздерживаться от посылки предложений потребителям, если только они сами не попросили об этом. Потребители обычно ищут информацию от компаний: они посещают их web-сайты, звонят по телефонам 800-й серии и даже заполняют «лотерейные карточки» на последних страницах журналов. Переход к системе «включения» сделает торговлю более эффективной, устраняя огромные затраты и усиливая общее количество взаимодействий между покупателем и продавцом.

Предпринимаем прямые действия против прямого маркетинга

Давайте попробуем представить наше похожее на ночной кошмар будущее, если прямой маркетинг будет развиваться тем же путем:

Вы планируете съездить в Нью-Йорк со своей возлюбленной на День святого Валентина. Вы звоните своему турагенту, чтобы заказать тур, и отправляетесь на ланч. Возвратившись, вы обнаруживаете, что ваш электронный почтовый ящик забит. В Большом Яблоке ^[p40] более 5 тысяч ресторанов, и треть из них прислали вам электронные купоны с 15 % скидкой на второе блюдо, если вы решите посетить их во время своей поездки.

¹⁵⁰ Paul Schwartz and Joel Reidenberg, *Data Protection Law*, p. 333. См.: Marc Rotenberg, «Testimony and Statement for the Record of Marc Rotenberg, Director Electronic Privacy Information Center, on the Children's Privacy Protection and Parental Empowerment Act, H.R. 3508, Before the House of Representatives, Committee on the Judiciary, Subcommittee on Crime, September 12, 1996». Доступно в Интернете по адресу [http:// www. epic. org/privacy/kids/EPIC_Testimony.html](http://www.epic.org/privacy/kids/EPIC_Testimony.html).

¹⁵¹ Ibid., p. 338.

p40

Big Apple – неформальное прозвище Нью-Йорка.

Вы тянетесь к телефону, чтобы позвонить турагенту и накричать на нее за продажу вашего имени. Но вам это не удастся. После снятия трубки вы слышите не гудок, а голос представителя авиакомпании United Airlines. Он сообщает вам, что ваш агент заказала вам билеты на рейс компании American. «Мы узнали об этом через систему резервирования билетов. Если вы возьмете билет для следующей деловой поездки в авиакомпании United, мы оплатим ваш билет на American и в качестве приветственного подарка предложим вам обслуживание по бизнес-классу».

Предложение United слишком хорошо, чтобы его упустить. Но в течение следующих 15 минут вы находите в нем столько препонов и ограничений, что решаете остаться верным авиакомпании American. Посмотрев на часы, вы обнаруживаете, что уже на 10 минут опоздали на совещание. Но как только вы встаете, телефон звонит опять. На определителе высвечивается номер вашей возлюбленной, поэтому вы снимаете трубку.

Сюрприз! На этот раз звонит местный турагент (которая запрограммировала свой телефонный коммутатор на выдачу ложной информации в систему определения номера вызывающего абонента). Она спешит сообщить вам, что у Cathay Pacific есть специальное предложение на короткую поездку Нью-Йорк – Гонконг. «Это прекрасная возможность продлить ваши каникулы, – говорит она. – И всего за 999 долларов».

Несколько дней спустя вы завалены каталогами для заказов по почте. Компании, торгующие всем, начиная от «костюмов в нью-йоркском стиле» до газовых баллончиков для самозащиты, пытаются завладеть вашим вниманием, предлагая поставить именно то, что вам будет необходимо в предстоящей поездке. Многие из этих каталогов напечатаны специально для вас: на обложках некоторых из них помещен коллаж, где ваше лицо приклеено к телу прекрасно выглядящей модели. В одном из каталогов изображены коробки с шоколадом, которые будут доставлены вам в номер отеля в подарочной упаковке. (Очевидно, что отель делает дополнительный бизнес на том, что продает ваше имя и планы путешествия.) За дополнительную плату, гласит реклама, мы можем нанести на коробки монограммы из ваших инициалов и инициалов вашей возлюбленной.

Но постоянная маркетинговая охота на вас на этом не прекращается. Получив авиабилеты, вы обнаруживаете на посадочном талоне рекламу предписанного вам лекарства, которое вы искали, чтобы взять с собой. Даже в полете, глядя на вмонтированный в спинку впереди стоящего кресла «воздушный телефон», вы замечаете, что он высвечивает небольшую персональную рекламу ювелирного магазина на Таймс-сквере. Если вы посетите его 14 февраля, то получите 40 % скидку на обручальные кольца.

Похоже, что все вокруг знает о вашем путешествии. Но откуда ювелирный магазин знает, что вы с вашей возлюбленной неженаты? В течение следующих нескольких дней этот вопрос снова и снова будет всплывать у вас в голове.

Когда вы наконец вернетесь домой неделю спустя, вы обнаружите, что ваш дом обокрали.

Мир полон компаний, желающих продать нам свою продукцию. Снижение стоимости коммуникаций в сочетании с все повышающейся доступностью персональной информации делают более чем реальной ситуацию, когда все компании одновременно завалят нас предложениями уже в ближайшие годы. И это не просто проблема человека, совершающего поездку в Нью-Йорк на День святого Валентина. Очень скоро все компании страны, или даже всего мира, будут соперничать за наше внимание и за наши деньги – прямое следствие снижения транспортных расходов и глобализации рынков.

К счастью, мы можем с этим бороться.

Тактика № 1: обеспечьте свою анонимность

Прямой маркетинг зависит от возможности находить цели – от возможности продавца идентифицировать, кто вы и что вы, скорее всего, купите. Одним из способов защитить себя

от маркетинговой машины является защита вашей личности.

Вероятно, самым надежным способом защиты личности является анонимность. Покупайте товары за наличные деньги. Не принимайте участия в «клубах дней рождений» [Birthday Clubs] или программах по предоставлению специальных скидок. Будьте подозрительными, когда компания пытается получить от вас персональную информацию, такую как дата рождения, адрес или номер телефона.

Еще более важна анонимность в Интернете, где владельцу web-сайта ничего не стоит отслеживать все ваши перемещения. На информационной супермагистрали отслеживание переходит в слежку, которая, в свою очередь, приводит к получению непрошенных предложений и нарушениям приватности. Поскольку персональная информация легко может быть передана через Интернет, все более важным становится создание сетевой архитектуры, в которой анонимный доступ является стандартным режимом работы.

Право на приватность включает право на анонимность. Единственный способ защитить это право – воспользоваться им.

Тактика № 2: предавайте гласности и обращайтесь в суд

Многие компании вольно обращаются с персональной информацией, не имея на то достаточных юридических прав. Чтобы избежать неизбежной негативной реакции общества, эти компании стараются сохранить свою деятельность в секрете. Но шила в мешке не утаишь.

Средства массовой информации являются одним из наиболее эффективных инструментов в борьбе с неправильным использованием персональной информации крупными уважаемыми компаниями. Дурная слава в результате «произвола с приватностью» значительно перевешивает потенциальный доход, который компания может получить от своих клиентов. Например, в феврале 1998 года *Washington Post* опубликовала информацию о том, что две крупные аптечные сети CVS и Giant Foods Pharmacy продавали информацию о продаже лекарств по рецептам, расположенной в Вобурне, штат Массачусетс, торгово-промышленной компании Elensys. Компании заявили, что они использовали Elensys лишь для отсылки своим клиентам почтовых напоминаний о необходимости продления рецепта. Но *Washington Post* установила, что эта информация была также использована и для прямого маркетинга и использовалась совместно с другими компаниями-производителями лекарственных препаратов. Giant Foods сразу же заявила, что прекращает эту практику; CVS все отрицала, по крайней мере поначалу, хотя в конечном счете вынуждена была признаться под давлением потока жалоб от клиентов.

Практика добровольного введения ограничений является похвальной, но она опасна. Поскольку введение таких ограничений не требуется законом, принявшая их компания может позднее в любой момент отказаться от них. В то же время менее аккуратные фирмы вообще не связываются с этим.

Единственный способ гарантировать добровольное выполнение компанией политики соблюдения приватности – подать иск против компании, которую вы подозреваете в нарушении своей приватности. Именно так поступил один человек из штата Массачусетс, после того как история с CVS поутихла. Утверждая, что он получил предложение, убеждавшее его использовать лекарственные препараты, произведенные Glaxo-Wellcome, Inc., он предъявил групповой иск CVS, Elensys и Glaxo-Wellcome за «вопиющее нарушение конфиденциальности потребителя и пациента».¹⁵²

Судебные процессы дают гораздо больше, чем простое привлечение внимания. В случае выигрыша создается обязательный прецедент, которому будут следовать и другие

¹⁵² Robert O'Harrow, Jr., «Prescription Sales, Privacy Fears; CVS, Giant Share Customer Records with Drug Marketing Firm», *Washington Post*, 15 февраля 1998, p. A01.

компании.^[p41]

Тактика № 3: контролируйте их методы слежения

Когда журнал предоставляет за плату информацию о своих подписчиках, он всегда вставляет в список несколько специальных имен, чтобы отследить использование этой информации. Обычно список предоставляется для однократного использования. Эти *меченые имена* позволяют владельцу списка установить, не использовался ли список более одного раза или с целью, отличной от разрешенной. Например, вице-президент компании по маркетингу может внести в список свой адрес и указать имя своей кошки Тельмы. Если Тельма получит по почте пять каталогов вместо одного или если ей позвонят по телефону и сообщат, что она выиграла 10 тысяч долларов (но для их получения необходимо заплатить 2500 долларов в качестве налога), скорее всего, за этим последует судебное разбирательство.

Все большее число потребителей использует эту же самую методику. Есть люди, которые подписываются на разные журналы, слегка изменяя свое имя, например Robert Johnson, Bob F. Johnson, R. Fox Johnson, просто чтобы отследить, как имя перемещается по информационным каналам экономики. Сегодня потребители мало что могут сделать с этой информацией, разве что предать гласности принятую в индустрии практику. Но со временем чем больше мы будем знать, тем проще будет добиться перемен.

Тактика № 4: используйте существующие законы и добивайтесь принятия новых

Сегодня мы имеем огромное количество принятых законов, защищающих приватность. Печально, но очень мало потребителей знает о своих правах. Доступные сегодня средства уже давно используются в борьбе против злоупотреблений маркетинговой индустрии. Мы также можем учиться на ошибках прошлого и использовать принятые ранее законы как шаблоны для принятия новых.

В 1960-е годы, после того как федеральные суды смягчили определение «непристойности», большое количество фирм стало приобретать почтовые списки у американского правительства по закону о свободе информации [public records laws] и использовать эти списки для рассылки людям предложений приобрести порнографию. Но конгресс эффективно решил эту проблему в 1970 году, приняв федеральное постановление, требующее от американского почтового департамента [US Post Office Department] – предшественника современной почтовой службы¹⁵³ – составить и поддерживать в актуальном состоянии список людей, не желающих получать почту сексуального содержания. Нарушение волеизъявления людей из списка влекло за собой уголовную ответственность для отославшего почту. К 1971 году более 500 тысяч людей поместили свои имена в список.¹⁵⁴ Вскоре маркетинговая практика индустрии изменилась. Вместо того чтобы рассылать предложения сексуального характера по всем адресам, которые они смогли купить, современные компании ограничиваются рассылкой каталогов лишь тем людям,

p41

В США действует англо-саксонская правовая система, базирующаяся на прецедентах. Это означает, что если в ходе судебного разбирательства принято определенное решение, то при рассмотрении аналогичных случаев в будущем с большой вероятностью вопрос будет решен точно так же.

¹⁵³ 12 августа 1970 года президент Ричард Никсон подписал «Закон о реорганизации почтовой службы» [Postal Reorganization Act]. Закон преобразовал Почтовый департамент [Post Office Department] в Почтовую службу Соединенных Штатов [United States Postal Service], принадлежащую правительству корпорацию.

¹⁵⁴ Westin, *Databanks in a Free Society*, p. 162.

которые их запрашивают.

Сегодня проблема порнографии встает вновь из-за нового поколения порнографов, рассылающих непрошеный «спам» по электронным почтовым ящикам, навязчиво рекламируя web-сайты с откровенно сексуальным содержанием. Но не существует причин, по которым найденное в 1960-е годы решение не заработало бы сегодня.

Подобное законодательство положило конец другой разновидности непрошеной рекламы – по факсу. В 1991 году конгресс принял «Закон о защите абонентов телефонных сетей» [Telephone Consumer Protection Act^[p42]], объявивший незаконным посылку рекламы по факсу без получения предварительного разрешения владельца факс-аппарата. Закон запретил также использование автоматических телефонных устройств, которые обзванивали потребителей и проигрывали предварительно записанное рекламное сообщение. Эти раздражающие факторы сегодня практически исчезли из жизни потребителей.

Законопроект 1991 года содержал также положение, запрещающее торговцам звонить людям, не желающим получать коммерческие предложения по телефону. Но конгресс сгруппировал. Вместо того чтобы утвердить создание общенационального *списка со звездочками*, т. е. списка людей, не желающих получать коммерческие звонки, законодатели оставили на усмотрение Федеральной комиссии по связи и коммуникациям [Federal Communication Commission, FCC] принятие решения о наилучшем способе реализации такого списка. FCC в свою очередь жестко лоббировалась маркетинговой индустрией. В конечном счете FCC приняла парадоксальное решение, что будет «более эффективно», если каждая компания введет свою собственную базу исключений, вместо создания общенационального реестра. В результате по американским законам вы должны теперь заявлять *каждой компании*, делающей коммерческие звонки, что вы не хотите получать звонки от нее, т. е. вы должны позвонить в каждую компанию и попросить ее поставить маленькую звездочку напротив вашего имени. (В этом есть и свои плюсы. Если вы получаете коммерческий звонок от компании, не ведущей «список со звездочками», вы можете предъявить ей иск на сумму от 500 до 1500 долларов. По данным президента Private Citizen Боба Балмаша [Bob Bulmash] в 1996 году американские потребители, используя данный закон, получили более 54 тысяч долларов.)

«По моему мнению, в этой стране требуется федеральный закон о „звездочках“, как это предлагалось конгрессу, – сказал активист движения за права потребителей и президент Junkbusters Corporation Джейсон Кэтлит [Jason Catlett]. – Вы должны иметь возможность бесплатно добавить свой номер (не имя) в общенациональный список и получить компенсацию в 10 тысяч долларов за каждый сделанный на ваш номер коммерческий звонок».¹⁵⁵

США явно требуется принять больше законов, регулирующих торговлю. Это законодательство должно сосредоточиться на том, чтобы дать потребителям больше информации о торговцах, предусмотреть высокие компенсации за нарушение приватности потребителей и уголовную ответственность за уклонение от исполнения закона.

В качестве хорошей отправной точки можно использовать предложенный в 1965 году конгрессменом Корнелиусом Галахером [Cornelius Gallagher] билль, который так и не был принят. Этот билль требовал, чтобы создаваемые компьютером почтовые наклейки включали кодовый номер для имени каждого адресата и номер телефона, по которому вы можете позвонить, чтобы вас удалили из соответствующего списка рассылки. Пересмотренная в соответствии с требованиями XXI века версия этого билля может

^{p42}

²⁰ декабря 1992 года Федеральная комиссия по телекоммуникациям и связи (FCC) установила набор требований и правил, обеспечивающих выполнение положений данного закона. Для частных абонентов и компаний эти правила отличались.

¹⁵⁵ Из личной переписки (электронная почта), 4 и 5 августа 1997.

одинаково хорошо применяться как к электронной почте, так и коммерческим телефонным звонкам.

Конгресс также должен обратить внимание на угрозу коммерческих телефонных звонков, приходящих из заграницы. Степень этой угрозы возрастает благодаря резкому падению стоимости международных телефонных звонков. Нам нужен работающий закон, который позволит идентифицировать и задержать преступника, даже если мошенничество «на расстоянии» происходит из заграницы. Затем данный закон должен быть расширен таким образом, чтобы блокировать коммерческие звонки из заграницы, за исключением случаев, когда вызываемый абонент явно указал, что он желает принимать такие звонки.

8

Кто владеет вашей информацией?

В предыдущих семи главах мы увидели, как много различных способов сбора персональной информации, использования ее без нашего разрешения, а зачастую и против нас. В этих главах я показал, что самым лучшим решением по предотвращению несанкционированного накопления и раскрытия персональной информации является принятие новых законодательных актов, специально разработанных для обеспечения права на приватность в компьютерную эру. Но другие современные мыслители на базе тех же самых фактов приходят к другому решению. «Мы не нуждаемся в новых законах, – говорят они, вторя либеральным настроениям, столь популярным среди сегодняшней информационной интеллигенции. – Все, что нам нужно, это рассматривать персональную информацию как объект права собственности, после чего использовать существующие законы о собственности для предотвращения несанкционированного ее использования».

Однако отнесение персональной информации под юрисдикцию права собственности может принести больше вреда, чем пользы, поскольку информация кардинально отличается от других – материальных – форм собственности. Применение к ней принципов традиционного права собственности может легко привести к неожиданным последствиям.

«Самое главное отличие информации от других материальных ресурсов заключается в игнорировании привычных способов измерения, – говорит С. Б. (Джек) Роджерс-мл. [С. В. (Jack) Rogers Jr.], главный администратор компании Equifax, занимающейся сбором информации о потребителях. – С одной стороны, я могу продать ее вам и в то же время оставить себе. Она не подвержена износу, ее ценность возрастает и возрастает при использовании, она является основным ресурсом в мировой коммерции и торговле».¹⁵⁶

Информация не только отличается от других форм собственности, но и защищается своими собственными законами. Хотя изначально большинство этих законов были приняты для защиты отдельных людей и стимулирования их творчества, в последние годы они повернулись таким образом, что теперь почти эксклюзивно служат интересам крупного бизнеса и корпораций. Несмотря на то что эти законы выглядят как привлекательные средства для защиты личной тайны, в конечном счете они могут стать ловушкой, которая принесет приватности больше вреда, чем пользы. Право владения – опасный путь сохранения приватности. То, чем владеешь, может быть продано, передано по сделке, изъято или потеряно.

Владеете ли вы своим именем?

Рэм Аврахами [Ram Avrahami] считал, что он владеет собственным именем, но на самом деле его именем владела частная компания с 500 служащими и стоимостью 310

¹⁵⁶ Интервью автору, 19 апреля 1995.

миллионов долларов. Аврахами обратился в суд, чтобы остановить практику компании по продаже его имени без его разрешения, и проиграл. Аврахами хотел изменить основные правила, по которым играет национальная индустрия прямого маркетинга, в которой крутятся триллионы долларов. Вместо этого он лишь усилил ее власть.¹⁵⁷

Злоключения Аврахами начались в феврале 1995 года, когда он получил по почте рекламное письмо, приглашавшее его подписаться на журнал *US News & World Report*. Через несколько недель он решил принять предложение и отослал карточку. В марте он получил счет и отправил чек на 15 долларов.

Два месяца спустя Аврахами получил другое письмо по почте – предложение Smithsonian Institution подписаться на их журнал *Smithsonian*. Но на этот раз Аврахами не принял предложение, а написал Smithsonian Institution письмо, в котором поинтересовался, откуда они узнали его имя и адрес. Отдел распространения *Smithsonian* ответил, что они «приобрели [ваше] имя у *US News & World Report* для однократного использования». Как и многие другие журналы *US News & World Report* регулярно предоставляет за плату информацию о 2,2 миллиона своих подписчиков другим фирмам, которые занимаются продажами товаров по почте. Как оказалось, имя Аврахами было одним из 100 тысяч имен, которые *US News & World Report* продал *Smithsonian* за 8 тысяч долларов.

Аврахами был измучен и утомлен почтовым мусором. Но вместо того чтобы просто выбросить письмо, как поступает большинство американцев, он решил изменить общество. Он провел некоторые исследования и узнал, что в штате Виргиния, где он жил, имеется закон, прямо запрещающий то, что сделал *US News & World Report*. Согласно разделу 8.01–40 кодекса Виргинии:

Любой человек, чье имя, портрет или образ использованы без предварительного получения письменного разрешения этого человека...в рекламных целях или для продажи, может подать иск против отдельного человека, фирмы или корпорации, использовавших его имя, портрет или образ, с целью прекращения такого использования; он может также подать иск о возмещении любых убытков, нанесенных в результате этого использования. Если ответчик сознательно использовал имя, портрет или образ человека способом, явно запрещенным или объявленным незаконным в данной главе, суд, по своему усмотрению, может назначить штрафные санкции.

Некоторые другие штаты имеют аналогичное законодательство. Эти законы были приняты после известного случая, произошедшего в 1905 году в Нью-Йорке, когда родители ребенка подали иск против Rochester Folding Box Company за печать на 25 тысячах коробок для муки фотографии их ребенка. Компания Rochester не получала разрешения родителей ребенка. Семья предъявила иск за вторжение в личную жизнь, используя в качестве аргумента опубликованную в конце XIX века Брэндисом и Уорреном статью «Право на приватность» [*The Right of Privacy*]. Но семья проиграла процесс.¹⁵⁸ Причина: в законах Нью-Йорка не было ни понятия «право на приватность», ни права семьи контролировать использование фотографии их ребенка. После оглашения этого решения законодатели по всей стране были настолько оскорблены, что немедленно были приняты законы явно запрещающие практику использования имени или изображения человека в коммерческих целях без разрешения самого человека.

Аврахами обвинил также *US News & World Report* в «преобразовании», т. е. в захвате и использовании журналом его имени в собственных целях без получения предварительного разрешения. Он пользовался услугами адвокатского бюро Джонатана Дэйли [Jonathan C.

¹⁵⁷ Интервью автору, 18–19 августа 1997.

¹⁵⁸ *Robertson v. Rochester Folding Box Co.*, 171 NY 538.

Dailey] в Арлингтоне, штат Виргиния.

Это дело казалось новой интерпретацией закона штата Виргиния, но полностью соответствовало значимости персональной информации в Америке конца XX века. Аврахами обратился к суду присяжных, запросив взыскать с ответчика 100 долларов в качестве компенсации и 1000 долларов в качестве штрафа. Конечно, он надеялся, что своими действиями вызовет лавину исков против держателей списков почтовой рассылки, – лавину, которая быстро бы заставила индустрию отказаться от «списка исключений» и получать разрешение потребителя на предоставление его имени другим лицам.

Суд был назначен на 21 августа 1995 года.

Объяснения перед судом

При поддержке Ассоциации прямого маркетинга, *US News & World Report* изложил суду свое видение дела, в котором убедительно аргументировал свою правоту. Среди прочих аргументов были приведены следующие:

- журнал заявил, что продажа, сдача в аренду и обмен информацией из почтовых списков рассылки являются «общепринятыми обычаями делового оборота» в Соединенных Штатах. Фактически, заявила компания, даже Управление правительственной печати (издательство правительства США – US Government Printing Office) «постоянно практикует продажу или сдачу в аренду информации из своих списков почтовой рассылки», по цене «приблизительно 85 долларов за 1000 имен». Аналогично «многие департаменты и агентства правительства штата Виргиния, включая экзаменационный совет коллегии адвокатов,^[p43] предоставляют свои списки почтовой рассылки компаниям и отдельным людям путем продажи или сдачи в аренду»;

- журнал заявил, что, если Аврахами не хотел получать коммерческие предложения, он должен был зарегистрировать свое имя в принадлежащей Direct Marketing Association Службе почтовых предпочтений, что он, по его собственному заявлению, не сделал;¹⁵⁹

- журнал утверждал, что *US News & World Report* фактически получил имя Аврахами от Союза потребителей [Consumers Union], издающего *Consumer Report*, вместе с другими 92 500 именами, которые журнал взял в аренду для своей собственной маркетинговой кампании. *US News & World Report* в рамках каждой маркетинговой кампании обычно арендует информацию об именах или обменивается ею с 60–100 фирмами. Имя Аврахами – всего лишь одно из миллионов;

- журнал также заметил, что в подписном бланке *Consumer Reports* есть маленький квадратик, который подписчик должен отметить, если он не хочет, чтобы его имя использовал кто-то еще. Аврахами никогда не ставил метку в этом квадрате. И конечно, говорит компания, когда *US News & World Report* прислал Аврахами предложение о подписке, он подписался. «Когда мистер Аврахами получает по почте интересующее его предложение, он подписывается, – заявил адвокат журнала. – Когда же он получил предложение, которое ему не интересно, вместо того чтобы выбросить его в мусорную корзину, он подает иск».

Статья 8.01–40 кодекса Виргинии «не предусматривает запрет продажи, сдачи в аренду

p43

State board of bar examiners. Bar examination – юридический экзамен на право заниматься адвокатской практикой. Представляет собой письменный тест коллегии адвокатов, который должен пройти юрист, чтобы получить сертификат от властей штата и быть принятым в адвокатуру.

¹⁵⁹ На самом деле Аврахами заявил, что он был зарегистрирован в службе – когда проживал в штате Канзас – и посчитал, что служба не работает. «Я попробовал воспользоваться ею, но компании продолжали слать мне коммерческие предложения, – сказал он. – Даже компании, которые я прямо проинформировал о своей подписке в DMA, продолжали слать мне предложения. Это привело меня к выводу, что [у них] нет реальной заинтересованности прекратить отсылку мне предложений».

или обмена списками почтовой рассылки, – заключает *US News & World Report*. – Законодательство Виргинии в области приватности предназначено для защиты людей, чьи имена и образы были использованы в рекламе без их разрешения, предоставляя им право подать иск». Компания обратилась к суду с просьбой закрыть дело и вынести судебное определение о том, что продажа, сдача в аренду и обмен списками почтовой рассылки с именем Аврахами не нарушает законодательства Виргинии.

Юридические препирательства продолжались до 6 февраля 1996 года, когда ведущий это дело судья вынес неожиданное постановление. К удивлению обеих сторон судья Карен Хененберг [Karen Henenberg] заявила, что рассмотрение данного дела находится вне ее юрисдикции. Аврахами должен был обращаться не в суд системы «права справедливости» [Courts of Equity], сказала Хенеберг, а в суд, действующий по нормам статутного и общего права [Courts of Law]. Этот небольшой юридический нюанс упускается многими блюстителями закона за пределами штата Виргиния. В любом случае, это временно приостановило дело.

Аврахами против учреждения, раунд 2

Аврахами вновь подал иск 28 марта 1996 года, на этот раз в суд общего права, с просьбой навсегда запретить *US News & World Report* использовать его имя. Он потребовал в качестве возмещения ущерба по одному доллару за каждое использование его имени и за общий доход, полученный *US News & World Report* от использования его имени, плюс 5 тысяч долларов штрафа.

В этот момент в деле всплыл один важный факт. Как и многие люди, желающие отследить использование персональной информации, Аврахами несколько изменил написание своего имени, когда подписывался на *US News & World Report*. Вместо Ram Avrahami он подписался как Ram Avrahani.

Небольшое искажение в написании имен является стандартной практикой в индустрии почтовых рассылок для отслеживания перемещения и использования персональной информации. Когда дело Аврахами рассматривалось в суде 6 июня 1996 года, Кэтрин Хани [Catherine Hagney], вице-президент по работе с клиентами *US News & World Report*, рассказала во время дачи показаний, что она постоянно включает имя Catherine Cagney со своим домашним адресом в списки рассылки, сдаваемые журналом в аренду другим компаниям. «*US News & World Report* избегает предоставлять информацию компаниям, которые пытаются продавать порнографию или вовлечены в другую сомнительную деятельность, – сказала она. – Мы используем эти имена-метки чтобы убедиться, что нас не обманывают и не используют нашу информацию для других типов рассылки».

Пять дней спустя суд вынес постановление, что, написав свое имя с небольшими искажениями, Аврахами создал фиктивную личность, на которую он не имеет никаких прав по законам Виргинии. Из-за этой «фиктивности» судья Уильям Ньюман [William T. Newman] отказал Аврахами в удовлетворении иска и закрыл дело.

Решение не было неожиданным. Во время слушания судья Ньюман был благосклонен к защите и сух по отношению к Аврахами. Например, судья позволял адвокатам *US News & World Report* копаться в фактах личной жизни Аврахами, не имеющих отношения к сущности дела. Представители *US News & World Report* задавали Аврахами вопросы о его религии, иммиграционном статусе, не использовал ли он судебный процесс для привлечения внимания к себе особ женского пола. Более того, судья Ньюман пресекал многочисленные попытки со стороны адвоката Аврахами продемонстрировать размах, с которым персональная информация, помимо имен и адресов, продается и покупается журналом.

Аврахами обратился с апелляцией в Верховный суд Виргинии, но апелляция была отклонена.

Проговорив почти год о важности данного дела, активисты приватности быстро принизили значение отрицательного решения. «Суд специфично отнесся к некоторым

необычным обстоятельствам дела, – сказал мне основатель Junkbusters Джейсон Кэтлит. – Если бы Аврахами вместо [изменения имени] использовал специальную метку в адресе, типа „комната 7С“, он мог бы выиграть».

Кэтлит надеется, что другие используют опыт Аврахами:

«Люди по-прежнему могут подавать аналогичные иски в других штатах с таким законодательством, и даже в Виргинии. Сам факт того, что Ассоциация прямого маркетинга вложила огромные ресурсы в создание мощной защиты, говорит о том, что ее юристы верили в возможность выигрыша Аврахами. Я думаю, это лишь вопрос времени, когда кто-либо другой выступит с более хорошо подготовленным иском, и индустрия, в которой крутятся триллионы долларов, будет вынуждена изменить свои основные правила. Это будет так, как будто права владения каждым месторождением нефти в мире внезапно перейдут к живущим рядом с ним людям». ¹⁶⁰

Стоимость имени в Нью-Джерси

Возможно, Кэтлит прав. Конечно, Ассоциация прямого маркетинга устроила аналогичную общественную кампанию с высокими ставками в 1996 году, когда сенатор от Нью-Джерси Ричард Коди [Richard 3. Cody] пытался провести билль, сделавший бы незаконной продажу имен и адресов людей без их согласия.

Коди выступил с законодательной инициативой не из-за единичного инцидента. Когда я брал у него интервью, он сказал, что просто устал от компаний, которые «продают мое имя, адрес и демографические данные без моего согласия. [Они] не имеют право продавать мое имя еще кому-то, кто будет ко мне приставать». ¹⁶¹

DMA атаковала билль Коди, используя свою стандартную тактику защиты, заявив, что национальная индустрия прямого маркетинга с оборотом 600 миллиардов долларов может просто оказаться не у дел, если имена нельзя будет покупать и продавать, как многие другие товары. «Статистические данные говорят нам, что более половины взрослого населения Америки приобретает товары таким способом, – утверждает старший вице-президент DMA Конни Хитли [Connie Heatley]. – Люди могут говорить, что не любят получать непрошеную почту, но большинство людей поступает по-другому». Конечно, именно так, как поступил Рам Аврахами, подписавшись на *US News & World Report*. ¹⁶²

Билль Коди – интересное примечание к делу Аврахами, но в конечном счете это не имело никакого значения. Предложение Коди так никогда не было принято. Оно было раздавлено, как букашка.

Имя как собственность

Между сенатором Коди и DMA существует некоторый промежуточный уровень. Вместо того чтобы разрешать или запрещать продажу имен, каждое имя может быть лицензировано, чтобы его владелец получал отчисления за каждое его использование. Но такая система в конечном счете принесет больше вреда, чем пользы.

«Приватизация [персональной информации] может закончиться тем, что в выигрыше окажутся не частные лица, а компании, получившие от них эту информацию», – говорит

¹⁶⁰ Из личной переписки (электронная почта), 4–5 августа 1997.

¹⁶¹ Интервью автору, 22 февраля 1996.

¹⁶² Интервью автору, 14 февраля 1995.

Памела Самюэльсон [Pamela Samuelson], профессор авторского права из Калифорнийского университета в Беркли. Если рассматривать персональную информацию как предмет права собственности, говорит она, то произойдет следующее:

«Когда кто-нибудь берет вашу информацию, если только вы передаете хотя бы часть прав на свою информацию, они получают права на все. Мне кажется, что, если вы не установите пределы, в которых люди будут иметь возможность передавать эту информацию, вы не сможете достигнуть результата, к которому вы стремитесь в первую очередь, – обеспечить целостность персональной информации и право на защиту от некоторых видов злоупотреблений».¹⁶³

У этого подхода, конечно, есть и другие проблемы. Если людям платить за использование их имен, то таких людей нужно каким-то способом находить, чтобы выплатить деньги. Практически система «плати-если-отправляешь-мне-почту»^[p44] потребует создания массивной базы данных, содержащей информацию об имени, адресе и банковских реквизитах каждого жителя Соединенных Штатов. Эта база данных сама по себе огромный источник персональной информации, который будет доступен любой организации, занимающейся прямым маркетингом.

Другая проблема заключается в размерах самих выплат. Когда Союз потребителей [Consumers Union] продал 92 тысячи имен *US News & World Report*, он получил приблизительно 8 тысяч долларов. Имена и адреса просто стоят очень дешево. В случае с Союзом потребителей стоимость составила приблизительно 8,6 цента за каждого подписчика. Если на самом деле выплачивать людям «авторские отчисления», то надо говорить о проценте, который получают авторы книг, журнальных статей и компьютерных программ за свою работу, – от 5 до 15 %. Так сколько же стоит ваше имя? Грубо говоря – копейку.

Используя эту цепочку логических рассуждений, Кэтлит показывает, что существующая сегодня цена в 8 центов за имя является искусственно заниженной, потому что рынок перенасыщен информацией об именах и адресах потребителей. Объединившись, считает он, потребители могут ограничить поставки имен и поднять их в цене, так же как члены нефтяного картеля ОПЕК подняли цену на сырую нефть в 1970-х годах. Одним из путей создания дефицита является запрет продаж имен без явного разрешения потребителей.

Ассоциация прямого маркетинга заявляет, что запрет на продажу имен приведет к разрушению индустрии с оборотом в миллиарды долларов. Это лицемерие. Торгующие по почте фирмы имеют массу других возможностей распространять информацию о своих каталогах. Они могут воспользоваться рекламой в газетах, журналах и на телевидении. Они могут создать web-сайты. Они могут предоставлять скидки новым клиентам, если те закажут каталог по телефону 800-й серии. Они могут за плату размещать свою рекламу в выписках по кредитным картам или в заказах других фирм. Индустрии, ворочающей миллиардами долларов, не грозит упадок, даже если завтра будут ограничены нарушающие приватность рыночные технологии.

Я думаю, что защитники приватности предлагают рассматривать персональную информацию как объект права собственности, надеясь, что увеличение стоимости работы с персональной информацией приведет к прекращению этой практики. Это околное и, скорее всего, нерабочее решение очевидной проблемы. Проблема состоит не в том, что люди ничего не получают от продажи их имен; проблема в том, что имена и адреса людей продаются без их разрешения. Согласно данным проведенного в 1996 году Harris-Equifax опроса о

¹⁶³ Интервью автору, 15 апреля 1997.

^{p44}

В оригинале – «pay-as-you-mail».

соблюдении приватности потребителей,¹⁶⁴ 73 % американцев желают, чтобы их имена были удалены из коммерческих списков рассылки, и только 44 % знают, что соответствующие процедуры существуют. Если куплю-продажу имен людей не примет большинство населения, то такая практика должна быть упорядочена, ограничена или запрещена законом.

Владеете ли вы своими ногами?

Вы можете не владеть своим именем, но трудно поверить, что вы не владеете своими волосами, своими руками или ногами. На протяжении многих столетий нуждающиеся в деньгах женщины продавали свои волосы изготовителям париков. И если кто-нибудь отрежет вашу руку или ногу, вы можете подать иск за телесные повреждения.

Право собственности на генетическую последовательность, хранящуюся в каждой клетке нашего тела, также кажется очевидным. В конце концов структура вашей ДНК – исключительно ваша. Она определяет цвет ваших глаз и волос, черты лица, пол, расовую принадлежность и бесчисленное количество других характеристик, сочетание которых – и есть вы. Как же вы можете не владеть своей генетической информацией?

Генетическая информация зачастую является тем, чем стоит владеть – по крайней мере, ее частью. В генетическом коде отдельных людей скрыты специфичные мутации, на основе которых исследователи-биотехнологи могут разрабатывать новые медицинские тесты и лекарства. Особенно это касается людей с редкими мутациями, людей, которые много курят и не болеют при этом раком или инфицированы ВИЧ и не болеют при этом СПИДом.

Некоторые люди имеют генетические особенности, которых лучше не иметь, – и они предпочитают хранить их в секрете от других. Например, имеют гены, которые делают организм предрасположенным к раку или некоторым другим болезням. В последние годы люди, у которых обнаружены различные типы генетических заболеваний, подвергаются дискриминации со стороны работодателей или страховых компаний. Для этих людей право владения означает право хранить свой генетический профиль в тайне, так же как право владения картиной дает вам право поместить ее в чулан, чтобы никто больше ее не видел. Право владения означает некий вид контроля.

Но генетическая информация не похожа на картину. Вы наследуете свои гены от родителей – половину от матери, половину от отца. Брат и сестра имеют около 25 % общих генов. А однояйцовые близнецы, частота появления которых в Северной Америке составляет три человека из тысячи, имеют полностью идентичные наборы генов. «Если вы знаете что-то о себе, то вы знаете что-то о ваших родителях и о ваших родственниках, – говорит доктор Лайза Геллер [Dr. Lisa Geller], много лет занимавшаяся биомедицинскими исследованиями до прихода в расположенную в Бостоне фирму Fish & Richardson по вопросам законодательства в области интеллектуальной собственности. – Чья это информация и кто имеет право ее знать?»¹⁶⁵

Двойные неприятности

Болезнь Гентингтона^[p45] – ужасное уродующее заболевание, вызывающее произвольные движения, деменцию^[p46] и в конечном счете приводящее к смерти. Для

¹⁶⁴ Harris-Equifax, *Consumer Privacy Survey*, 1996.

¹⁶⁵ Интервью автору, август 1997.

p45

Другое название – хорей Гентингтона.

p46

Приобретенное слабоумие, которое проявляется в ослаблении познавательной способности, обеднении

нее не существует эффективного лечения. Вызывающая эту болезнь мутация происходит из Европы и распространилась в Америке после ее колонизации. В отличие от большинства других генетических заболеваний, ген, вызывающий болезнь Гентингтона, является доминантным: ребенок с вероятностью 50 % наследует этот ген от больного родителя. Но развитие болезни также сильно отличается: одни люди заболевают в 30 лет, другие – в 50. Одни люди умирают в течение 10 лет после появления симптомов, другие живут 20 лет. А некоторые люди, носители гена, умирают в результате несчастного случая или других болезней еще до того, как появятся симптомы.

Болезнь Гентингтона занимает особое место в летописи генетических заболеваний: в 1983 году группа исследователей из Бостона разработала тест, который может показать, имеет ли человек данный генетический дефект и, как следствие, угрожает ли ему эта болезнь.

В 1995 году *Journal of Genetic Counseling* опубликовал озадачивающее письмо, описывающее случай с однойцовыми близнецами.¹⁶⁶ В семье близнецов были случаи заболевания болезнью Гентингтона. Проблема, которая встала перед авторами письма, заключалась в том, что один из близнецов изъявил желание протестироваться. Другой не желал знать, является ли он носителем болезни. Это одно из первых заболеваний, которые диагностируются генетическими методами.

Сегодня можно привести множество доводов «за» и «против» генетического тестирования на предрасположенность к некоторым заболеваниям. С одной стороны, если вы являетесь носителем смертоносного гена, вы можете более правильно спланировать свою жизнь. Вы можете, например, купить дом без лестниц. Вы более свободны в опасных увлечениях или выборе рискованной, но высокооплачиваемой работы. Если вы хотите иметь детей – вы можете их усыновить или исследовать зародыш во время беременности и прервать ее, если плод является носителем смертельной мутации.

С другой стороны, некоторые люди предпочитают не знать, что они являются носителями смертельного и неизлечимого генетического дефекта. Для некоторых людей лучше не знать о присутствии гена, чем знать о нем и мучиться вопросом, насколько тяжелой будет болезнь и наступит ли она вообще. Существует и угроза генетической дискриминации: что если вам откажут в работе или страховке лишь потому, что однажды вы можете заболеть и умереть? В последние годы зарегистрировано сотни случаев генетической дискриминации.¹⁶⁷ Если вы являетесь носителем определенного гена, вы вряд ли захотите, чтобы эта информация попала в ваш медицинский файл. Простейший способ избежать этого – не тестироваться вообще.

Невозможно протестировать одного из однойцовых близнецов, не протестировав де-факто другого. И когда первый близнец предложил скрыть информацию от своего брата,

чувств, изменении поведения, сильном затруднении при использовании знаний и прошлого опыта.

¹⁶⁶ A. Heimler and A. Zanko, «Huntington Disease: A Case Study Describing the Complexities and Nuances of Predictive Testing of Monozygotic Twins», *Journal of Genetic Counseling* 11 (1995): 125–137. (Letter and replies *Journal of Genetic Counseling* 5:47–50.)

¹⁶⁷ По отношению к генетическим тестам страховые компании избрали средний вариант. В настоящее время ни одна страховая компания не требует от желающего застраховать жизнь или здоровье проходить обследование на генетические заболевания – частично потому, что эти тесты достаточно дороги, – но, если заявитель прошел такое обследование, страховая компания запрашивает результаты. Они опасаются обратного отбора, при котором люди, знающие, что они являются носителем генетического заболевания будут использовать экстравагантные политики страхования, в то время как те, кто уверен в чистоте своего генетического здоровья будут обходиться без страхования. Наложение этих двух факторов может привести к тому, что страховые выплаты компаний будут все больше и больше расти на фоне уменьшения количества здоровых людей, выплачивающих им страховые премии. Результатом может стать катастрофический упадок страхового бизнеса.

живущего в другом конце страны, исследователи отнеслись к этому иронически: как такая информация может быть надолго скрыта от брата? С другой стороны, с точки зрения медицинской этики, одинаково плохо как тестировать человека без его согласия, так и отказывать в тесте тому, кто об этом просит. Эта дилемма встала перед исследователями, поскольку одна и та же генетическая последовательность принадлежала двум разным людям.

К счастью, все разрешилось просто. Второй близнец согласился получить генетическую консультацию и в конечном счете протестироваться. Близнецы были одновременно проинформированы о результатах теста в двух офисах – один в Бостоне, другой – в Сан-Франциско. Исследователи даже учли трехчасовую разницу во времени между двумя городами.

Селезенки и толстые кости

Перенесший рак Джон Мур [John Moore] столкнулся с проблемой другого рода.¹⁶⁸ В 1976 году он перенес операцию по удалению селезенки, выполненную доктором Дэвидом Гоулдом [David W. Golde] из Калифорнийского университета в Медицинском центре Лос-Анджелеса. Мур страдал серьезным заболеванием – ворсинчатоклеточной лейкемией [«hairy cell» leukemia]; его селезенка увеличилась в весе от 220 г до более 6 кг. Она была удалена хирургическим путем, и Мур думал, что на этом все закончилось, пока в сентябре 1983 года Муру не позвонил Гоулд.

Перед операцией Мура попросили подписать бланк, в котором он давал разрешение использовать удаленную ткань для медицинских исследований. В частности, соглашение подразумевало передачу университету всех прав на «любую клеточную линию», созданную из клеток опухоли, которую врач собирался удалять. Скорее всего, объяснил Гоулд, в 1983 году Мур по невнимательности «неправильно заполнил бланк соглашения», обведя слова «не разрешаю» вместо «разрешаю». Мур прямо запретил университету использовать его клетки для медицинских исследований.

Клеточная линия – выращенная в лабораторных условиях группа клеток, обычно происходящая от единичной раковой клетки и продолжающая жить поколение за поколением. Ученые называют эти клетки *бессмертными*. Для биотехнологических исследований и разработки лекарств в мире используются сотни клеточных линий. По иронии судьбы очень часто эти клеточные линии живут дольше людей, от которых изначально была взята раковая клетка. На самом деле, некоторые из особо распространенных в современной биомедицине клеточных линий взяты от женщины по имени Хелен Лэйк [Helen Lake], умершей от рака в 1940-е годы.

Джон Мур не знал, что доктор Гоулд использовал клетки из его опухоли для создания «клеточной линии Мо».^[p47] Эта клеточная линия была производительной, поскольку в отличие от других клеточных линий она породила мощный антибактериальный и противораковый протеин, названный GM-CSF.¹⁶⁹ UCLA^[p48] решил запатентовать клеточную линию в 1983 году, когда юристы обнаружили, что Мур, кажется, никогда не

¹⁶⁸ Захватывающая история Джона Мура заимствована из 12-й главы «Outrageous Fortune: Selling Other People's Cells» прекрасной книги George J. Annas, *Standard of Care: The Law of American Bioethics*.

p47

Вероятно, это первые две буквы фамилии пациента: Moore – Мо.

¹⁶⁹ GM-CSF (granulocyte-macrophage colony stimulating factor) – гранулоцитарно-макрофагальный колониестимулирующий фактор.

p48

UCLA (University of California at Los Angeles) – Калифорнийский университет в Лос-Анджелесе.

передавал прав на использование своих клеток для этой цели.

Вместо того чтобы подписать соглашение, о котором его просили, Мур нанял адвоката. Когда в 1984 году патент был выдан, он подал иск против Калифорнийского университета, доктора Гоулда, его ассистента Ширли Куан [Shirley Quan] и двух корпораций, которые получали существенную прибыль от клеток его опухоли. Дело выглядело очевидным. В конце концов Мур явно отказал UCLA в праве использования своей клеточной линии в коммерческих целях. Но суд был другого мнения.

«По существу, суд первой инстанции решил, что Мур не имел права подавать иск», – пишет в своей книге «Стандарт заботы» [*Standard of Care*] Джордж Аннас [George J. Annas]. Апелляционный суд изменил решение, заявив, что врачом Мура было совершено нарушение в форме *присвоения прав*.^[p49] Это было то же самое обвинение, которое Аврахами позднее выдвинул против *US News & World Report*. Но в июле 1990 года Верховный суд Калифорнии снова поменял решение, заявив, что он не готов создавать новое право собственности на человеческие клетки и что биотехнологической индустрии будет нанесен невосполнимый финансовый ущерб, если выплачивать компенсацию людям, подобным Муру. По существу, пишет Аннас, Верховный суд Калифорнии встал на позицию «ответчика: исследователи, врачи, университеты и частные компании, а не отдельные люди, могут владеть человеческими клетками».

Случай Мура уникален не тем, что в его клетках содержался чудодейственный протеин, а тем, что он первый подал иск. Большое число компаний находило отдельных людей или целые семьи с редкими генетическими особенностями, выделяло соответствующий ген и использовало его для создания прибыльных продуктов – медицинских тестов и медикаментов. Мне не известно ни одного случая, когда человек или семья, благодаря которым был создан препарат, участвовали бы в будущей прибыли.

В середине 1990-х исследователи Крейтоновского университета в Небраске обнаружили человека с необычной генетической особенностью: его кости были более массивными, чем у обычных людей. Мутация была обнаружена случайно, в буквальном смысле этого слова. С человеком произошел несчастный случай – он попал в автомобильную аварию, в которой любой другой человек получил бы перелом ноги, но этого не произошло. Врач скорой помощи решил выяснить, почему перелома не произошло и обнаружил генетическую особенность под названием «повышенная масса костей» [High Bone Mass, HBM].

Исследователи из Крейтона провели работу и обнаружили, что эта особенность присуща всей семье. Членов семьи попросили принять участие в исследовании, которое заключалось в визите в лабораторию для сдачи анализа крови, чтобы помочь идентифицировать ген. Затем, в апреле 1997 года Крейтоновский университет объявил о заключении партнерского соглашения с Genome Therapeutics Corporation для выделения ответственного за особенность гена. Genome хотела разработать лекарство, действие которого было бы подобно этому гену. Будучи созданным, это лекарство могло быть использовано для лечения остеопороза – болезни, которой в США страдают две трети женщин старше 65 лет.

«Если мы сможем клонировать ген и идентифицировать причину болезни, а также создать лекарство для борьбы с ней, то [прибыль от продажи] лекарства может быть весьма существенной», – сказал в конце 1997 года финансовый директор Genome Therapeutics Финель Элой [Finel Eloi].¹⁷⁰ Элой отказался сообщить мне, насколько большим может быть рынок сбыта для лекарства от остеопороза. Вместо этого он отослал меня к статье,

p49

В оригинале – «tort of conversion» – деликт, гражданское правонарушение; незаконное присвоение имущества, незаконное использование чьего-либо имущества в собственных целях.

¹⁷⁰ Интервью автору, 27 августа 1997.

опубликованной в *Business Week* 1 сентября 1997 года. В ней сказано, что от остеопороза страдает больше женщин, чем от рака груди, рака матки и яичников вместе взятых, и что в 1995 году на лечение этих болезней в мире потрачено 14 миллиардов долларов.

Если Genome Therapeutics вдруг хорошо обогатится на этом, Крейтоновский университет получит часть прибыли за создание технологии. Но семья, являющаяся донором гена НВМ, не получит ничего. «С ними обходятся так же, как и с другими участниками научных исследований, – говорит Лори Элиот-Бартл [Lori Elliot-Bartle], пресс-секретарь университета. – Общепринято, что участникам исследований платят за время и причиненные неудобства в связи с участием в исследованиях. Обычно это не очень большие деньги».¹⁷¹

Возможно, людям и не надо платить много денег за их уникальную генетическую информацию. «Они делают это на благо общества», – говорит Лайза Геллер. Заключенный в рамках одной семьи, ген НВМ не имеет социальной или финансовой ценности. Более того, сам по себе ген не является обязательно необходимым для производства будущих чудодейственных лекарств – он просто помогает сделать свое дело компаниям вроде Genome Therapeutics, что гораздо проще.

С другой стороны, люди, являющиеся носителями неблагоприятных генов, принимают на себя все тяжести болезни. Общество не торопится предоставить справедливую компенсацию тем, кто родился с кистозным фиброзом (муковисцидозом), болезнью Гентингтона или фенилкетонурией. Мы не добавляем зарплату людям с аномально маленьким ростом, чтобы скомпенсировать их генетическую наследственность. Хуже того, мы позволяем страховым компаниям отказывать этим людям в страховом покрытии в связи с «ранее существовавшим состоянием». Говорить, что люди не должны на равных участвовать в прибыли, когда они имеют дело с исключительно удачливыми генетиками, значит соглашаться с Верховным судом Калифорнии: компании могут владеть генами, а отдельные люди – нет.

«Легко понять, почему люди хотят получить свои дивиденды», – говорит Марк Хэнсон [Mark Hanson], сотрудник расположенного в штате Нью-Йорк научно-исследовательского центра Hastings Center, специализирующегося на вопросах биоэтики. Но Хэнсон не считает, что вопрос лежит в плоскости права собственности; он считает, что это проблема информированного согласия. Если человек осведомлен об огромной финансовой прибыли и сознательно отказывается от прав, то это прекрасно, считает Хэнсон.¹⁷²

Пациентам можно предоставить выбор. Им можно предложить разовую оплату в несколько тысяч долларов с учетом того, что большинство использованных в исследованиях материалов не приводят к созданию лекарств, стоимостью миллиарды долларов. Либо пациент может выбрать вариант с получением определенного процента от прибыли. Пациент может даже согласиться не получать никаких денег вообще, обязав компанию перечислять определенный процент из будущей прибыли на благотворительность. Но трудно представить, что кто-то скажет: «Уважаемая Большая Генетическая Компания, пожалуйста, используйте мои гены для получения миллиардных прибылей и не беспокойтесь о том, чтобы поделиться со мной. Можете даже не дать мне ни одной акции. Ваше финансовое благополучие – моя награда вам».

В случае с Муром биотехнологическая индустрия заявила, что такое подробное отслеживание и ведение записей являются непомерным бременем для ученых и бухгалтеров компании. Но фактически для производства этих лекарств в первую очередь требуется более сложная система отслеживания. Биотехнологические компании не просто берут у людей кровь и сливают ее в одну большую емкость. Они *точно* знают, какой ген и от какого человека позволил получить данный результат. Дело не в технической возможности, для

¹⁷¹ Интервью автору, 27 августа 1997.

¹⁷² Интервью автору, 28 августа 1997.

соблюдения этого типа прав необходимы организационные процедуры.

Человеческая ткань не анонимна

Рассмотренные в этой главе медицинские проблемы усложняются тем, что многие люди просто не знают, что на образцах их тканей проводятся медицинские исследования. Согласно действующему этическому кодексу, исследования, проводимые на частях тела, не считаются нарушением прав пациента, если на образцах отсутствует имя пациента. Считается, что удаление имени человека с образца делает образец «анонимным».

Многие больницы, например, постоянно делают анализы крови на ВИЧ или присутствие запрещенных препаратов. Результаты этих анализов предоставляются в центры по контролю над заболеваемостью [Centers for Disease Control, CDC] для использования в статистических отчетах. «Недавно CDC в Атланте объявил о начале исследования, которое будет проводиться в течение года среди всех родившихся в Джорджии детей с целью оценки степени вреда от приема кокаина на последних стадиях беременности. Исследование будет анонимным и будет производиться на образцах крови, которые берутся в рамках обязательной программы штата по выявлению наследственных метаболических заболеваний (например, тест на фенилкетонурию)», – сообщается в статье, опубликованной в 1993 году в *Southern Medical Journal*. 173

Чаще всего эти «анонимные» анализы используются для внутренних исследований, но некоторые лаборатории продают образцы сторонним ученым и корпорациям. И иногда с них не удаляют имена. Одна моя знакомая, биолог из Бостона, однажды работала на фирму, разрабатывающую расширенный тест на бесплодие. Для исследований фирма получила несколько тысяч пробирок с сывороткой человеческой крови. Пробирки были получены из лаборатории, использующей самый современный тест на бесплодие, на каждую пробирку была нанесена информация о концентрации двух женских гормонов. Но как выяснилось, на пробирки была нанесена и другая информация: имя женщины, у которой был взят анализ. По существу, моя знакомая получила информацию об именах нескольких тысяч женщин Бостона, пытающихся забеременеть! «Предполагалось, что имена будут удалены с пробирок, но они забыли это сделать, – рассказывала мне она. – Среди имен мне встретилось имя, принадлежащее хорошо известной женщине. Мой руководитель не захотел извещать компанию, от которой мы получили образцы из-за боязни, что они не захотят продавать нам их в будущем». Стремясь защитить конфиденциальность этих женщин, моя знакомая взяла толстый черный маркер и закрасила имена на пробирках. Это был маленький акт протеста в защиту конфиденциальности.

Но даже анонимные образцы недостаточно анонимны, особенно если речь идет о генетических исследованиях. «Вы можете удалить имя, возраст, номер социального страхования, но вы не можете удалить необходимую для исследования информацию типа семейных связей, возраста приобретения заболевания и наступления смерти. Это существенно при производстве исследований», – говорит патологоанатом Линкольн Штайн [Lincoln Stein], работающий в проекте «Геном человека» в Институте Уайтхеда в Кембридже, штат Массачусетс. Очень мало людей, умерших от лейкемии в возрасте 65 лет, чья мать была жива в возрасте 91 год, объясняет Штайн. Человек может быть идентифицирован путем сопоставления «анонимных» медицинских данных с другой, свободно доступной информацией. Этот подход называется *триангуляцией*. 174

173 Jane E. Ellis, Larry D. Byrd, William R. Sexson and C Anne Patterson-Barnett, «In Utero Exposure to Cocaine: A Review», *Southern Medical Journal*, vol. 86 (7) (1993): 725–731.

174 Интервью автору, 28 августа 1997.

Еврейский ген

Но даже если не нарушена приватность отдельного человека, может пострадать приватность группы людей. В последние годы обнаружено большое число генетических заболеваний, присущих определенным этническим группам – особенно евреям европейского происхождения, так называемым евреям-ашкенази. Хотя исследователи не могут сказать, является ли данный конкретный человек носителем больных генов, исследование неизбежно бросает тень на всю этническую группу. Рассмотрим три медицинских исследования.

Рак груди. В 1995 году группа ученых из Национального ракового института [National Cancer Institute] обнаружила распространенное среди евреев-ашкенази специфичное изменение в определенном гене. Но этот ген не являлся подтверждением избранности евреев. Наоборот, ген BRCA1 у женщин существенно повышал риск развития рака груди.

Исследователи изучили 858 анонимных образцов крови, взятых у евреев-ашкенази, и обнаружили генетический дефект под названием 185delAG у восьми из них, чуть менее 1 %. Согласно данным другого исследования, 185delAG увеличивает шанс заболевания раком груди у женщин в 5 раз, от 4 из 25 (16 %) до приблизительно 4 из 5 (70–87 %).¹⁷⁵ «Эта частота изменения гена BRCA1 как минимум в три раза выше, чем все изменения гена BRCA1 вместе взятые у остального населения», – сказал в интервью *Baltimore Jewish Times* доктор Лоуренс Броди [Dr. Lawrence C. Brody].¹⁷⁶

Доктор Броди сразу же уточнил, что из этого не следует, что евреи-ашкенази чаще болеют раком груди, чем остальное население. В конце концов, ген BRCA1 имеет действие лишь на небольшой процент еврейских женщин. Но несмотря на это, ген неразрывно связан с еврейскими женщинами как с сообществом.

Основываясь на этих результатах, врачи провели исследование, в ходе которого 5 тысяч евреев-ашкенази из Вашингтона, федеральный округ Колумбия, были привлечены для сдачи крови и предоставления подробной истории болезни. Опубликованный 15 мая 1997 года в *New England Journal of Medicine* отчет снизил оценку канцерогенной способности 185delAG, но по-прежнему делал вывод, что еврейские женщины с мутировавшим BRCA1 или BRCA2 геном с вероятностью 56 % могут заболеть раком груди в какой-то момент своей жизни. «Мы не знаем, какие факторы изменяют риск заболевания раком, – говорит доктор Джеффри Стрюинг [Dr. Jeffery P. Struwing], возглавлявший исследование. – Здесь могут быть замешаны другие гены или факторы окружающей среды».¹⁷⁷

Рак кишечника. В августе 1997 года биологи онкологического центра Джонса Хопкинса [Johns Hopkins Oncology Center] в Балтиморе объявили, что ими обнаружен другой генетический дефект, присущий некоторым евреям-ашкенази. На этот раз дефект имел отношение к раку кишечника, одной из наиболее распространенных форм раковых заболеваний у американцев. Вероятность заболеть раком кишечника среди населения США составляет 9-15 %. У людей с дефектом гена эта вероятность вдвое выше. Ученые из онкоцентра Хопкинса обнаружили, что приблизительно 6 % евреев-ашкенази являются носителями дефектного гена, дающего 18–30 % вероятности заболеть раком. (Достаточно интересный факт: ученые не пытались установить встречаемость дефекта в целом у населения.)

Шизофрения и раздвоение личности. Когда я собирал материал для этой книги, я наткнулся в *New York Times* на объявление, призывавшее добровольцев принять участие в

¹⁷⁵ US Department of Health and Human Services, «Three Breast Cancer Gene Alternations in Jewish Community», National Cancer Institute Press Office, 05-20-1997.

¹⁷⁶ Melinda Greenberg, «Dr. Lawrence C Brody on Breast Cancer», *Baltimore Jewish Times*, 13 октября 1995.

¹⁷⁷ Интервью автору, 9 июля 1997.

еще одном исследовании по поиску дефектов у евреев (см. текст в рамке). В сентябре 1998 года исследователи опубликовали в журнале *Nature Genetics* статью, рассказывающую о том, что ими обнаружены области двух хромосом, которые, похоже, являются ответственными за предрасположенность к шизофрении.¹⁷⁸

Участие во всех трех исследованиях было анонимным – имена были удалены с образцов крови перед анализом. Во втором и третьем исследованиях анализ крови брался специально для исследовательских целей. (В первом случае ученые даже не озаботились получением разрешения – они просто получили образцы крови, оставшиеся после проведения обычного теста на болезнь Тая-Сакса.^[p50])

Семьи евреев-ашкенази должны помочь ученым понять биологическую природу шизофрении и раздвоения личности

Исследование будет проводиться факультетом психиатрии и эпидемиологическо-генетических программ университета Джонса Хопкинса. Исследователи ищут семьи с двумя или более детьми, диагностированными этими заболеваниями, у которых жив один из родителей, или семьи с двумя родителями и одним диагностированным ребенком.

Но хотя имена были удалены с образцов, наследственная информация осталась. Проведя анализы на образцах крови с наследственной информацией, ученые фактически провели генетическое тестирование всего сообщества.

Чтобы быть до конца честным, доктор Стрюинг сделал попытку получить некоторую форму коллективного согласия на проведение исследования среди 5 тысяч человек федерального округа Колумбия.

Мы создали оргкомитет, – говорит Стрюинг. – В комитет входило большое количество раввинов. Одного из членов комитета, раввина Авис Миллер [Avis Miller] из общины «Адаш Израэль», Вашингтон, федеральный округ Колумбия, специально попросили заняться вопросом получения согласия сообщества.

Как оказалось, я тоже отношусь к евреям-ашкенази. Поэтому, когда я услышал, что раввин Миллер дала согласие Стрюингу от моего имени, я позвонил ей и спросил, на каком основании. «Мы дали разрешение, – сказала мне раввин Миллер. – Я думаю, что нет никаких аргументов, во всяком случае, они мне неизвестны, и я о них не слышала, которые бы перевешивали пользу, которую это принесет сообществу».

Она продолжила:

Честно говоря, я не слышала опасений относительно проявлений антисемитизма, которые могут быть вызваны этим исследованием. Я слышала опасения, что способ использования информации может нанести вред отдельным людям. Я не слышала чтобы [люди говорили] о том, что можно использовать ее в евгеническом контексте. Мы слышали о том, что афро-американцы являются носителями серповидных клеток^[p51] [и подверглись дискриминации в результате], но евреи не те, кто будет чинить препоны науке из этих соображений, – по крайней мере, это относится к тем евреям, с которыми я

¹⁷⁸ John Hopkins School of Medicine, «Ashkenazi Jewish Families», Advertisement, *New York Times*, 23 сентября 1997.

p50

Генетическое заболевание, встречающееся в семьях евреев-ашкенази: вызывает раннюю смерть вследствие поражения мозга и нервной системы.

p51

По-видимому, речь идет о гене, вызывающем серповидно-клеточную анемию.

контактирую. Возможно, с нашей стороны было недальновидно не заглянуть за пределы кольцевой дороги, но антисемитизм в этой стране, по крайней мере, согласно многим исследованиям, снижается. Возможно, в 1930-е и 1920-е годы было больше поводов беспокоиться об этом.¹⁷⁹

Так, вероятно, и было бы. В 1940-е годы нацисты в Германии заявляли, что евреи являются низшей генетической ветвью и поэтому должны быть уничтожены. Имей Гитлер и его министр пропаганды Йозеф Геббельс информацию о гене BRCA1 или участке хромосомы, ответственном за шизофрению, им было бы во много раз легче убедить Европу пойти по германскому пути «окончательного решения еврейской проблемы».

Проект по исследованию разнообразия генома человека [Human Genome Diversity Project] часто сталкивается с проблемой согласия общественности, говорит доктор Джордж Аннас. Цель проекта – собрать репрезентативный генетический материал со всех этнических групп на земном шаре. Перед учеными встал вопрос: как получить разрешение? «Они хотели получить ДНК от индейцев племени Навахо, – рассказывает Аннас. – У Навахо есть совет племени, поэтому [ученые] обратились за разрешением в этот совет. Но не все группы имеют такой орган. От кого получать согласие на тесты евреев-ашкенази?»

Вероятно, из-за близости Национального ракового института к Бетесде, штат Мэриленд, привлеченные к исследованию BRCA1 и BRCA2 ученые решили, что представители еврейского сообщества Вашингтона, федеральный округ Колумбия, имеют некое позволение давать полномочное согласие от имени всего мирового сообщества евреев-ашкенази. Возможно, лучше было бы получить более представительный ответ. Возможно, у ученых есть причина не забрасывать слишком большую сеть: чем больше людей опросят ученые, тем выше шанс, что кто-нибудь будет протестовать против исследования. Аннас говорит: «Ученые [привлеченные к проекту] действительно не хотят заниматься этим вопросом, поскольку он очень сложный».

Расшифровка Исландии

Одно из генетически однородных сообществ, непосредственно столкнувшееся с вопросами владения и управления генетической информацией, – это Исландия.

Исландия выделяется своим географическим положением и наследственностью. Населяющий Исландию народ, численность которого составляет 270 тысяч человек, ведет свое происхождение всего от 20 тысяч «основателей». Нация, на которую в последние сто лет почти не оказывала влияния иммиграция, имеет очень подробные медицинские данные со времен Первой мировой войны и хранит образцы тканей и ДНК начиная со Второй мировой войны. Эта информация, с точки зрения теории, может помочь генетикам относительно легко идентифицировать генетическую природу многих заболеваний, возможно, тысяч.¹⁸⁰

В 1996 году профессор медицинского факультета в Гарварде доктор Кэри Стифансон [Dr. Kari Stefansson] решил создать коммерческое предприятие по сбору генетического наследия у себя на родине. Он привлек 12 миллионов долларов из американских венчурных компаний и организовал компанию deCODE Genetics, Inc. В планы компании входило производство генетических исследований в Исландии совместно с правительством и населением.

Компания Стифансона заявила, что для оправдания инвестиций, ей необходима эксклюзивная лицензия на генетическую информацию страны. В ответ было обещано, что

¹⁷⁹ Интервью автору, 1 сентября 1997.

¹⁸⁰ Прекрасное резюме истории с исландской базой данных и проекта deCODE может быть найдено в статье Ricki Lewis «Iceland's Public Supports Database, but Scientists Object», *Scientist*, vol. 13:15 (1999).

deCODE продаст свои акции жителям Исландии. Но обращение deCODE было не только чисто финансовым: компания утверждала, что Исландия находится в уникальном положении по сравнению с остальным человечеством и что она по этой причине обязана использовать свой генетический банк. В марте 1998 года парламенту Исландии был предложен билль, дававший deCODE искомую лицензию; три месяца спустя данные опроса Gallup Poll показали, что 90 % населения поддерживает такое решение.

В декабре 1998 года парламент принял билль, дающий deCODE эксклюзивную 12-летнюю лицензию на создание общеисландской базы здравоохранения [Iceland's Health Sector Database, HSD]. Спорным элементом принятого парламентом билля стало понятие «предполагаемое согласие». Если только человек не заполнил специальный бланк и не выслал его в адрес главного хирурга страны, его генетическая информация автоматически должна была включаться в базу данных. К июлю 1999 года только 9 тысяч человек из 270 тысяч населения страны исключили себя из списков.

Хотя банки данных, подобные HSD, предсказывались в научно-фантастической литературе, ничего подобного раньше даже не предпринималось. Неудивительно, что это вызвало противоречия. MANNVERND, Ассоциация исландцев за этику в науке и медицине [Association of Icelanders for Ethics in Science and Medicine], развернула кампанию против этой базы данных:

HSD намеревается завладеть всей медицинской информацией обо всем населении Исландии. Сюда попадают текущие записи, будущая информация и информация, как минимум, 30-летней давности. Закон позволяет скооперировать медицинские данные с обширной генеалогической базой данных, а также с базой индивидуальных генотипов ДНК. MANNVERND считает, что этот закон нарушает права человека, неприкосновенность личной жизни и общепринятые медицинские, научные и деловые стандарты. Мы считаем, что этот закон имеет общемировое значение, и отмена этого закона должна стать приоритетной задачей мирового сообщества борцов за права человека. Правительство Исландии в самой жесткой форме должно быть предупреждено о необходимости пересмотра этого законодательного акта и немедленной отмены постановления.¹⁸¹

Академическая общественность по всему миру протестовала против этого проекта. Типичным является письмо правительству Исландии, направленное профессором права Стэндфордского университета доктором Генри Грили [Dr. Henry T. Greely], генетиком с мировым именем, и профессором генетики и медицины из Вашингтонского университета доктором Мэри Клэр Кинг [Dr. Mary Claire King].¹⁸² В своем письме Грили и Кинг критикуют проект по следующим четырем пунктам:

Разрешение. По вопросу получения разрешения Кинг и Грили считают, что народ Исландии не мог дать должного разрешения на проект, поскольку не знал, как будет использоваться информация.

Билль дает возможность людям отказаться от участия полностью или частично, но не требует их информирования о том, какие именно исследования будут проводиться с их данными. Так, например, человек, который не желает принимать участие в любом виде исследований возможной генетической предрасположенности к алкоголизму, не обязательно будет знать, что его данные могут быть использованы с этой целью.

Конфиденциальность. Конфиденциальность – еще одна проблема проектов, подобных рассматриваемому, пишут ученые. Хотя база данных не будет содержать имен, информация из нее может быть легко использована для «вычисления» людей, от которых получен генетический материал.

Даже в Соединенных Штатах, на базе относительно небольшого количества

¹⁸¹ Адрес Mannvernd в Интернете <http://www.mannvernd.is/english/index.html>.

¹⁸² См.: http://www.mannvernd.is/english/articles/greely_&_king-e.html.

идентифицирующих признаков, «анонимные» клинические записи могут быть сведены к небольшому кругу людей среди 265-миллионного населения. В Исландии такая ценная медицинская информация, как пол, возраст, место рождения и число родственников, может позволить исландцу, работающему с этими данными, очень точно идентифицировать человека. Эта проблема неразрешима. В свете научной и медицинской ценности этой базы данных люди могут принять обоснованное решение об участии в проекте, но у них не должно возникнуть чувства ложной уверенности, что полная конфиденциальность может быть реально обеспечена.

Финансовые выгоды. Проблема финансового вознаграждения заразила проект с самого начала. На своем web-сайте deCODE хвастается, то 70 % капитала компании находится в руках исландцев. Однако этот капитал находится в руках исландских банков, а не населения страны. Хотя компания обещала обеспечить Исландии бесплатное медицинское обслуживание и ежегодно платить за пользование информацией, Грили и Кинг сомневаются, что эта компенсация является чем-то большим, нежели «легкая фракция» валового дохода проекта.

В качестве одной из наиболее значимых выгод для Исландии было обещано открыть новые рабочие места, связанные с базой данных, которая «не может быть экспортирована». Но электронная сетевая база данных на самом деле существует в любом месте компьютерной сети; ее физическое присутствие в Исландии не играет роли. Исследования с помощью такой базы данных могут быть и будут производиться учеными, которые сидят за компьютерами по всему миру. Просто трудно поверить, что значительная часть исследовательских ресурсов в области фармацевтики и биологии переместится в Исландию, поближе к базе данных. Так что заявление, будто база данных обеспечит высокооплачиваемую работу большому количеству исландцев, скорее злая шутка, чем реальность.

Научная открытость. Наконец, Грили и Кинг подвергают критике научную открытость проекта. Поскольку использование банка данных контролируется частной компанией, занимающейся медицинскими исследованиями, эта компания может заблокировать доступ конкурентам.

Это увеличивает финансовую ценность базы данных для лицензиата, но и снижает научную ценность информации, которая может быть использована более эффективно, если доступ к ней более свободен. В сущности, это означает, что контроль над научным использованием базы данных, так же как и над доходами от нее, находится не в руках народа Исландии, а руках корпорации, заботящейся о получении прибыли. Не имеет значения, насколько заслуживает доверия и патриотически настроено теперешнее руководство этой корпорации, решение о передаче полномочий по контролю должно быть принято Исландией очень взвешенно.

Если говорить о генетических исследованиях этнических групп, то горькая правда заключается в том, что результат – положительный или отрицательный в равной мере – коснется людей, которые не давали согласия на проведение исследования. Поскольку знание невозможно скрыть, жизненно важно принять законодательство, которое защитило бы всех людей от генетической дискриминации до того, как эти исследования будут запланированы и проведены.

Владеете ли вы своими книгами?

Когда вы покупаете журнал в супермаркете, все, что вы реально покупаете, это находящаяся в ваших руках бумага, чернила, оставляющие пятна на ваших пальцах, и лицензия на единичную копию содержимого журнала в печатной форме. Сами слова и изображения не продаются. Этот тезис справедлив и тогда когда вы покупаете компакт-диск, компьютерную программу и даже когда слушаете радио. Хотя возникает впечатление, что вы покупаете содержимое, на самом деле это не так: вы покупаете лицензию. Более того, зачастую делать вторую копию материала – незаконно.

Жаль бедных издателей: современные компьютерные технологии позволяют как никогда просто делать качественные копии опубликованных материалов. В этой ситуации логичной реакцией со стороны издателей должно было бы стать снижение цен, улучшение качества и ассортимента, упрощающие получение каждым желающим собственной лицензированной копии, вместо самостоятельного ее изготовления или поиска пиратской. Но очень малая часть издателей мыслит подобным образом. Вместо этого издатели разрабатывают технологии, затрудняющие копирование и упрощающие поиск и наказание виновных. В любом случае, эти технологии систематически нарушают права потребителей

В течение десятилетий различие между физическим владением отпечатанной книгой и правом обладания находящимися в ней словами оставалось для большинства людей непонятным. Высокая стоимость копирования печатной информации эффективно удерживала людей от изготовления своих собственных, неавторизованных копий содержимого книг. Но даже если несколько человек и делали копии, кого это волновало? Несмотря на то что в 1950-х годах существовало два коммерческих процесса фотокопирования: диффузионная передача и термография, – ни один из них не давал возможности делать копии на обычной бумаге. Получаемые копии имели странный запах, были странными на ощупь и выглядели не очень хорошо.

Все изменилось в 1959 году, когда компания под названием Haloid Xerox, Inc., представила на рынок копировальный аппарат Xerox 914. Базирующаяся на изобретении, сделанном Честером Карлсоном [Chester Carlson] в 1937 году, модель 914 стала первой копировальной машиной, автоматически делающей фотокопии на обычной бумаге.¹⁸³ Машина внесла революционные изменения в офисную жизнь и сделала Haloid Xerox, переименовавшийся в 1961 году в Xerox Corporation, гигантом, ворочающим миллиардами долларов. В 1963 году Xerox предложил миру первый настольный копировальный аппарат – Xerox 813. Три года спустя Xerox предлагает Xerox Telecopier, первый факсимильный аппарат, который мог передавать изображения по обычным телефонным линиям. В 1973 году Xerox начал продажу цветного копира модели 6500 – машины, способной делать полноцветные копии на обычной бумаге или прозрачной пленке.

Сделанные при помощи копировальных аппаратов Xerox копии могли быть использованы наряду с оригиналами для любых целей. В некоторых случаях копия даже была лучше, например фотокопия газетной статьи не была желтой. С появлением в 1968 году модели Xerox 3600 (первый копировальный аппарат, производивший 60 копий в минуту на обычной бумаге), а в 1970-м – модели Xerox 4000 (первая модель, способная делать двухсторонние копии), издателям стало совершенно ясно, что копировальная техника становится печатным станком, позволяющим самостоятельно переиздавать материалы, защищенные авторским правом.

Фотокопировальное оборудование не единственная технология, нарушающая права на интеллектуальную собственность. Появившиеся в 1960-е годы аудиокассеты позволили потребителям самостоятельно записывать музыку на ленту – копированием записей или непосредственно записывая радиотрансляцию. Видеомагнитофоны, появившиеся в начале 1970-х, открыли для пиратства фильмы. Домашние компьютеры создали принципиально новую категорию нелегально копируемой информации: компьютерное программное обеспечение. И в отличие от копировальной техники, аудио- и видеомагнитофонов, компьютеры создали принципиально новую угрозу авторскому праву: поскольку цифровая

¹⁸³ На самом деле Haloid Xerox, Inc. представила копировальный аппарат Model A, известный также под именем «Ох Вох» 22 октября 1948 года на ежегодной встрече Optical Society of America в Детройте. Весившая около 270 кг машина хотя и была выпущена на рынок год спустя, но для производства копии требовалось 14 ручных операций. В 1955 году компания выпустила Xerox Copyflo – первое автоматическое ксерографическое устройство, способное производить непрерывные копии на обычной бумаге. (Источник: *1987 Fact Book*, Xerox; а также «News Stories in 1948» с web-сайта Национальной службы здравоохранения [Nation's Health Service], <http://www.nhs50.nhs.uk/nhsstory-thisweek-oct25.htm>).

информация может быть скопирована без потерь, компьютеры могут делать идеальные копии компьютерных программ и, конечно, любой информации, которая может быть оцифрована.

В 1976 году конгресс пересмотрел национальное законодательство об авторском праве. В намерения законодателей входило приблизить авторское право к современным реалиям, когда технология позволяет изготавливать дешевые, но качественные копии оригинальных произведений. Согласно старому законодательству, автор должен был прямо заявить об авторском праве на произведение, иначе оно переходило в публичную область; новый закон установил, что все что угодно, зафиксированное однажды в материальной форме, автоматически защищается авторским правом. Закон также оговорил специальные исключения – для библиотек и для случаев «справедливого использования» [fair use]. По существу, *справедливое использование* означает, что конгресс Соединенных Штатов дает пользователям неявную лицензию на изготовление ограниченного числа копий защищенных авторским правом материалов без необходимости предварительного получения разрешения владельца авторских прав. (Например, принцип справедливого использования позволяет мне приводить цитаты из журнальных статей в этой книге без предварительного получения письменного разрешения.)

Для упрощения процесса получения разрешения на перепечатку, в 1978 году конгресс основал Клиринговую палату по авторским правам [Copyright Clearing House]. Клиринговая палата является централизованной некоммерческой организацией, принимающей платежи от конечных пользователей фото- и электронных копий и перечисляющей их в доход держателей авторских прав.

Новый закон об авторских правах предусматривает жесткие наказания за нарушение авторских прав. За эти годы конгресс сделал их еще жестче: во многих случаях нарушение авторских прав является уголовным преступлением, за которое грозит штраф в сотни тысяч долларов и десятки лет тюремного заключения.

Но издатели не стали полагаться лишь на защиту закона, они решили сделать неавторизованное копирование невозможным. В 1970-х годах некоторые издатели информационных бюллетеней стали печатать свои выпуски на серой бумаге специальными «невоспроизводимыми» синими чернилами. Издатели видеокассет испытывали различные системы искажения видеосигнала на кассетах таким образом, чтобы их можно было просмотреть, но не переписать. Разработчики программного обеспечения для компьютеров экспериментировали с различными формами защиты от копирования программного обеспечения. Все эти системы защиты от копирования работали, но лишь до некоторой степени: ни одна из них не смогла остановить пиратство сложного программного обеспечения; почти все они мешали работе законных пользователей.

Расцвет Всемирной паутины еще более усложнил проблему незаконного копирования. В Интернете нет ничего проще, чем скопировать статью или фотографию и послать ее кому-нибудь по электронной почте. Защищенные авторским правом статьи постоянно пересылаются в электронные списки рассылки, которые читают тысячи читателей. Почти всегда это происходит без получения разрешения и даже уведомления держателя авторских прав. Но одновременно с большим количеством невинных нарушений в Интернете приобрела мировой размах торговля пиратским программным обеспечением, так называемым «варезом».^[p52] Те же самые возможности компьютеров, которые делают их чрезвычайно полезными для использования в легитимных целях – высокоскоростной доступ, поисковые службы и шифрование, – оказались полезными и пиратам.

Согласно данным проведенного в 1996 году Business Software Alliance и Software Publisher Association исследования, «из 523 миллионов новых коммерческих программных приложений, использованных в 1996 году, 225 миллионов – почти каждая вторая копия –

p52

Компьютерный жаргон; калька от англ. warez.

были пиратскими...Потери доходов индустрии программного обеспечения от пиратства за 1996 год оцениваются в 11,2 миллиарда долларов».

Когда стало понятно, что защита от копирования не работает, издатели решили задействовать для борьбы с пиратством другую технологию – скрытую маркировку с помощью водяных знаков. Сама по себе маркировка не может предотвратить пиратство, но она дает потенциальную возможность установить людей, вовлеченных в этот процесс, или, по крайней мере, людей, слишком неосторожных в обращении со своими компьютерами.

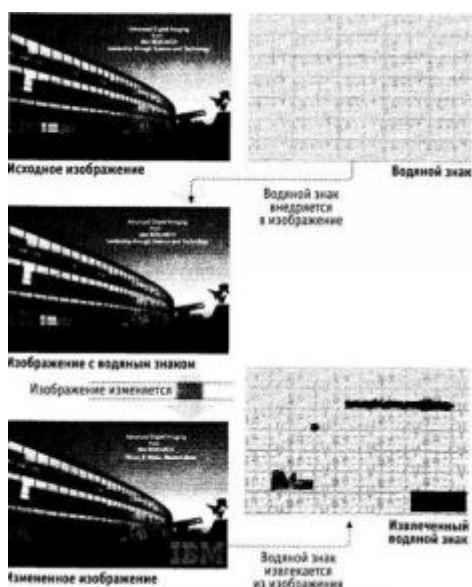
Соккрытие информации

Возьмите листок дорогой гербовой бумаги, посмотрите его на свет и вы сможете увидеть *водяные знаки* – узор, получаемый путем прижатия к бумаге в процессе сушки фигурной конструкции. Водяные знаки были изобретены в Италии в XIII веке. Итальянские производители бумаги использовали их как способ маркировки своего оборудования и как средство обнаружения подделок и подлогов.

Водяные знаки возродились в цифровую эпоху. Аналогично бумажным водяным знакам, цифровые водяные знаки – это часть информации, невидимая при обычном осмотре объекта, но заметная тем, кто знает, как ее найти. Большинство цифровых водяных знаков разработано в рамках систем управления правами на интеллектуальную собственность. Эти системы разрабатывались с целью предоставить возможность безопасно публиковать фотографии и другие виды цифровой информации в электронной форме. Скрытно поместив водяной знак в документ, издатель позднее может доказать, что какой-то человек или организация скопировала его информацию и использовала ее без разрешения. Лучшими считаются системы цифровых водяных знаков, в которых водяные знаки обладают *гибкостью*, т. е. остаются на месте даже при обрезке изображения или обработке его с помощью какого-либо цифрового фильтра.

Существует множество систем цифровых водяных знаков. Одна из таких систем, разработанная исследователями компании IBM, может скрывать водяной знак размером с кредитную карту в фотоизображении размером с журнальную страницу без видимых изменений последней. Во время демонстрации ученые спрятали слова IBM Research внутри фотографии здания исследовательской лаборатории IBM (IBM Watson Research Labs). Водяной знак может быть извлечен из изображения, даже если оно было изменено, – в этом случае водяной знак явно укажет на попытку обмана. В качестве дополнительной меры изображение водяного знака может быть зашифровано специальным ключом. Используя этот ключ, владелец может расшифровать водяной знак и доказать факт кражи. Но потенциальные пираты могут проверить изображение на предмет наличия водяного знака или изменить его настолько сильно, что водяной знак исчезнет.

Цифровые водяные знаки



Эти изображения, предоставленные доктором Минервой Янг [Minerva M. Yeung] из IBM T. J. Watson Research Center, демонстрируют скрытие водяного знака в изображении таким образом, чтобы он оставался даже в случае повреждения изображения. В первом ряду показано оригинальное изображение и помещаемый в него водяной знак. После внедрения водяного знака результирующее изображение фактически неотлично от исходного. В нижних двух изображениях показано, как внесение небольшого изменения в фотографию вызывает повреждения на извлеченном водяном знаке. Системы цифровых водяных знаков дают широкие возможности для отслеживания перемещения изображений как в Интернет, так и вне его. Поскольку водяные знаки могут быть зашифрованы, пользователи изображений могут даже не знать о их существовании. [Изображения любезно предоставлены компанией IBM]

Фотоизображения не единственный вид цифровой информации, который может быть помечен водяными знаками. Разработанная компанией DICE Company система Argent Digital Watermark System помещает цифровые водяные знаки в аудио- и видеозаписи. Система Argent может записывать в аудиопоток до 2100 бит в секунду, что эквивалентно 70 страницам текста в 10-секундном фрагменте. Информация может быть зашифрована, чтобы только издатель песни мог расшифровать данные, или помещена в открытом виде, чтобы доступ к ней имел каждый. Система обладает также высокой производительностью: водяной знак может быть вставлен в музыку непосредственно во время трансляции по радио или загрузки из Интернета.

Одна из интересных особенностей Argent – возможность сохранения в одном произведении нескольких каналов водяных знаков одновременно. DICE предлагает различные варианты использования этих каналов. Один канал может быть нешифрованным, чтобы компьютер или high-end проигрыватель мог отображать информацию о правообладателе, название, номер дорожки и другую информацию, связанную с музыкальным произведением. Другой канал может быть зашифрован и использоваться в качестве *защищенного канала распространения*, т.е. содержать информацию о специальных условиях, на которых производитель передает музыкальное произведение распространителю.

Самым крупным лицензиатом системы Argent является MCA Studios в Лос-Анджелесе, говорит президент DICE Скот Москович [Scott Moskowitz].¹⁸⁴ MCA экспериментирует с использованием системы для фирменной маркировки музыки, передаваемой распространителям для продажи публике. Технология Argent может быть также

¹⁸⁴ Интервью автору, 20 января 1997.

использована для поиска незаконных копий оцифрованной музыки в Интернете или библиотеках поставщиков онлайн-услуг. DICE надеется также лицензировать технологию и самим поставщикам онлайн-услуг, чтобы они могли использовать ее для защиты своих архивов. Поисковая технология может быть встроена и в поисковые системы, которые могли бы автоматически сканировать Интернет в поисках нарушения авторских прав.

Однако система Argent способна на большее, чем простое встраивание информации о правообладателе. Третий, также зашифрованный, канал цифровых водяных знаков – *защищенный канал владения* – может нести в себе информацию об имени человека, купившего фонограмму, уплаченной сумме, времени и месте покупки, а также об особенностях предоставленной ему лицензии на использование фонограммы. Таким образом каждая обработанная с помощью Argent фонограмма, содержит в себе подписанный цифровой подписью чек. При использовании этого канала каждый человек получает свою уникально персонализированную копию фонограммы, например загруженную именно на его компьютер или специально записанную для него на CD. Персонализированная таким образом музыка, по мнению Московича, могла бы стать мощным средством борьбы с пиратством. «Если вы говорите [покупателям], что распространение содержимого аналогично распространению номера кредитной карточки, они, скорее всего, будут более осторожны», – объясняет Москович. Но борьба с угрозой таким способом не простая задача. Она требует, чтобы личность каждого, кто покупает или получает фонограмму другим способом, была идентифицирована распространителем, и идентифицирующая информация заносилась в фонограмму до ее передачи. Это также подразумевает, что распространитель должен хранить эту информацию в файлах, чтобы при обнаружении нарушения авторских прав можно было отследить и наказать потребителя. Столкнувшись с такими драконовскими мерами, многие покупатели могут отказаться от приобретения музыки, преднамеренно предоставить ложную информацию или еще каким-либо образом обойти систему.

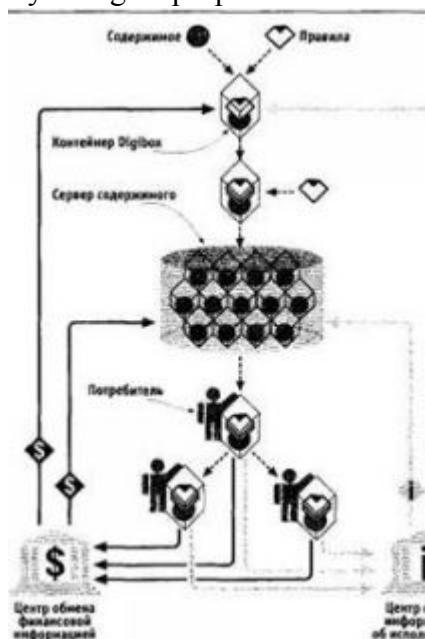
Ваш компьютер против вас

Подобные же водяные знаки разрабатываются для маркировки документов и изображений, обрабатываемых с помощью компьютера. Многие из этих систем зависят от запущенного на компьютере конечного пользователя *доверенного программного обеспечения* [trusted software]. Программное обеспечение конечного пользователя взаимодействует по сети с программным обеспечением на компьютере издателя. Программное обеспечение на компьютере издателя обеспечивает, чтобы каждый пользователь был обеспечен своей собственной, уникальной, персонализированной и снабженной водяными знаками версией документа. Программное обеспечение на компьютере клиента присматривает за конечным пользователем. Клиентское программное обеспечение регистрирует факт использования, пытается предотвратить попытки пользователя сделать несанкционированную копию и в некоторых случаях передает статистическую информацию издателю. Клиентское программное обеспечение называется «доверенным», потому что конечный пользователь вынужден доверять ему:

Электронное управление правами

DigiBox от InterTrust – система транспортировки защищенной авторским правом информации от создателя, через дистрибьютора к конечному потребителю и взыскания с последнего платы. Эта система *управления правами* базируется на «сильной» криптографии для защиты информации и специализированном программном обеспечении, защищающем информацию от копирования после расшифрования на компьютере конечного пользователя. Но систему можно обойти при помощи специального программного обеспечения, запущенного на домашнем компьютере. По этой причине в 1999 году конгресс принял, а

президент Клинтон подписал Digital Millenium Act.^[p53] Наряду с другими вещами, Digital Millenium Act инкриминирует человеку в преступление отключение программного обеспечения защиты от копирования, работающего на его компьютере. [Рисунок любезно выполнен Крисом Рейли из Reilley Design с разрешения InterTrust]



поскольку это программное обеспечение работает на его компьютере и нет эффективного способа проверки его функционирования. Современные компьютеры редко по доброй воле вступают в сговор с такими системами. Настольный компьютер общего назначения под управлением операционной системы Windows или Macintosh может быть легко перепрограммирован на обход любой формы диктата со стороны владельцев авторских прав. Но в будущем, конечно, компьютеры могут быть укомплектованы специальным оборудованием, которое обеспечит выполнение ограничений касательно авторских прав. Расположенная в Силиконовой долине фирма InterTrust – одна из нескольких компаний, создающих основу для таких систем. InterTrust разработала всесторонне продуманную схему доставки цифровой информации конечным пользователям со следующими предопределенными «бизнес-правилами».

Приобретение [purchase]. Пользователь однократно вносит плату и получает право на неограниченное использование.

Плата за каждое использование [pay-per-use]. Пользователь вносит небольшую плату каждый раз, когда пользуется информацией.

Смешанная оплата [upfront fee]. Осуществляется первоначальный платеж, за которым следуют последовательные небольшие платежи.

От аренды к владению [rent-to-own]. Неограниченный доступ предоставляется после определенного количества выплат.

Свободное использование [free use]. Как понятно из названия, это правило подразумевает неограниченный доступ без оплаты.

Система автоматически отслеживает каждого пользователя, взыскивает с него определенное количество денег, не позволяет ему удалить информацию об авторских правах

p53

Полное название – Digital Millenium Copyright Act, DMCA. На основании положений этого закона во время конференции, проходившей в Лас-Вегасе в июле 2001 года, был арестован сотрудник московской компании «Элкомсофт» Дмитрий Скляров. Российского программиста обвинили в нарушении упомянутого закона за то, что он разработал программу, позволяющую владельцу законно приобретенной копии электронной книги (e-book – специальный защищенный от копирования формат хранения информации) делать дополнительные копии.

и предотвращает попытки с его стороны воспользоваться правами, которые ему не предоставлены. В системе InterTrust вы можете заплатить пять центов за право просмотра документа через Интернет, дополнительно оплатить десять центов за право распечатать документ и один цент за право переслать документ другу, с которого, в свою очередь, будет взыскано пять центов за право прочитать больше, чем несколько первых абзацев. InterTrust базируется на идее, что корпорации будут заинтересованы распространять большое количество информации по очень низким ценам, если будут уверены, что каждое законное использование будет оплачено, а незаконное будет автоматически запрещено.

Цифровая подпись – один из базовых кирпичиков, на которых строятся системы управления правами, подобные InterTrust. *Цифровая подпись* – это полученный с помощью криптографических преобразований блок информации, который может быть создан одним человеком (или организацией) и проверен другим. С использованием цифровой подписи становится возможным снабдить документ уникальным идентификатором, именем подписавшего, информацией о времени и месте подписания и другими данными. [p54]

Подпись – очень гибкая технология. Подобно водяным знакам, музыкальное произведение может быть подписано автором, потом издателем, а затем каждым человеком, желающим передать его в электронном виде. В то же время цифровые подписи могут быть проверены очень быстро. Электронные сети вроде Интернета могут быть запрограммированы таким образом, чтобы не передавать информацию, пока отправитель не подпишет ее своей цифровой подписью. Аналогичным образом компьютеры могут быть запрограммированы так, чтобы принимать только должным образом подписанную информацию.

Водяные знаки и цифровые подписи являются мощными средствами искоренения анонимности, присущей сегодня цифровым носителям. Жители будущего, оглядываясь на последние дни XX столетия, удивятся, что идентичные копии книг, компакт-дисков, видеокассет и электронной информации когда-то распространялись среди тысяч, даже миллионов потребителей. Еще больше они будут поражены тем, что все эти люди владели компьютерами, магнитофонами и копировальными машинами, способными производить бесконечное число прекрасно подходящих для использования, если не полностью идентичных копий. Что могло остановить широкое распространение пиратства, кроме человеческой совести?

Конечно, боязнь водяных знаков может эффективно снизить уровень бесхитростного, случайного пиратства, столь распространенного сегодня. Но эти системы, скорее всего, бессильны против определенного круга посвященных лиц, имеющих доступ к цифровой информации еще до нанесения на нее водяных знаков. «В декабре прошлого года [1996] я был в Дублине, когда U2 закончили свой новый альбом. Не прошло и месяца, как два сингла из альбома стали распространяться через Web без разрешения», – рассказывает Москович. Вероятнее всего, утечка этих треков произошла через сотрудников студии.

Но даже если системы водяных знаков станут распространенными повсеместно, определенные пираты все равно будут находить способы неотслеживаемого получения дисков, которые они хотят скопировать. МСА может потребовать, чтобы диски продавались только после предъявления удостоверения личности с фотографией и снятия отпечатков пальцев. Но это не сможет воспрепятствовать банде пиратов ворваться в дом невинной девочки-подростка, украсть все ее любимые записи и выпустить их миллионным тиражом, подставив ее под удар. В конечном счете системы водяных знаков почти готовы для использования опасений и контроля в качестве средств предотвращения нарушения

p54

Следует упомянуть и еще об одном важном свойстве цифровой подписи. Она не только несет информацию о подписавшем ее лице, но и жестко связана с подписанным документом. Если эту подпись просто прикрепить к другому документу или изменить в исходном документе хотя бы один символ или даже бит, это сразу же будет установлено при проверке.

авторских прав.

Владеете ли вы тем, что делаете?

Если вы хотите попасть на премьерный показ кинофильма в Нью-Йорке, вы должны спланировать это заранее. Потому что на Манхэттене никто больше не выстраивается в длинные очереди за билетами. Вместо этого люди звонят по телефону 777-FILM – обычно в начале недели – и покупают билеты на выбранный сеанс по телефону. Основанная в 1989 году компания MovieFone продает сегодня билеты в 11 500 залов в 30 крупнейших городах – 60 % кинотеатров страны – и получает от 1,5 до 2,5 миллионов звонков еженедельно. Когда в мае 1999 года на экраны вышел фильм «Звездные войны: Эпизод I – Скрытая угроза» билеты во все манхэттенские кинотеатры были раскуплены заранее через MovieFone.

В настоящее время MovieFone получает доход от рекламы, прокручиваемой по телефону, и комиссионных от продажи билетов. Но у компании, приобретенной в феврале 1999 года America Online, [\[p55\]](#) вскоре может открыться еще один источник дохода: рынок аналитической информации, которая прогнозирует, какие фильмы будут успешными, какие неудачными и насколько.

Когда в День поминовения [\[p56\]](#) в 1997 году на экраны вышел фильм «Затерянный мир: Парк юрского периода», продажи билетов на него составили 59 % из всех проданных MovieFone билетов. К концу праздников фильм получил 61 % рынка всех проданных в США билетов. И это не было случайным всплеском. Когда 24 января 1997 года вышел «Любовь и война», продажи билетов на него через MovieFone составили 8 %, а в целом по рынку – 9 %.

Как говорится в опубликованной *New York Times* статье, это неслыханно высокий уровень прогнозирования:

«Крупнейшая компания по изучению мнения о фильмах National Research Group из Лос-Анджелеса зависит в своих прогнозах доходности фильма от дорогостоящих интервью с выборкой потенциальных зрителей. Этот метод, по сообщениям, дает погрешность плюс-минус пять процентов».¹⁸⁵

Другие службы делают это не лучше.

«В то время пока большая часть киноиндустрии вплоть до пятницы и субботы не знает, как „пойдет“ фильм, беглый взгляд на информацию MovieFone может дать вам точную оценку уже в начале недели», – сказал *New York Times* аналитик Alex, Brown & Sons Дрю Маркус [Drew Marcus]. Возможно, это происходит потому, что MovieFone *не является* оценочной службой. MovieFone представляет реальный срез рынка.

Подобная аналитическая информация представляет большую ценность для индустрии кинопроката: она позволяет кинотеатрам с несколькими залами определить, сколько экранов под какой фильм выделить, что позволяет получить наибольший доход. MovieFone изучает способы использования неожиданно открытой ею золотonosной информационной жилы. И конечно, фирма MovieFone не одинока. Президент Amazon.com [\[p57\]](#) Джеф Безос [Jeff Bezos]

p55

Один из крупнейших поставщиков услуг Интернета.

p56

Memorial Day – официальный нерабочий день, отмечаемый в США в память о погибших во всех войнах.

185

Sreenath Sreenivasan, «What Is a Hit Film? Moviefone May Know», *New York Times*, 2 июня 1997.

p57

Один из крупнейших web-магазинов, торгующих через Интернет различными товарами, в том числе книгами.

сказал мне, что его компания может спрогнозировать, насколько хорошо будет продаваться книга за несколько месяцев до ее выхода на основе предварительных заказов клиентов. Система поиска информации в Интернете Infoseek построила список наиболее часто находимых web-сайтов путем анализа наиболее часто вводимых в строку поиска слов. Эта информация может быть обработана и продана рекламным агентствам.¹⁸⁶

Но чью информацию на самом деле продают эти компании? Информация располагается на компьютерах MovieFone, поэтому она, судя по всему, принадлежит этой компании. С другой стороны, ни MovieFone, ни Amazon.com, ни Infoseek не смогли бы создать эту информацию без помощи клиентов: возможно, доходы должны быть поделены. И кто устанавливает границы использования накопленной компаниями информации? Поскольку клиенты оплачивают заказанные через MovieFone билеты при помощи кредитных карт, MovieFone знает личность каждого клиента, и она, конечно, может продать эту информацию торговцам. Или новый владелец MovieFone – America Online – может совместить кинопредпочтения с другой информацией и продать полученный поток данных на информационном рынке.

Как мы увидели в предыдущей главе, многие супермаркеты и аптеки уже используют информацию о своих клиентах таким способом. Супермаркеты, по крайней мере, платят своим клиентам за это право путем предоставления скидки, когда клиенты предъявляют свои клубные карточки.

Информация о транзакциях в сочетании с информацией о личности очень ценна. Возможно, что в будущем газеты будут иметь разную стоимость, в зависимости от того, какое количество персональной информации вы готовы раскрыть: бесплатно – если вы согласны сообщить издателю свои имя, адрес и номер телефона; десять центов – если вы согласны раскрыть свои возраст и пол; один доллар – если вы хотите читать ее анонимно, т. е. не позволяя издателю использовать вашу личность в коммерческих целях.

Конечно, информация о личности – это еще не все. MovieFone показала, что потенциально прибыльная информация может быть получена из транзакций путем обезличивания и консолидации. Но было бы неразумным думать, что такие компании, как MovieFone, ограничатся продажей простых массивов информации, если персонально идентифицируемая информация может принести дополнительную прибыль.

Хотите ли вы использовать право владения для защиты вашей приватности?

Идеи права собственности и приватности существуют уже тысячи лет, но идея использовать режим интеллектуальной собственности для защиты приватности так и не прижилась. Возможно, это и к лучшему, что вышло именно так. Совершенно не очевидно, что корпоративная Америка с радостью уступила бы такое ценное право потребителям. Американцам пришлось бы платить ренту за право пользоваться своими собственными именами.

На слушаниях по вопросам приватности в Федеральной комиссии по торговле, вице-президент Equifax по вопросам приватности и внешних отношений, Джон Форд [John Ford] сказал, что существует два взгляда на владение информацией. Некоторые люди могут сказать: эта информация принадлежит мне, и поэтому вы не должны ее использовать. Другие могут возразить, что это не ваша информация, это информация о вас.¹⁸⁷

Я храню на своем компьютере адресную книгу с именами, телефонными номерами и адресами электронной почты моей семьи, моих ближайших друзей и других людей, с

¹⁸⁶ Лекция в Вашингтонском университете, 25 февраля 1997.

¹⁸⁷ Джон Форд был процитирован в интервью автору Джеком Роджерсом [Jack Rogers] 19 апреля 1995.

которыми я встречался. При последнем подсчете в файле было 1386 имен. У меня есть и еще один файл – с деловыми контактами. В нем 1579 записей, некоторые с тремя или четырьмя фамилиями. Должен ли я предоставить этим людям или компаниям возможность удалить себя из моей адресной книги? Скорее всего, нет. В конце концов, это моя адресная книга.

9

Экстремисты и террористы

Семнадцатого июля 1996 года. Рейс 800 авиакомпании Trans World Airlines начался, как и многие другие, – с задержкой. Стояла жаркая летняя ночь, и лайнер ожидал на полосе своей очереди на взлет более 30 минут. Боинг-747 с 230 пассажирами на борту быстро покинул нью-йоркский аэропорт имени Джона Ф. Кеннеди и стал набирать высоту над проливом Лонг-Айленд. Приблизительно через 30 минут полета случилось нечто ужасное. Очевидцы на земле наблюдали небольшой взрыв, два летящих в воздухе объекта, а затем второй, более мощный взрыв. Лайнер упал в воду с высоты более 3 км. Все находившиеся на борту погибли.

Почти сразу же агенты нью-йоркского офиса ФБР начали следствие путем изучения обломков самолета, плавающих на месте падения. Фрагменты, обломки и личные вещи были помещены в огромный ангар на Лонг-Айленде, где следователи решали тяжелую и кропотливую задачу по реконструированию каркаса самолета. Через несколько дней водолазы начали поиск на дне моря дополнительных доказательств. Тем временем, как внутри, так и за пределами Бюро, циркулировали самые разные версии причин катастрофы. Вскоре стало ясно, что существует только три возможных объяснения катастрофы: отказ оборудования, бомба на борту или ракета класса «земля-воздух».

Беспрецедентные усилия по сбору доказательств продолжались в течение следующих нескольких месяцев. Покореженные кусочки металла, болты и найденные обрывки ткани были помещены в ангар и проанализированы. Стоимость расследования составила в конечном счете более 100 миллионов долларов. ФБР приступило к действиям. Исходя из предположения, что рейс 800 погиб в результате взрыва бомбы, ФБР совместно с политиками и официальными лицами авиакомпаний усилили режим безопасности в аэропортах. Многие поборники гражданских свобод подвергли резкой критике меры ФБР, утверждая, что это широкомасштабная атака на личную независимость и гражданские свободы американских граждан. Но чем больше погибших было извлечено из воды, тем слабее были эти протесты.

Две недели спустя после катастрофы рейса 800 произошел второй взрыв. На этот раз целью были выбраны летние Олимпийские игры в Атланте: один человек погиб, более ста получили ранения.

Теперь при посадке в самолет от пассажиров стали требовать предъявления документа с фотографией, даже если рейс был внутренним. Затем ФБР настояло на общенациональной системе профилирования пассажиров, чтобы лица, вызывающие подозрения в предрасположенности к совершению террористических актов, задерживались и досматривались в аэропортах. (В результате этих досмотров тысячам американцев арабского происхождения были доставлены неудобства, а в некоторых случаях их задерживали.)

Тем временем Американская почтовая служба установила широкомасштабные ограничения: пакеты и письма весом более одного фунта [454 г] отныне нельзя было бросать в почтовые ящики – ведь такое отправление могло содержать бомбу! Вместо этого тяжелые почтовые отправления должны были сдаваться служащему почтового отделения, что обеспечивало визуальную идентификацию. Эти ограничения продолжают действовать и по сей день.

За последнее десятилетие меры, принятые из-за угрозы внутреннего терроризма, стали оказывать существенное влияние на жизнь большинства американцев. Эта глава ставит

очень простой вопрос: дали ли эти меры реальный эффект? Чтобы понять это, мы должны сначала больше узнать о самом терроризме.

Демократизация деструктивных технологий

Лицо терроризма меняется. Большую часть XIX и XX веков терроризм был средством, которым добивались политических перемен. Терроризм был войной, которую вели угнетенные народы. У террористов были определенные цели: избавление от рабства, свержение определенного режима, политическое признание, – и они использовали насилие или его угрозу для достижения этих целей.

Террористы «старого стиля» часто действовали в составе больших групп; иногда они были частью легальных политических или околополитических организаций. В любом случае, большинство членов этих групп оказывали некую форму сдерживающего влияния на действия террористов. Даже если один из безумцев хотел лишь убить как можно больше невинных свидетелей, его соратники могли остановить его, убедив, что бессмысленное насилие не укрепит позиции, а наоборот, лишь усилит решимость оппонентов.

Террористы 1980-х и 1990-х годов были переходным звеном. Несмотря на то что это были боевики, сотрудничающие с крупными организациями и даже правительствами, они использовали террор не как средство достижения изменений, а как форму мести. Взрыв рейса 103 авиакомпании Pan American над Локерби в Шотландии в 1988 году, скорее всего, был мстью за бомбардировку Соединенными Штатами Триполи в начале 1980-х. Захваты в 1980-е годы американцев в заложники в Ливане были, наиболее вероятно, ответом на обстрел Бейрута США в 1984-м. Хотя американская общественность рассматривала эти действия как террористические, более правильным было бы классифицировать их как военные действия.

Террорист завтрашнего дня – иррациональный террорист. Этот новый террорист не ставит своей целью изменение мнения противника. Он «рассматривает полное физическое уничтожение противника как продуктивный результат», – говорит Луис Рене Берес [Louis Rene Beres], профессор политологии университета Пардью, не один десяток лет изучающий истоки терроризма и способы борьбы с ним.¹⁸⁸ Новое поколение террористов действует небольшими ячейками, парами или в одиночку.

Эти новые террористы часто даже не заинтересованы в переговорах, не оценивают отдаленные последствия своих действий и зачастую даже не заботятся о сохранении своих собственных жизней – фактически они активно стремятся к своей смерти. «Иррациональный террорист может быть членом группы безумцев, которая рассматривает массовую смерть как желаемый результат, с экологической точки зрения, – говорит Берес. – Либо иррациональный террорист может рассматривать террористический акт и потерю жизни как спусковой механизм для каких-либо других политических событий».

«Мы имеем дело с [новым] видом патологии – болезнью», – сказал профессор Берес на лекции в Вашингтонском университете весной 1997 года. До сих пор США везло – мы сталкивались лишь с небольшими проявлениями антиамериканского террора. Но Берес считает, что наше везение может скоро кончиться.

Вопрос, который при этом встанет перед нами, очень простой: возможно ли предотвратить террористические акты путем систематического мониторинга всех потенциальных террористов и заключения их в тюрьму до того, как они нанесут удар? И если да, то какова цена этих мер?

Блюдо смерти

¹⁸⁸ Луис Рене Берес, лекция в Вашингтонском университете, май 1997 года.

Через почтовый отдел штаб-квартиры B'nai B'rith International, расположенной в Вашингтоне, федеральный округ Колумбия, ежедневно проходит огромное количество отправок. Однако этот конверт отличался от остальных. Пупырчатая обертка размером 8x10 была повреждена, и из нее сочилась желеобразная субстанция. Отправление было адресовано просто «B'nai B'rith», – ни имени, ни номера комнаты.

Служащий почтового отдела передал отправление Кармену Фонтана [Carmen Fontana], директору по безопасности еврейской организации. Фонтана рассказал мне:

Пакет выглядел необычно. Я понюхал его. От него исходил запах, похожий на аммиак. Я на 100 % был уверен, что это бомба. Я немедленно поместил его в мусорный контейнер и вынес наружу. Вернувшись, я попросил охранника вызвать полицию.

Прибывшие саперы изучили содержимое при помощи рентгена. Внутри ничего не было видно, похожего на бомбу. «Тогда они открыли его, – рассказывает Фонтана. – Внутри пакета оказалась чашка петри [p58] с красной субстанцией. На чашке петри были нанесены какие-то цифры. Они прочитали их и идентифицировали содержимое как сибирскую язву». ¹⁸⁹

За этим последовала восьмичасовая блокада. Вашингтонская полиция немедленно закрыла район в 20 кварталов вокруг штаб-квартиры B'nai B'rith. Пакет был помещен в обеззараживающую коробку и передан для анализа в Военно-морской госпиталь в Бетесде. Но центр города, полиция и пожарные готовились к самому худшему. Городские улицы, здания и парковки были закрыты, не давая возможности более чем 10 тысячам человек уйти домой. Еще больше людей застряло в пробках, быстро образовавшихся в столице. Тем временем, во избежание заражения, 150 служащим B'nai B'rith было сказано не покидать здание.

В 20.30 в госпитале закончили предварительный анализ. Красная субстанция содержала какие-то бактерии, но они не были сибирской язвой. Специальный уполномоченный по вопросам здравоохранения Вашингтона доктор Харви Слоан [Dr. Harvey Sloane] объявил, что служащие еврейской организации могут идти домой. Все произошедшее было розыгрышем.

Этот инцидент, произошедший в апреле 1997 года, показал, что столица абсолютно не готова к биологической атаке. Несмотря на то что в процессе подготовки к инаугурации президента в 1996 году проводились тренировки по отработке подобных инцидентов, 14 сотрудников спасательных служб города по неосторожности получили контакт с субстанцией и также подлежали обеззараживанию. В то же время карантин для 150 служащих был плохо продуман, считает доктор Джонатан Такер [Dr. Jonathan B. Tucker] из Центра исследований проблем нераспространения [Center for Nonproliferation Studies]. «Желеобразный биологический агент представляет опасность только при прямом контакте... Вместо того чтобы в течение нескольких часов держать служащих на карантине внутри здания, подвергая их дополнительному воздействию опасного материала, более правильным было перевести их в другое место и держать под наблюдением, пока не станут известны результаты анализов». ¹⁹⁰

«Неподготовленность просто поразила меня, – говорит директор по безопасности Фонтана. – Я не пытаюсь бросить камень в полицейских или пожарных – они сделали все, что могли. Но их подготовка была чрезвычайно мала, если была вообще. У пожарных не

p58

Низкая закрывающаяся емкость, используемая в микробиологии.

¹⁸⁹ Интервью автору, 14 мая 1997 года.

¹⁹⁰ Интервью автору, 11 августа 1997 года.

было необходимого оборудования».

И при этом они, кажется, не имели соответствующего опыта. Рассказывает Фонтана:

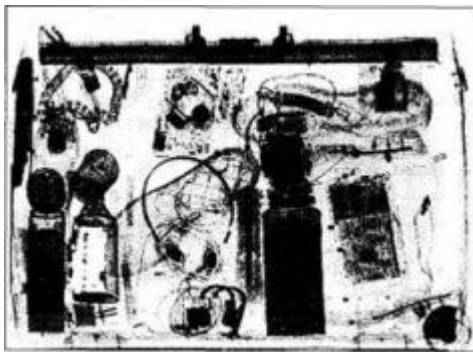
Это надо было видеть собственными глазами. У нас не было дезинфекционной палатки, поэтому они поставили рядом два грузовика и натянули поверх них кусок брезента. Затем они поместили на землю кусок пластика. Это стало дезинфекционным душем...Затем нас обработали хлороксом, который в процессе обработки собрался на пластике, – они просто сложили его и вытряхнули на улицу. Это поразило меня до глубины души. Я сказал: «Хорошо, а что будет, если хлорокс не полностью убил сибирскую язву? Вы просто заразите весь город». Им просто не хватало подготовки. Я вспоминаю, как 35 лет назад на военной службе мы отрабатывали действия на случай применения химического и биологического оружия, там не было ничего похожего на то, что делали эти парни.

На следующий день B'nai B'rith выпустила пресс-релиз, в котором благодарила городскую полицию и пожарных за быструю реакцию и самоотверженную работу, но заметила, что «серьезно обеспокоена очевидной недостаточностью подготовки»: «Для полиции и пожарных такого уязвимого к террористическим актам города непростительно не иметь высочайшего уровня подготовки и соответствующих ресурсов для действий в таких потенциально смертельно опасных ситуациях, как эта. Мы обращаемся к городским и федеральным властям с просьбой немедленно осуществить проверку, насколько город готов к подобного рода инцидентам», – заявил исполнительный вице-президент B'nai B'rith доктор Сидни Клерфилд [Sidney M. Clearfield] в распространенном на следующий день пресс-релизе.

Если бы террорист хотел совершить акт в штаб-квартире B'nai B'rith, он мог бы это сделать с гораздо меньшим шумом и с гораздо более катастрофическими результатами. Вместо того чтобы отсылать чашку петри с фальшивыми бактериями, террорист мог послать в запечатанной трубочке постер и порошок, содержащий споры настоящей сибирской язвы. Для осуществления гораздо менее технически сложной атаки, террорист мог узнать название предпочитаемого B'nai B'rith предприятия общественного питания и приготовить отравленную еду для доставки к следующему благотворительному обеду организации.

Сканер багажа компании Vivid

Компания Vivid Technologies, штаб-квартира которой расположена в Вобурне, штат Массачусетс, является производителем сложных систем досмотра багажа и ручной клади для аэропортов и офисных зданий. Система обнаруживает спрятанные в багаже оружие, взрывчатые вещества и наркотики путем просвечивания рентгеновскими лучами и обработке полученного изображения системой искусственного интеллекта. В отличие от обычных рентгеновских систем досмотра, которые контролируют лишь контуры предметов, система компании Vivid анализирует изменение энергии прошедших сквозь предметы рентгеновских лучей, определяя атомы и молекулы, характерные для взрывчатых веществ и других подлежащих контролю субстанций. На сегодняшний день основные продажи компании Vivid осуществляются за пределами Соединенных Штатов, поскольку Федеральное управление авиации [Federal Aviation Administration] запретило аэропортам конкурировать между собой в вопросах обеспечения безопасности. [Фотография любезно предоставлена Vivid Technologies]



С такими уязвимыми объектами, такими неподготовленными гражданскими органами власти и с такой высокой доступностью токсических веществ имеет ли смысл установить всемирную сеть для отслеживания и задержания подозреваемых в терроризме до того, как они нанесут удар? Правительство США все больше склоняется к положительному ответу на этот вопрос.

Изменяющееся лицо терроризма

Несмотря на то, что атака на штаб-квартиру B'nai B'rith произошла почти год спустя после гибели рейса 800 авиакомпании TWA в апреле 1997 года, она показала неэффективность предложенных ФБР антитеррористических рекомендаций в борьбе с новым поколением террористов. Досмотр авиапассажиров не дает эффекта, когда целями становятся здания. Запрет на пересылку почтой отправлений весом более одного фунта не принесет своих плодов, поскольку одна небольшая пробирка может вместить количество бактерий достаточное, чтобы убить целый город.

В мире всегда существовали сумасшедшие и фанатики. Но постоянно увеличивающаяся доступность деструктивных технологий меняет ставки. Вооруженный двустолковой сумасшедший сотрудник офиса может убить трех или четырех сослуживцев. С автоматическим оружием этот же человек может лишить жизни дюжину людей. Но разбив пузырек с бактериями сибирской язвы о пол лифта, безумец может убить всех в огромном офисном здании. Опасность состоит в том, что при существующем развитии событий в распоряжении разгневанного или душевнобольного человека окажется целый арсенал деструктивных технологий, которые он может использовать против общества в целом. Таким образом, даже если число экстремистов и террористов останется примерно постоянным, вместе с увеличением доступности смертоносных технологий нам следует ожидать ежегодного увеличения числа жертв массовых убийств, взрывов и широкомасштабных атак.

К сожалению, количество экстремистов и террористов не остается постоянным: оно увеличивается. С ростом населения общество становится более сложным, все больше людей оказывается выброшенными на обочину и вынужденными к активным действиям. Современные коммуникации и увеличивающаяся легкость перемещений лишь умножают число опасных психов, поскольку насилие, как и многие другие болезни, заразно. Одиноким помешанный может совершить не более одной смертоносной операции. Но путешествующий и учительствующий безумец может посеять семена десятков инцидентов.

Террористов ободряют также действия или бездействия народов мира. В 1980-х годах мир безучастно наблюдал, как Ирак использует химическое оружие, сначала в ирано-иракской войне, а затем против своих же граждан – курдов. «Убийства при помощи химического оружия сходили Ираку с рук в течение пяти лет, – говорит Леонард Коул [Leonard A. Cole], преподаватель Ратджерского университета, изучающий химическое и биологическое оружие. – В то время мы рады были, что Саддам Хусейн и Аятолла Хомейни заняты друг другом».¹⁹¹ Но, не осудив использование этого оружия, мировое сообщество

¹⁹¹ Интервью автору, 11 августа 1997 года.

узаконило его.

Сочетание харизмы и криминального таланта достигло своего пика в марте 1995 года во время химической атаки в токийском метро, произведенной религиозным культом Аум Синрике («Высшая истина»). Несмотря на то что Япония давно имеет дело с террористическими организациями, она оказалась полностью не готовой к такой атаке. В результате погибли десятки людей, а более 5 тысяч получили отравление. Среди пострадавших было 135 токийских пожарных и полицейских, устремившихся в подземку без соответствующих средств защиты.

В распоряжении религиозных террористов был подробный план токийского метро, что позволило им оптимально разместить емкости с ядом. Преступная организация не предъявляла никаких требований, и атака началась без всякого предупреждения. Единственной целью Аум было убить как можно больше людей, приблизив тем самым конец света. Действительно, глобальный план Аум направлен на уничтожение человечества. «Было очевидно, что у них достаточно исходных химических веществ для получения зарина в количестве, достаточном, чтобы убить половину населения Земли», – говорит Джеймс Колстром [James D. Kallstrom], возглавлявший нью-йоркский офис ФБР и курировавший расследование взрыва рейса 800 TWA.¹⁹² В череде следовавших за токийской атакой разоблачений, Колстром рассказывал о раскрытых ФБР планах Аум по созданию биологического оружия и проводившихся работах с бактериями сибирской язвы и ботулизма.

Почему же в результате атаки не погибло больше людей? Потому что на этот раз человечеству повезло. Или по причине пробелов в японской системе образования. В своем стремлении воплотить в жизнь план по уничтожению мира, руководители Аум задействовали ученых, а не инженеров. Ученые разбирались в химической составляющей создаваемого ими оружия, но они не знали, как правильно распылить вещество.

Как и многие другие эксперты-практики, Коул считает, что для предотвращения химического, биологического и ядерного терроризма одновременно должны быть сделаны две вещи. Первая – признание всеми народами мира неприемлемости этих видов оружия и запрет их использования. Вторая – выделение необходимых ресурсов на мониторинг исходных составляющих, необходимых для создания такого рода оружия террора, а также мониторинг потенциальных террористов.

Доморощенный терроризм

Мониторинг террористов стал высокоприоритетной задачей ФБР, которое постоянно повторяет, что задача по защите Америки от терроризма осложняется современными технологиями. В начале 1990-х ФБР проталкивало несколько технических предложений, призванных облегчить задачу. Среди этих предложений была разработка новых технологий перехвата информации, ограничение на использование криптографии и досмотр авиапассажиров. Одним из главных сторонников этих программ внутри ФБР был Джеймс Колстром, возглавлявший техническое подразделение ФБР в Куантико, штат Виргиния, до того как стал директором офиса ФБР в Нью-Йорке.

В 1997 году я встретился с Колстром, чтобы поговорить о проблемах терроризма и их потенциальном влиянии на свободу и приватность. Встреча проходила в разгар расследования взрыва рейса 800 TWA, и уже было ясно, что ведение расследования серьезно скажется на Колстроме. Год спустя он ушел из ФБР на должность вице-президента крупного финансового учреждения. Колстром сказал мне, что мониторинг террористов очень сложен:

Когда я пришел в ФБР, основной проблемой была организованная преступность. Но это просто детские игрушки по сравнению с группами, с которыми мы имеем дело сегодня. У

¹⁹² Интервью автору, 11 августа 1997 года.

них нет определенной иерархической структуры. У них нет дисциплины и установленных правил поведения. У них нет совещательного органа управления. У них отсутствует централизованное управление. У них нет всех тех вещей, которые позволяют вам, если вы имеете минимальный доступ к организации, в достаточной степени знать, чем организация занимается.

Сегодня мы имеем людей, которые открыто говорят о проблемах в любом сегменте нашего общества, заводя слушателей страстным красноречием. Вы не знаете, какая группа из двух или трех психов воспримет эти речи и претворит их в жизнь, – если только вы не один из этих людей.

В гораздо большей степени, чем другие страны, Соединенные Штаты знакомы с проблемой насилия, совершаемого одиночками. Одной из причин этого является простота получения доступа к оружию в Соединенных Штатах.

Джон Уилкс Бут [John Wilkes Booth] открыто поддерживал рабство и организовал банду для убийства Авраама Линкольна и госсекретаря Уильяма Сьюарда [William Seward], но в конечном счете именно Бут нажал на курок и убил Линкольна 14 апреля 1865 года. Чарльз Гито [Charles J. Guiteau] застрелил президента Джеймса Гарфилда 2 июля 1881 года. Анархист Леон Уолгош [Leon Czolgosz] застрелил президента Уильяма Мак-кинли [William McKinley] 6 сентября 1901 года на выставке Pan-American в Буффало. Ли Харви Освальд выстрелил и убил президента Джона Ф. Кеннеди 22 ноября 1963 года. Джон Хинкли-младший [John W. Hinckley, Jr.] выстрелил и серьезно ранил президента Рональда Рейгана 30 марта 1981 года. Попытки покушения на жизнь президента продолжаются и сегодня: во время первого пребывания на посту президента Билла Клинтона был задержан человек, стрелявший по Белому дому из автоматической винтовки.¹⁹³ Другой человек погиб, направив легкий самолет на лужайку Белого дома, как раз под окнами спальни президента Клинтона.¹⁹⁴

Но пока ФБР озабочено одинокими преступниками, реальную угрозу сегодня представляют действия террористов, направленные на массовые убийства. И снова способствующим фактором является широкая доступность деструктивных технологий. За последнее десятилетие террористы взорвали заминированную машину перед зданием Всемирного торгового центра в Нью-Йорке, погибло шесть человек, тысячи ранены, нанесен ущерб в 500 миллионов долларов. Тимоти Маквей взорвал заминированный автомобиль перед федеральным зданием Alfred Murrah в Оклахоме, убив сотни людей.

Колстром считает, что в ближайшие 30 лет вполне возможно ожидать, что один террористический акт унесет жизни более 10 тысяч человек. «Я не хотел бы предрекать это, но я думаю, что было бы наивным говорить, что это невозможно», – говорит он. И если это произойдет, продолжает он, со стороны части законодателей и общественности последует бурная реакция с требованием ввести драконовские законы и установить настоящее полицейское государство, чтобы такие акты стали невозможны в дальнейшем. «Законодатели обычно не реагируют на вещи без человеческих потерь или предсказания таких потерь – они не хотят слышать об этом. Они хотят видеть человеческие потери. Недостаточно пощупать дверь и ощутить, что она горячая; вам надо дождаться дыма из-под нее... На пороге нового тысячелетия риск от такого образа мышления громаден». Вместо того чтобы дожидаться массовой гибели людей и последующей за ней атаки конгресса на гражданские свободы, говорит Колстром, Соединенные Штаты должны уже сегодня начать готовиться к самому невероятному.

¹⁹³ William Scally, «Man Charged Following White House Attack», Reuters Newswire, 30 октября 1994 года.

¹⁹⁴ William Neikirk and Christopher Drew, «Small Plane Crashes on White House Lawn, Pilot Dies», *Chicago Tribune*, 12 сентября 1994 года.

Бесконтрольное ядерное оружие

Ядерный терроризм, похоже, самая страшная угроза мировой безопасности. Насколько серьезно мы должны быть ею озабочены?

При беглом взгляде на проблему большинство людей считает, что ядерная бомба могла бы быть идеальным оружием террористов. Ядерная бомба размером с небольшой кейс может мгновенно испарить огромную часть большого города. Бомбы могут быть легко доставлены в большинство городов на лодке, грузовике или легком самолете. небоскребы могут быть использованы в качестве дешевого способа осуществления воздушного взрыва, максимально увеличив радиус поражения. Более того, ядерные устройства могут управляться дистанционно или быть оформлены в виде мины-ловушки, попытка обезвредить которую приведет к взрыву.

Но фактически ядерная бомба вряд ли станет популярным оружием доморощенных террористов. Ядерное оружие очень сложно в сборке, для него требуется большое количество обогащенного оружейного ядерного сырья, такого как уран-235 или плутоний-239. Лишь наиболее развитые страны смогли создать и испытать свои собственные устройства. Таким образом, вряд ли террористические организации будут пытаться создать свое ядерное оружие.

Поэтому велика вероятность похищения ядерного устройства, получения его от покровительствующего государства или приобретения на черном рынке. К счастью, насколько нам известно, ядерное оружие по-прежнему охраняется на высочайшем уровне. Более того, многие бомбы оснащены компьютерными системами блокировки, предотвращающими детонацию без соответствующей авторизации. Важность контроля над атомным оружием настолько очевидна, что сомнительно, чтобы оно могло попасть в руки террористов.

Хотя массовая культура заиклется о риске, который представляют взрывные ядерные устройства, гораздо более серьезная угроза – распыление террористами радиоактивных материалов. По сравнению с ядерным оружием, уровень контроля над этими материалами поразительно низок. Получить эти материалы можно из самых разных источников: радиоактивных отходов, лабораторного и медицинского оборудования и даже промышленных генераторов радиации – большинство этих источников охраняется плохо. И эти материалы сами по себе являются мощным оружием в руках террористов, гарантируя рак каждому, кто подвергся их воздействию в достаточной степени.

Использование террористами плутония как средства радиоактивного заражения имеет множество преимуществ перед использованием его в бомбе. Террорист может использовать ядерную бомбу только один раз, но тот же самый террорист может разделить плутониевый заряд на несколько частей и использовать каждый из них по отдельности. Террористическая организация не пожалеет усилий, убеждая политических лидеров и прессу в том, что именно она установила ядерный заряд в Нью-Йорке, и это не блеф. С другой стороны, та же самая террористическая организация может соскоблить несколько миллиграмм плутония, запечатать его в пластик и выслать для анализа ABC News.

Другая проблема с использованием ядерной бомбы в террористических целях заключается в том, что эти устройства уничтожают большое количество людей на огромной территории. Кто будет капитулировать перед террористической организацией, взорвавшей Хартфорт, штат Коннектикут? С другой стороны, террористическая организация, неделю за неделей выпускающая небольшое количество радиоактивного плутония на ключевых станциях метро, в конечном счете добьется того, что кое-кто будет воспринимать ее требования серьезно. В ближайшие годы радиологический терроризм будет представлять гораздо более серьезную угрозу, чем терроризм при помощи ядерного оружия. К счастью, даже эту угрозу можно контролировать.

Если террористы готовы умереть за свое дело, то поставщики материалов боятся быть отравленными. Более того, радиация сама по себе как сигнальный маячок может вывести

соответствующие структуры на логово террористов. The Sandia National Laboratories разработала серию переносных гамма- и нейтронного детекторов, сконструированных для Службы аварийного поиска ядерных материалов Министерства энергетики [Department of Energy's Nuclear Emergency Search Team, NEST]. Террорист, пригрозивший распылить несколько граммов плутония, очень скоро может оказаться обнаруженным.

Текущая политика разоружения игнорирует риск радиологического терроризма, не выделяя средств на безопасное уничтожение ядерных материалов из снимаемых с боевого дежурства российских боеголовок. Говорит политолог Берес:

Мы снижаем риск международной ядерной войны, но повышаем риск ядерного терроризма, не выделяя средств на безопасное хранение и уничтожение получающихся материалов. Доведенные до нищеты ученые-ядерщики продают [ядерные] материалы...Безопасность человечества зависит от бедных российских ученых, не имеющих денег на покупку холодильника. Дешевле было бы купить им холодильник.¹⁹⁵

Во многих странах мира, включая Соединенные Штаты, террористам даже не нужно доставать ядерные материалы, чтобы заниматься ядерным терроризмом. Все, что им нужно для создания бомбы, — это атомная электростанция. Большинство атомных станций строилось в те времена, когда обычное оружие не могло повредить герметичную бетонную оболочку реактора толщиной 1,5–3 метра. В результате реакторы защищены от ядерных атак или внутреннего саботажа, но не против разработанных в последние годы образцов обычного мобильного бронебойного вооружения повышенной мощности. В своей книге «Атомные электростанции как оружие врага: непризнанная военная угроза» [*Nuclear Power Plants as Weapons for the Enemy: An Unrecognized Military Peril*] Бенет Рамберг [Bennett Ramberg] отмечает, что обычная бомба мощностью в 1 тонну пробивает бетон толщиной более 5,5 метров и сталь толщиной до 40 сантиметров. «Тяжелые направленные заряды еще более эффективны», — замечает он.¹⁹⁶ Разрушенная при помощи обычного вооружения типичная атомная станция может заразить площадь в 10 тысяч квадратных километров.

Природа ядерной угрозы такова, что усилия по глобальному антитеррористическому мониторингу будут более эффективны, если мы будем осуществлять мониторинг потенциальных источников радиоактивных материалов вместо мониторинга потенциальных террористов. В конце концов мы знаем, где находятся ядерные материалы, но мы не знаем, кто может оказаться террористом. Мониторинг материалов дешевле и создает меньше проблем по отношению к гражданским свободам.

Химико-биологический терроризм

Семнадцатого сентября 1984 года управление здравоохранения Васко-Шерман в Орегоне начало получать сообщения о заболевших с симптомами в виде жара, озноба, головной боли, тошноты, рвоты, болей в области живота и кровавого стула. Все эти люди поели в одном из двух ресторанов в Даллесе, штат Орегон. Врачи провели анализ стула и определили, что все пациенты пострадали от вспышки *Salmonella Typhimurium*. Вспышка коснулась более чем 38 ресторанов, заболел 751 человек, 45 из них были госпитализированы.

Проводившие расследование специалисты не могли объяснить причину отравлений. Между случаями отравления не было явной корреляции, кроме того факта, что многие люди ели овощные блюда в закусочных. В одном ресторане пострадали все, кто использовал для салата заправку из голубого сыра; в другом — это был соус «франчо». В одном из отравленных

¹⁹⁵ Лекция Береса, май 1997 года.

¹⁹⁶ Ramberg, *Nuclear Power Plants as Weapons for the Enemy*.

ресторанов было организовано два частных банкета – оба с салатным баром, и никто из их участников не пострадал. Другие люди, заразившиеся сальмонеллой, лишь выпили кофе.

Результаты лабораторных анализов стула были странными. Все бактерии обладали одинаковыми и необычными характеристиками. Например, штаммы в образцах не ферментировали сахар-алкогольный дульцитол, хотя 98 % сальмонелл при традиционном сальмонеллезе ферментируют дульцитол. Еще больше сбивало с толку то, что все сальмонеллы, обнаруженные у жертв, имели идентичные плазмиды и антибиограммные структуры; однако во время проведенного в 1979 и 1980 годах исследования 233 штаммов *Salmonella Typhimurium* не было обнаружено бактерий с подобными характеристиками.

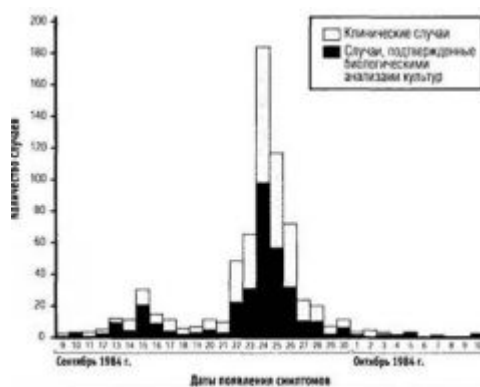
У правоохранительных органов сразу же возникло подозрение в искусственном происхождении вспышки заболевания. Но они не могли понять, кто и зачем мог это сделать, – не было ясного мотива. Главным подозреваемым стало сообщество последователей Бхагвана Шри Раджниша [Bhagwan Sri Rajneesh], основавшее город Раджнишпурам в предместьях Даллеса и почти сразу вступившие в конфликт с коренными жителями. Естественно, основатели Раджнишпурама были вызваны в суд, и органы местного самоуправления запретили группе дальнейшее строительство. В ответ на это сектанты выдвинули своих кандидатов в органы местного самоуправления на ноябрьских выборах 1984 года. Во время выборной кампании были отмечены многочисленные нарушения.

В процессе расследования было обнаружено важное доказательство связи группы из Раджнишпурама с отравлением: медицинская лаборатория коммуны заказала пробирку с *Salmonella Typhimurium* в Американском хранилище биологических культур [American Type Culture Collection] в Роквилле, штат Мэриленд, фирме-поставщике биомедицинских компонентов. В 1985 году следователи ФБР и штата Орегон провели обыск в клинической лаборатории Раджнишпурама. Там они обнаружили открытую пробирку с *Salmonella Typhimurium*. Лабораторные исследования бактерий из этой пробирки показали их полную идентичность штаммам, выявленным во время вспышки заболевания в 1984 году. Очевидно, медицинская лаборатория коммуны культивировала бактерии в больших количествах, члены группы принесли их в рестораны и незаметно добавили в заправки для салатов и сливки для кофе.

Биотеррористическая атака в Орегоне

Надписи: вертикальная ось – количество случаев; горизонтальная ось – даты появления симптомов; расшифровка, серый квадрат – клинические случаи, черный квадрат – случаи, подтвержденные биологическими анализами культур.

На этом графике изображено протекание крупнейшего одиночного акта биологического терроризма на территории США. В период с 9 сентября по 20 октября 1984 года – более 750 человек, инфицированных бактериями сальмонеллы, обратились в клиники и госпиталь Даллеса, штат Орегон. Все эти люди были умышленно заражены религиозным сообществом, производившим биологическое оружие. Сообщество планировало использовать это оружие на ближайших выборах. Члены группы, которые постарались избежать заражения, должны были оказать решающее воздействие на исход выборов. [Рисунок выполнен Крисом Рейли из Reilley Design]



В конечном счете осведомитель помог составить целостную картину этой истории. По его словам, сентябрьское отравление было тестовым испытанием части предвыборного плана группы. Конечной целью было добиться того, чтобы в день выборов больными оказалось такое количество людей, чтобы кандидаты от секты могли победить. Сентябрьская атака была экспериментом по определению необходимого количества бактерий. Предыдущие тесты, произведенные в августе, были неудачными.

Прямые улики и показания свидетелей позволили 19 марта 1986 года предъявить обвинения в отравлении продуктов двум членам сообщества. Обвиняемые были осуждены в апреле 1986 года и приговорены к четырем с половиной годам тюремного заключения каждый. Один из осужденных, глава группы последователей Раджниша Ма Ананд Шила [Ma Anand Sheela] после отбывания двух с половиной лет наказания была освобождена и депортирована в Европу.

Отравление более 700 американцев религиозной сектой должно было стать событием, достойным освещения в печати. Однако следователи Центра по контролю заболеваний (CDC) решили не предавать случай огласке из опасения, что это может инспирировать повторные отравления, как это было с серией отравлений подмешанным к тайленолу цианидом в 1982 году. «Отчет о полученных в ходе расследования CDC сведениях был направлен территориальным органам здравоохранения, но не предназначался для публикации», – говорится в опубликованной 6 августа 1997 года в *Journal of the American Medical Association* статье. Инцидент практически не привлек внимания национальной прессы. Авторы решили обнародовать информацию об отравлении лишь после случая отравления людей нервно-паралитическим газом в Японии в 1995 году. Они надеялись, что сегодня более широкое распространение информации об эпидемиологической вспышке в Даллесе приведет к более глубокому осознанию возможности подобных инцидентов и раннему их распознаванию, если они произойдут, говорят авторы статьи.¹⁹⁷

Ученые Раджнишпурама были не единственными людьми, которые заказывали по почте потенциально смертоносные микроорганизмы. 5 мая 1995 года лаборант из Огайо по имени Ларри Харрис [Larry Harris] заказал в том же Американском хранилище биологических культур образцы бубонной чумы. Компания не знала, что Харрис является членом организации, проповедующей превосходство белой расы, направившим запрос на поддельном бланке; она лишь проверила его кредитную карту, но не полномочия. И пробирка, скорее всего, была бы выслана, не прояви Харрис нетерпения: через четыре дня после отправки заявки он позвонил, чтобы узнать, почему заказ выполняется так долго. Внезапные подозрения заставили компанию обратиться в федеральные органы. Харрис был признан виновным в совершении почтового мошенничества в ноябре 1995 года.

Инцидент с Харрисом привлек внимание нации. На следующий год конгресс дополнил антитеррористический закон 1996 года [Antiterrorism Law 1996] положениями, требующими от Центра по контролю заболеваний тщательно контролировать отгрузку инфекционных

¹⁹⁷ Torok et al., «A large Community Outbreak of Salmonellosis Caused by International Contamination of Restaurant Salad Bars», *Journal of the American Medical Association*, 278:5 (1997), p. 389.

агентов. Другими словами, CDC стал присматривать за Американским хранилищем биологических культур. Но ученые, высказавшие свое мнение о вспышке сальмонеллеза в Орегоне, не считают, что такого рода законодательные ограничения могут эффективно предотвращать акты биологического терроризма:

Могут ли быть предупреждены другие вспышки, подобные произошедшей в Даллесе? Вряд ли какое-либо регулирование коммерчески доступных патогенов сможет предотвратить вспышку. Нет никакой необходимости приобретать их, поскольку эти культуры могут быть легко получены в инфекционных отделениях больниц или из сырых продуктов животного происхождения, доступных в любом гастрономе. Производство бактерий в больших количествах недорого, не требует сложного оборудования и навыков. Стандартный подход к организации работы закусочных не может предотвратить аналогичных случаев с сальмонеллой или другими патогенами в будущем. Как и во многих других областях нашего открытого общества, общепринятые обычаи неадекватны для предотвращения умышленного заражения продуктов клиентами.¹⁹⁸

Биологические агенты несут в себе фундаментальную опасность для общества. Леонард Коул пишет в декабрьском выпуске 1996 года *Scientific American*: «Химические агенты безжизненны, но бактерии, вирусы и другие живые агенты могут быть заразными и самовоспроизводящимися. Будучи помещенными в определенную среду, они могут размножаться. В отличие от других видов оружия, их опасность со временем возрастает».¹⁹⁹ И заражение может продолжаться длительное время, отмечает он: «Остров Грайнард [Gruinar Island], расположенный недалеко от побережья Шотландии, оставался зараженным спорами сибирской язвы в течение 40 лет, после того как в 40-е годы на нем было произведено испытание биологического оружия».

В научно-фантастическом триллере «Двенадцать обезьян» (кинокомпания Universal Pictures, 1996) режиссер Терри Гиллиам [Terry Guillian] рассказывает историю биотеррориста, похитившего смертоносный вирус из лаборатории генной инженерии в Филадельфии и распространившего его в стратегически важных городах по всему миру. Результат: 90 % человечества вымерло. Те же, кто остался, «жили под землей, как животные», – говорит Коул, главный герой фильма в исполнении Брюса Уиллиса. Его послали из 2020 года назад в прошлое, на еще незараженную землю, чтобы добыть образец исходного вируса, необходимого для создания противоядия.

Если отвлечься от путешествий во времени, то идея фильма чрезвычайно проста. Инфекционное заболевание может охватить планету, уничтожив людей и оставив одни лишь растения и животных. В истории уже были прецеденты.

В 1633 году эпидемия оспы поразила коренных жителей Америки, проживавших в Новой Англии. Джеймс Лойвин [James W. Loewen] в своей книге *Lies My Teacher Told Me* приводит убедительный факт: во времена Колумба на американском континенте проживало от 10 до 20 миллионов человек; более 95 % из них погибло от болезни. Утверждается, что многие смерти были не случайностью, а результатом того, что колонисты давали индейцам одеяла и другие вещи, которыми пользовались умершие от оспы. «Целые города оказались вымершими», – читаем мы в отчете 1829 года, цитирующем более ранний источник. «Живые были не в состоянии похоронить умерших, и останки оставались лежать непогребенными еще годы спустя. Среди индейцев Массачусетса количество воинов сократилось с 30 000 до 300».²⁰⁰

¹⁹⁸ Ibid.

¹⁹⁹ Leonard A. Cole, «The Specter of Biological Weapons», *Scientific American*, декабрь 1996. Доступно в Интернете по адресу: <http://www.sciam.com/1296issue/1296cole.html>.

²⁰⁰ J. W. Barber, *Intresting Events in the History of the United States* (New Haven: Barber, 1829), цитируется по: James W. Loewen, *Lies My Teacher Told Me* (Simon & Schuster, 1995).

Как видим, практически невозможно предотвратить будущие биологические атаки на территории США: просто существует слишком много способов получения и применения биологических агентов. Тот факт, что в США и в остальном мире не происходит большого количества биологических атак, означает лишь то, что их угроза преувеличивается. В любом случае их последствия могут быть самыми драматическими, поэтому мы должны быть готовы к ним.

Информационные войны

Вернемся в штаб-квартиру ФБР в Нью-Йорке. Чего больше всего опасался Джеймс Колстром, так это не угрозы биологического или ядерного терроризма, а атак через компьютерные сети, направленных на нарушение работы компьютеров банков, госпиталей, транспорта и других важных для нашего общества систем. Говорит Колстром:

Мы используем самые эффективные технологические достижения компьютерной эры для управления такими каждодневными вещами, как светофоры, системы службы спасения 911, системы управления зданиями, коммуникационными сетями и энергосистемами. Даже система водоснабжения управляется компьютерами. Мы все дальше движемся в этом направлении. В старые времена... Форт Нокс^[p59] был символом того, как надо защищать самое ценное: мы помещали ценности в здание с толстыми бетонными стенами. Мы ставили вооруженную охрану у дверей со сложной системой замков и задвижек. Мы могли даже построить ров и посадить в него крокодилов...Сегодня никого не удивляет, если какой-нибудь подросток проникает внутрь по телефонным линиям и крадет эти ценные вещи. И правительство, и частный сектор оказались не готовы к этому.

Компьютеры создают особые проблемы безопасности, поскольку, в отличие от других машин, они являются устройствами общего назначения. Достаточно изменить программу, и поведение компьютера изменится. Атомы, составляющие бетонные стены Форт Нокса не могут быть волшебным образом преобразованы в ядовитый газ, который убьет охрану внутри охраняемой территории, но компьютер, управляющий химическим производством, может быть запрограммирован или перепрограммирован так, чтобы открыть не тот клапан и взорвать завод. Нарушение работы компьютеров уже приводило к подобным взрывам. Насколько нам известно, это были аварии.

Один из участников, проходившей в 1997 году в Берлингейме, штат Калифорния, конференции «Компьютеры, свобода и приватность», сформулировал это так:

«Я обоснованно полагаю, что если я купил пылесос, то он не будет высасывать деньги из моего кошелька и отсылать их производителю пылесоса. Но с компьютерами нет никакой гарантии, что [загруженная из Интернета программа] не утащит деньги из приложения Microsoft Money».

И не перешлет их по сети кому-то другому. Эта проблема усугубляется требованиями бизнеса и пользователей компьютеров по созданию новых возможностей и постоянно улучшающейся связью с внешним миром – даже если эти возможности и связь могут быть использованы хорошо осведомленным злоумышленником.

p59

Fort Knox – бывшая военная база, находящаяся в штате Кентукки, неподалеку от города Луисвилля. В 1935 году Министерство финансов США организовало здесь хранилище золотого запаса. В военное время здесь также хранились Конституция США и Декларация независимости.

Большинство лидеров бизнеса, говорит Колстром, похоже, совершенно не готовы к тому, чтобы даже осознать проблему. Колстром считает, что американские компании создали двухъярусную систему, в которой высшее руководство «вообще технически неграмотно», а молодые служащие очень хорошо разбираются в технологиях, но не очень хорошо знают саму компанию, ее цели, ее историю или ее обязанности. В результате «вы имеете иерархию людей, не знающих, что происходит, и делегирующих огромную власть и ответственность людям, не имеющим опыта, людям, ставящим „я“ выше „мы“».

Сюжеты в прессе и на телевидении зачастую восхваляют подростков, которые могут относительно легко взломать важные банковские, медицинские или военные компьютеры. Но даже если пресса не так уж и благосклонна, угроза наказания мало страшит их.

В апреле 1996 года генеральный прокурор Джанет Рино объявила, что ФБР впервые осуществило перехват информации в Интернете [Internet wiretap]. Злоумышленник проник в компьютеры Гарвардского университета и использовал их для взлома систем Исследовательской лаборатории армии США и Военно-морской исследовательской лаборатории, после чего использовал их возможности для атак на другие машины. В конечном счете злоумышленник взломал множество военных и коммерческих систем от Калифорнии до Южной Кореи и Гавайев. След привел в Аргентину к старшекласснику по имени Хулио Сесар Ардита [Julio Cesar Ardita]. Расследование остановилось на этом, так как Аргентина не выдала юного злоумышленника, поскольку он не нарушил законов своей страны. (В декабре 1997 года Ардита был выдан и признан виновным; он был приговорен к штрафу в размере 5 тысяч долларов США и получил три года условно.²⁰¹)

В другом случае психически неуравновешенный юнец, действовавший под псевдонимом Phantom Dialer, [\[p60\]](#) постоянно взламывал компьютеры в университетах, крупных корпорациях, банках, правительственных агентствах и даже совершенно секретных учреждениях по разработке ядерного оружия. Хотя он и был в конечном счете задержан ФБР, официальные лица решили не предъявлять обвинений, поскольку считали, что ни один суд присяжных не признает его виновным.²⁰²

А что, если в следующий раз, когда Соединенные Штаты ввяжутся в непопулярную войну, шестеро аспирантов Вашингтонского университета, несогласные с целями войны, заставят вооруженные силы США остановиться при помощи Интернета? Или подросток, чью мать уволили из банка, решит собственноручно отомстить и сотрет информацию, хранящуюся в банковских компьютерах? Современные технологии дают огромную власть в руки тех, кто не может разумно ею распорядиться. Эффект неизменно будет дестабилизирующим.

Преступные мысли

В течение многих лет борцы за гражданские свободы протестовали против попыток ФБР расширить свое влияние, мотивируя это тем, что вся история ФБР доказывает, что этой организации нельзя доверять в вопросах уважения конституционных прав людей.

Утверждения, что ФБР составляет списки неблагонадежных лиц и разведывательных групп, вызывают огромное беспокойство борцов за гражданские свободы, знакомых с длительной историей систематического преследования ФБР и американским правительством

²⁰¹ «Argentine Computer Hacker Agrees to Surrender», Associated Press, 6 декабря 1997. Доступно в архиве по адресу http://www.techserver.com/newsroom/ntn/info/120697/info_7_5811_noframes.html.

p60

Звонильщик-призрак (англ.).

²⁰² David H. Freedman and Charles C. Mann, *At Large: The Strange Case of the World's Biggest Internet Invasion* (New York: Simon & Schuster, 1997).

людей, придерживающихся непопулярных политических взглядов или относящихся к национальным меньшинствам. Зачастую эти злоупотребления происходили под предлогом обеспечения национальной безопасности в военное время. В те времена граждане страны, законодатели, исполнительная власть и судебная система объединялись для создания атмосферы страха, ненависти и нетерпимости. Чтобы понять беспокойство людей за будущее, достаточно совершить краткий экскурс в прошлое.

История современного полицейского государства восходит к временам Первой мировой войны. До войны небольшие нарушения гражданских свобод были широко распространены, но с ними мирились, пишет историк Пол Мерфи [Paul Murphy], автор книги «Первая мировая война и истоки гражданских свобод» [*World War I and the Origin of Civil Liberties*]. Но эти нарушения никогда не были организованными в масштабах нации.

В начале Первой мировой войны Бюро расследований США (предшественник ФБР) располагало всего лишь сотней агентов. У Бюро не было возможности вовремя увеличить штаты для деятельности в военное время. Напуганный возможностью саботажа и диверсий на территории США, рекламист из Чикаго Альберт Бриггс [Albert M. Briggs] создал в помощь бюро Американскую лигу защиты [American Protective League]:

К середине июня 1917 года лига имела отделения более чем в 600 населенных пунктах, число ее членов составляло около 100 тысяч человек. На пике число членов достигло 250 тысяч. Член лиги платил 1 доллар и получал значок, на котором сначала было написано «Подразделение Секретной службы», а затем (после того как Министерство финансов воспротивилось, во избежание путаницы со своей Секретной службой) – «Помощник Министерства юстиции США». Штаб-квартира Американской лиги защиты располагалась в Вашингтоне, федеральный округ Колумбия; лига действовала от лица Министерства юстиции так, как будто ее члены были формальными помощниками этого ведомства. Результат был пугающим для многих. Не имея данных законом полномочий производить аресты, сотрудники лиги участвовали в расследованиях по проверке лояльности граждан, в работе призывных комиссий, установлению действительного статуса лиц, отказывающихся от военной службы по религиозным или политическим мотивам, в отслеживании тысяч сообщений о подозрительной деятельности, поступающих от людей со всей страны в ответ на призыв к бдительности, выявлению шпионов и лиц, виновных в саботаже. Члены лиги проявили такую энергичность в своем крестовом походе против нелояльности, что Министерство юстиции в конечном счете ограничило деятельность агентов лиги.²⁰³

Американская лига защиты была всего лишь одной из множества полуофициальных организаций, зародившихся во время войны. Среди них были «Лига защиты отечества» [Home Defense League], «Мальчики-разведчики Америки» [Boy Spies of America], «Критики мятежа» [Sedition Slammers] и «Ужасная угроза» [Terrible Threateners]. Изначально эти организации выявляли и наказывали людей, высказывавшихся против военных действий. Но вскоре они стали преследовать людей, настроенных против любого аспекта американского образа жизни.

По мере продолжения войны правительство США стало использовать войну как предлог для нападков на зарождающееся в стране рабочее движение. Наиболее грязными были нападки на организацию «Промышленные рабочие мира» [Industrial Workers of the World, IWW], известную также под названием «шатающиеся» [Wobblies]:

В ответ на раздувание истерии относительно Wobblies, Генеральный прокурор Грегори смотрел сквозь пальцы на массовые преследования лидеров организации. Местные отделения IWW обыскивались, зачастую без ордера на обыск, агенты Бюро расследований пытались что-нибудь обнаружить в их книгах, счетах, письмах и бумагах. Грегори редко делал различие между людьми, поддерживающими теорию и идеологию IWW, и членами организации,

²⁰³ Murphy, *World War I and the Origin of Civil Liberties*, p. 90.

совершившими преступления, предусмотренные федеральным законом. Министерство юстиции также предостерегало лиц, склонных к поддержке IWW или обращению в суды справедливости, от защиты «так называемых „гражданских свобод“... „народных советов“, „юридических консультаций“ или антивоенных организаций», намекая, что эти группы являются частью вражеского заговора по воспрепятствованию продолжению войны.²⁰⁴

Министр почтового ведомства США Берльсон [A. S. Burleson] совершил своеобразную месть против IWW. Берльсон заблокировал доставку почты IWW, заявив, что она является подрывной. Когда социалистическое издание *Milwaukee Leader* опубликовало объявление о сборе средств для защиты IWW, почтовое ведомство лишило *Leader* почтовых привилегий второго класса.

Leader подало в суд на министра. В конечном счете дело было рассмотрено в Верховном суде, который поддержал цензуру Берльсона в деле «Milwaukee Publishing Co. против Берльсона». ²⁰⁵ Частично в этой истерии повинно правительство США, популяризовавшее войну среди населения. Правительственный Комитет общественной информации [Committee on Public Information] подготовил чрезвычайный президентский указ, который распространялся в школах и колледжах, объяснявший, почему Америка участвует в войне.

Эти буклеты включали «доказательства» масштабной нелояльности в Соединенных Штатах и «доказательства» того, что немцы постоянно совершают немыслимые по своей жестокости поступки... Другие брошюры были откровенно антигерманской направленности, зачастую содержащими лживые сведения об упадке немецкой культуры, немецких ценностей и образа жизни. Утверждалось, что за большинством забастовок в Соединенных Штатах стоят немецкие агенты, Германия финансирует пацифистские газеты, агенты Германии всеми силами стремятся навязать американскому народу самые худшие традиции пруссачества. Эти документы распространяли мнение о том, что американцы немецкого происхождения якобы нелояльны, а пацифисты поддерживают Германию. Поставив под сомнение лояльность этих людей, пропаганда делала их объектом враждебных действий и преследований со стороны множества групп и отдельных людей.²⁰⁶

Опасности военного времени часто используются для оправдания старых предрассудков. В начале Второй мировой войны Соединенные Штаты интернировали более 100 тысяч японцев, 79 тысяч из которых родились в Америке. Подробные списки американцев японского происхождения с указанием адресов были представлены военному ведомству^[p61] Бюро переписи населения без постановления суда, несмотря на то что в соответствии с законом данные переписи должны оставаться конфиденциальными в течение 99 лет. Но это отнюдь не было началом антияпонских настроений в американской культуре, а всего лишь их высшей точкой. Американское правосудие узаконивало дискриминацию японцев более ста лет. Законы были поддержаны Верховным судом США, постановившим в 1922 году в деле «Озава против Соединенных Штатов» [*Ozawa v. United States*], что японцы

²⁰⁴ *New York World*, 28 января 1918, p. 1–2; *New York Times*, 18 июня 1919, p. 8; см.: Murphy, *World War I and the Origin of Civil Liberties*, p. 95.

²⁰⁵ *Milwaukee Publishing Co. v. Burleson*, 255 U.S. 407 (1921).

²⁰⁶ Murphy, *World War I and the Origin of Civil Liberties*, p. 109–110.

p61

Военное ведомство [War Department] – предшественник Министерства обороны. Существовало с 1789 по 1947 год, когда было преобразовано в Национальное военное ведомство [National Military Establishment], а в 1949 году – в современное Министерство обороны [Department of Defense].

и другие азиаты не подлежат натурализации из-за расовой принадлежности. Аналогичным образом Верховный суд поддержал интернирование японских граждан во время Второй мировой войны, несмотря на то что подавляющее большинство не совершило ничего противоправного.

В 50-х годах XX века директор ФБР Эдгар Гувер использовал всю разведывательную мощь своего ведомства против подозреваемых в принадлежности к коммунистам и гомосексуалистам во властных структурах по всем Соединенным Штатам. В 1960-е и 1970-е годы Бюро выслеживало студенческие организации в университетских городках. ФБР вело слежку и внедрялось в различные группы – женские, чернокожих, защитников окружающей среды и геев. Все эти действия предпринимались якобы с целью обеспечения безопасности американцев и борьбы с внутренним терроризмом.

Проблема не в том, что ФБР и другие организации не нуждаются в законном расширении своих полномочий для борьбы с новыми угрозами. Проблема в том, что и ФБР, и страна в целом показали свою готовность быть втянутыми в решение злободневных проблем и несправедливо обвинять, преследовать и заключать в тюрьму людей лишь за то, что они говорят и во что верят, а не за конкретные действия. После этого очень сложно доверять заявлениям ФБР, что все суперсовременные технологии и полномочия необходимы для выслеживания и ареста террористов и убийц. Какие гарантии может дать Бюро, что в будущем оно не будет злоупотреблять своим могуществом и властью, как это было в прошлом?

Перехват

Одним из наиболее мощных средств в борьбе с преступлениями, диверсиями и мятежами является возможность перехватывать письменные и устные коммуникации. Именно эту привилегию ФБР отстаивает особенно рьяно.

Перехват давно известен в американской истории. В 1624 году комендант новоиспеченной колонии в Плимуте – Бредфорд [Bradford], провожая корабль, отправляющийся в Англию, взшел на борт и вскрыл письма, которые премьер-министр колонии направил своему коллеге в Англию.²⁰⁷ Он вернулся с письмами и предъявил их многоуважаемому мистеру Лайфорду [Lyford] на городском собрании. Лайфорд хранил молчание, но его сообщник Олдхем [Oldham] попытался поднять мятеж, заявив, что Бредфорд не может больше оставаться правителем, поскольку вскрыл частные письма, но Бредфорд ответил, что он вскрыл письма правомерно, дабы «предотвратить вред и разрушения, которые этот заговор и интриги могли принести несчастной колонии».

Дэвид Флаэрти [David Flaherty] в тезисах своей диссертации, посвященной вопросам приватности в предколониальной Америке, пишет:

Этот эпизод подчеркивает колониальное отношение к вскрытию чужих писем. В смутное время раннего становления и во время кризиса комендант вынужден был объяснять, зачем он вскрыл чужие письма. Он считал, что в этих условиях безопасность превышает приватности. Этот комендант из Новой Англии XVII века чувствовал даже некий элемент неуверенности в корректности своих действий, поскольку люди предполагали, что почта должна быть приватной.²⁰⁸

²⁰⁷ Полное описание эпизода см.: Bradford, *Of Plymouth Plantation* (New York: Random House, 1952), p. 149–53.

²⁰⁸ Flaherty, *Privacy in Colonial New England*, p. 125–126. Указанные Флаэрти источники информации включают: Kenneth Ellis, *The Post Office in the Eighteenth Century: A Study in Administrative History* (London, New York: Oxford University Press, 1958), p. 60–77; William Cobbett, *Cobbett's Parliamentary History of England* (London: R. Bagshaw, 1806–1820), IX (1733–1737), p. 839–848.

Возможность тайно вскрывать почту очень привлекательна, – привлекательна настолько, что очень быстро провоцирует злоупотребления. Как пишет Флаэрти, английский «Закон о почтовой службе» [Post Office Act] 1710 года запрещал вскрытие чьей-либо почты, «за исключением случаев особого собственноручного письменного разрешения одного из основных министров на каждое вскрытие». С такими ограниченными позволениями на перлюстрацию почты Англия создала Тайную службу, сотрудники которой были настолько опытные, что могли вскрыть письмо, не оставив никаких следов вмешательства. Но к 1735 году члены парламента стали жаловаться, что их почта постоянно вскрывается. Фактически, они заявили на парламентских слушаниях, что Тайная служба вскрывает так много писем, что любой, кому есть что скрывать, не станет пользоваться почтовой службой. Таким образом, «свобода на вскрытие писем в почтовых отделениях не приносит более результатов, но позволяет мелким клеркам в офисе совать нос в личные дела любого купца или дворянина в королевстве».

Перехват неизменно сопровождал электронным коммуникациям с самого их зарождения. Вскоре после изобретения в 1845 году Самюэлем Морзе телеграфа люди стали беспокоиться о конфиденциальности передаваемых с помощью этого устройства сообщений. Во время Гражданской войны между Севером и Югом войска обеих сторон перехватывали телеграфные сообщения, передаваемые по линиям связи врага, получая таким образом информацию о передвижении войск и их численности. После войны многие штаты занимались перехватом. Федеральное правительство приняло первый закон на эту тему в 1918 году; он допускал использование технических средств перехвата в качестве контрразведывательного средства. Однако перехват оказался настолько эффективным, что правоохранительные органы продолжали использовать его и после войны, для борьбы с подпольными торговцами спиртным и обуздания разгулявшейся преступности во времена «сухого закона».

В последующие годы федеральное правительство продолжало использовать перехват и другие формы электронного наблюдения. В 1950-е годы агенты ФБР использовали микрофоны для прослушивания домов, офисов и квартир в тайне от их обитателей – и без постановления суда. Верховный суд США одобрил эту практику в 1954 году, вынеся определение по делу «Ирвайн против штата Калифорния» [*Irvine v. California*²⁰⁹], в котором говорилось, что, поскольку разговор не является вещественной собственностью и федеральные агенты не вторгались на территорию офиса подозреваемого, закон не был нарушен.

Суд изменил свое мнение на прямо противоположное в 1961 году, постановив в деле «Сильверман против Соединенных Штатов» [*Silverman v. United States*²¹⁰], что использовать информацию, полученную с подслушивающих устройств, недопустимо. В 1967 году в деле «Кац против Соединенных Штатов» [*Katz v. United States*²¹¹] суд постановил, что общественные телефонные будки не могут ставиться на прослушивание без ордера. Суд мотивировал это тем, что, поскольку телефоны общего пользования находятся в общественных местах, пользующиеся ими люди резонно рассчитывают на обеспечение приватности.

После этого решения в 1968 году конгресс принял Omnibus Crime Control Act,^[p62]

²⁰⁹ *Irvine v. California*, 347 U.S. 128.

²¹⁰ *Silverman v. United States*, 356 U.S. 505.

²¹¹ *Katz v. United States*, 389 U.S. 347.

p62

Сводный закон о контроле над преступностью, регулирующий различные аспекты этой проблемы.

официально позволивший использовать прослушивание при выполнении определенных процедур.

В последующие годы электронный перехват устных переговоров стал одним из наиболее мощных средств борьбы с преступностью в арсенале правоохранительных ведомств. Перехват выполняет несколько ключевых функций:

- перехват представляет доказательства совершенных в прошлом преступлений;
- перехват позволяет выявить имена сообщников;
- перехват позволяет узнать подробности планируемых незаконных действий.

Тем или иным способом подслушивающие устройства и «электронные жучки» предоставляют правоохранительным органам своеобразное окно в мысли преступника. После ареста записи перехваченных разговоров могут стать бесценным доказательством в суде. Именно поэтому полиция рассматривает подключение к линиям и электронные подслушивающие устройства как свое основное оружие в борьбе с преступностью.

Несмотря на свои внушительные возможности, прослушивание используется в повседневной деятельности правоохранительных органов поразительно вяло. Например, согласно данным, опубликованным в 1999 году Административным управлением судов Соединенных Штатов [Administrative Office of the United States Courts] в специальном отчете *Wiretap Report*, в 1998 году в Соединенных Штатах судьями федеральных судов и судов штатов было выдано всего лишь 1329 разрешений на осуществление прослушивания.²¹² О количестве прослушиваний в целях национальной безопасности на территории США не сообщается.

Перехват приносит свои плоды. В 1998 году благодаря электронному наблюдению было арестовано 3450 человек; в одном случае всего одно прослушивание в процессе расследования по наркотикам в северном округе Огайо позволило арестовать и доказать вину 54 человек. В штате Флорида осуществленное в ходе расследования по наркотикам прослушивание сотовых телефонов позволило арестовать десять человек и вынести три обвинительных приговора. В Шинектади, штат Нью-Йорк, «30-дневное прослушивание, бывшее частью расследования аферы, позволило арестовать восемь человек, пять из которых были признаны виновными».²¹³ *Wiretap Report* отмечает: «Когда обвиняемые слышали свой собственный голос на пленке, это имело сокрушительное воздействие».

Как видно из приведенной ниже таблицы, подавляющее большинство прослушиваний осуществляется в рамках расследований незаконного оборота наркотиков. *Wiretap Report* цитирует одного из участников расследования в Северной Каролине, приведшего в результате к 21 аресту и доказательству вины в 16 случаях:

Без санкционированного прослушивания следствию не удалось бы установить, что деятельность обвиняемых по транспортировке наркотиков связана с интернациональной организацией, несущей ответственность за импорт и распространение сотен килограммов кокаина и кокаинового сырья.²¹⁴

Еще в одном случае осуществленное в Нью-Йорке прослушивание привело к шести обвинительным заключениям и конфискации одного миллиона долларов. Но наркотики являются не единственной целью: в 1996 году прослушивание было с успехом использовано для обезвреживания нигерийской банды, занимающейся мошенничеством с кредитными

²¹² 1999 *Wiretap Report*, Administrative Office of the United States Courts.

²¹³ 1998 *Wiretap Report*, Administrative Office of the United States Courts, p. 11. Доступно в Интернете по адресу <http://www.uscourts.gov/wiretap98/content.html>.

²¹⁴ Ibid.

картами, которая «использовала телефоны для совершения мошенничеств и продажи незаконно добытой информации по кредитным картам по всему миру».²¹⁵

Расследуемое преступление – Количество разрешений на прослушивание – Общее число перехватов, %

Взяточничество – 9 – 1

Аферы – 93 – 7

Убийства и физическое насилие – 53 – 4

Кражи и грабежи – 19 – 1

Ростовщичество и вымогательство – 12 – 1

Наркотики – 955 – 72

Незаконное предпринимательство, открытие подставных фирм – 153 – 12

Другое – 30 – 2

ВСЕГО – 1 329 – 100

Средняя длительность прослушивания составляет 28 дней; если следствие хочет осуществлять прослушивание более 30 дней, необходимо получить специальное разрешение суда. Самое длительное прослушивание в истории США длилось 2073 дня – более пяти лет, продлялось 146 раз. Прослушивание проводилось в рамках следственных мероприятий по организованной преступности в Нью-Йорке. Следующее по длительности прослушивание длилось 600 дней; оно проводилось в рамках расследования преступления, связанного с незаконным оборотом наркотиков в Лос-Анджелесе.

Забавно, но относительно небольшое количество осуществляемых каждый год прослушиваний обеспечивает их высокую эффективность. В отличие от членов парламента, отсылавших письма в Англии XVIII века, очень не многие преступники в Америке XX века полагают, что их телефоны действительно прослушиваются. Если бы прослушивание было более широко распространено при расследовании преступлений, преступники относились бы более внимательно к тому, что они говорят по телефону.

Прослушивание рассматривалось как тайная сторона деятельности правоохранительных органов до начала 90-х годов XX века, когда у ФБР начались проблемы с получением разрешения на прослушивание в крупных мегаполисах. Проблема была не в недостатке средств или людей, но в технологических затруднениях. Первые 60 лет истории телефонии для прослушивания чьего-либо телефона достаточно было повесить пару зажимов-«крокодилов» на телефонные провода. Но когда в начале 1980-х телефонные системы стали цифровыми, правоохранительные органы обнаружили, что их возможность перехватывать разговоры ограничена развитием современных технологий. Особенно остро эта проблема проявилась в сети телефонной сотовой связи Нью-Йорка. Несмотря на то что нешифрованные аналоговые сигналы сотовых телефонов легко можно было поймать ручным сканером, вычленив в этом потоке разговор с конкретного телефона было куда более сложной задачей. Единственным местом, куда можно было подключить подслушивающее устройство, был специальный *технический порт* на коммутаторе системы сотовой связи. Одна из установленных в Нью-Йорке сотовых систем Autoplex 1000 компании AT&T, рассчитанная на обслуживание 150 тысяч абонентов, – имела всего семь технических портов. Полиции зачастую приходилось месяцами ждать возможности воспользоваться разрешением на прослушивание.

Проблемы для ФБР создавали также и более простые технологии. В большинстве случаев прослушивание предполагает установку специального записывающего устройства на телефонную линию подозреваемого. Перенаправление звонков позволяет подозреваемому автоматически перенаправлять звонки на другой телефонный номер в городе, стране или в мире, одновременно избегая прослушивания и меняя юрисдикцию. Цифровые

²¹⁵ 1996 *Wiretap Report*, Administrative Office of the United States Courts.

ISDN-телефоны^[p63] создали еще большую проблему: для подключения к ISDN-линии необходимо специальное оборудование, но, когда разворачивались первые ISDN, в распоряжении правоохранительных органов еще не было такого оборудования. Любой, кто использовал цифровой телефон, получал почти гарантированно неприслушиваемую телефонную линию.

Сначала ФБР пыталось сговориться с производителями телефонного оборудования о встраивании средств, обеспечивающих перехват. Но согласно документу, попавшему в распоряжение Информационного центра электронной приватности [Electronic Privacy Information Center, EPIC], ФБР получило резкий отказ.²¹⁶ Вместо того чтобы просто попытаться восстановить статус-кво, ФБР захотело, чтобы в оборудование встраивались средства удаленного мониторинга, что позволило бы сотрудникам ФБР осуществлять прослушивание телефонов, не привлекая телефонную компанию и не ставя ее в известность. Более того, ФБР хотело, чтобы телекоммуникационные сети проектировались таким образом, чтобы пользователи не могли узнать о прослушивании. И наконец, Бюро хотело, чтобы возможности мониторинга были существенно расширены по сравнению с доступными в настоящее время.

Когда тайные усилия ФБР потерпели неудачу, Бюро предложило законопроект, который обязывал телефонные компании и производителей оборудования удовлетворить его требования. Первоначально названный «Законом о цифровой телефонии» [Digital Telephony Act] и переименованный позднее в «Закон о содействии правоохранительным органам в телекоммуникациях» [Communication Assistance to Law Enforcement Act], документ был принят, несмотря на протесты защитников гражданских свобод, в октябре 1994 года. По различным оценкам, стоимость доработки национальной телефонной системы для возможности прослушивания составила от 300 миллионов до 1 миллиарда долларов.

Передовые технологии прослушивания всего лишь один из способов, которым ФБР надеялось использовать современные коммуникационные технологии в правоохранительных целях. Беспроводные телефонные системы, например, должны постоянно отслеживать местонахождение каждого телефона, чтобы иметь возможность послать сигнал, когда кто-то его вызывает. Для обеспечения расширенного сервиса 911 мобильным телефонам операторы сотовой связи должны устанавливать оборудование, которое обеспечивает точное определение местоположения 60 % телефонов в пределах 100 метров. ФБР хотело бы получить доступ к этим системам, чтобы иметь возможность отслеживать преступников, пользующихся сотовыми телефонами. Аналогичные системы в Европе уже использовались для раскрытия многих преступлений.

Заглянув в будущее, не трудно увидеть, как передовые технологии распознавания в сочетании с технологиями слежения могут быть использованы для построения впечатляющей машины по сбору информации. Сегодня ФБР может поставить подслушивающее устройство на конкретную телефонную линию. В будущем ФБР сможет прослушивать определенных людей – с помощью телефонной системы, автоматически распознающей голоса и записывающей телефонные разговоры, где бы ни находились абоненты. Одним из ключевых доказательств в деле о взрыве здания в Оклахоме была видеозапись, зафиксировавшая подъезжающий взятый на прокат грузовик Ryder. В будущем для ФБР станет возможным соединить сетью все камеры видеонаблюдения в городе, чтобы автоматически обнаруживать и отслеживать подозреваемых в терроризме. ФБР сможет вести поиск информации на всей территории США об отдельных лицах или группах лиц, систематически покупающих компоненты, необходимые для создания бомбы или

p63

ISDN, Integrated Service Digital Network – цифровая сеть с интеграцией услуг.

²¹⁶ Bruce Schneier and David Banisar, eds, *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance* (New York: Wiley, 1997).

биологического оружия, – по записям о покупках.

По отдельности все эти технологии перехвата информации могут выглядеть неплохой идеей. Но если такие агрессивные меры будут приняты, они обойдутся дорого. И если ФБР не сможет выявить новых террористов, замешанных в ядерных, биологических или химических атаках, то законодатели, санкционировавшие затраты, будут побуждать ФБР использовать новые технологии для борьбы с традиционными преступлениями.

Прослушивание мозга

В конечном счете перехват не может остановить все террористические акты, поскольку террористы-одиночки вряд ли будут обсуждать свои планы с другими. Для поимки этих людей требуется еще более агрессивная методика мониторинга: *прослушивание мозга [brain wiretapping]*.

Истории о чтении мыслей уходят вглубь веков, несмотря на то что большинство их в лучшем случае недостоверны. Но что, если чтение мыслей будет значительно усовершенствовано и может быть выполнено в любой момент, по желанию? По слухам, американские военные в 1960 – начале 1980-х годов работали над множеством программ, направленных на то, чтобы превратить миф в реальность. Одна из программ под названием «Звездные врата» [Star Gate] специализировалась на телепатии и выполнялась по контракту SRI International. Согласно многочисленным отчетам, команда SRI обнаружила по крайней мере семь человек, имеющих способность достоверно описать действие, место действия и мысли людей на значительном расстоянии. Но проект был прекращен в 1995 году, после того как был подвергнут насмешкам в ходе расследования комиссией конгресса.²¹⁷

Вообразите, как легко было бы правосудию, если бы полиция могла просто заглянуть в разум подозреваемых. Забудьте о личных капризах судей и присяжных: полиция могла бы мгновенно узнавать, кто преступник, а кто невиновен. Она могла бы очень просто выследить и арестовать заговорщиков.

Полицейские управления были просто очарованы детекторами лжи, или полиграфами, с тех пор как они впервые появились в 1924 году. Детектор лжи записывает электрическую реакцию кожи человека, частоту пульса и дыхания, когда ему задают вопросы. Когда человек лжет, он испытывает стресс или другие сильные переживания, и эти показатели изменяются, иногда очень сильно.

Проблема с детекторами лжи состоит в том, что некоторые подготовленные люди *могут* контролировать свои реакции, большинство же к этому не способно. А некоторые люди непроизвольно испытывают те же самые реакции, когда говорят правду. По словам Дуга Уильямса [Doug Williams], имеющего лицензию для работы на полиграфе и шестилетний опыт работы в подразделении внутренних дел полицейского управления Оклахомы, люди, проходящие тест на детекторе лжи и говорящие правду, «имеют лишь 50 % шанс пройти его успешно». С другой стороны, столько же людей могут пройти тест, говоря неправду. Сегодня Уильямс учит людей, как сделать результаты своего теста положительными и даже написал книгу «Как обмануть тест на детекторе лжи» [*How to Sting the Lie Detector Test*].²¹⁸

Еще одна форма «прослушивания мозга» включает применение наркотиков, блокирующих волю. В шпионских фильмах часто присутствует «сыворотка правды», которая при правильном применении заставляет захваченного разведчика выдать секреты.

²¹⁷ См.: «STAR GATE [Controlled Remote Viewing]», на сайте Федерации американских ученых [Federation of American Scientists], [http:// www.fas.org/irp/program/collect/stargate.htm](http://www.fas.org/irp/program/collect/stargate.htm).

²¹⁸ Doug Williams, *How to Sting the Lie Detector Test* (Chickasha: Sting Publications 1976). Имеется в наличии у фирмы Sting Publications, P.O. Box 1832, Chickasha, OK 73023.

Многие наркотики обладают эффектом сыворотки правды, это хлоралгидрат, некоторые барбитураты, амитал натрия, амибарбитал натрия и даже веселящие наркотики вроде LSD, метилendioксиметамфетамин («экстази») и обычный алкоголь. Но в отличие от шпионов, действующих над законом, полиции запрещено использовать наркотики. Но даже если бы такого запрета и не было, данные препараты дают непредсказуемую реакцию, зачастую продуцируя фантазии вместо правды.

Настоящее прослушивание мозга будет базироваться, конечно, не на мистике, физиологических измерениях или наркотиках. Оно произойдет из попыток сканирования человеческого мозга. В настоящее время существует две системы, которые можно использовать для этой цели: функциональное магнито-резонансное сканирование [Magnetic Resonance Imaging, fMRI] и позитронная томография [Positron Emission Tomography, PET]. Система fMRI настроена на контроль кровообращения. Теория гласит, что, когда клетки мозга работают, им требуется больше кислорода, поэтому кровеносные сосуды вокруг мозговых клеток слегка расширяются. Если провести несколько MRI-сканирований мозга подряд, можно обнаружить расширение кровеносных сосудов. Система PET использует радиоcontrastную глюкозу для определения частей мозга, потребляющих больше энергии.

Задача построения картины мозга тесно связана с его происхождением. В отличие от обычных компьютеров, мозг растет органически. Позиция каждого нейрона не программируется предварительно. Вместо этого по мере роста мозг самообучается. В результате мозг каждого человека слегка отличается от мозга других людей.

В 1993 году в качестве добровольца я участвовал в серии экспериментов по fMRI-сканированию в Massachusetts General Hospital. Целью экспериментов была идентификация областей человеческого мозга, отвечающих за восприятие языка. Для эксперимента меня уложили на спину на пластиковую каталку, голова была зафиксирована при помощи мешочков с песком, после чего меня закатили в машину. Перед моими глазами был помещен небольшой пластиковый экран.

Во время эксперимента на экран проецировались слова и изображения. Пока я смотрел на них, fMRI-сканер снимал изображения моего мозга. Через год после этого исследовательская группа опубликовала документ, рассказывающий, каким образом определенные области мозга связаны с определенными аспектами языка. С тех пор было проведено еще множество исследований с использованием fMRI и PET, продолжающих составление карты отдельных частей мозга.

Составление карты мозга жизненно необходимо для нейрохирургии. Когда пациенту делают операцию по поводу рака мозга, очень важно, чтобы в процессе операции врач не повредил ключевые области, отвечающие за речь, двигательную активность или память. Такая же высокая точность необходима при планировании высоких доз лучевой терапии.

В Медицинском центре Вашингтонского университета проводится другой эксперимент по составлению карты мозга, включающий нейрохирургию. При этом способе составления карты у пациента производится разрез кожи, череп распиливается и открывается, обнажая поверхность мозга. Затем различные участки мозга стимулируются электрическим током, а нейрохирург спрашивает пациента о его ощущениях. После того как каждый функциональный центр мозга идентифицирован, на поверхность мозга помещаются небольшие, около половины дюйма в диаметре, метки, похожие на липкие листочки для записей. Эти метки указывают врачу области, которые нельзя резать. Врачи надеются, что в конечном счете они смогут использовать нетравмирующие технологии, такие как fMRI, которые сегодня недостаточно точны. Группой исследователей в Вашингтонском университете руководит доктор Джордж Ойман [Dr. George Ojemann]; аналогичные работы проводились в университете Джонса Хопкинса доктором Барри Гордоном [Dr. Barry Gordon]. В дальнейшем подобные технологии, сегодня еще недостаточно отработанные, будут совершенствоваться. Одним из движущих факторов будет *интерфейс человек-машина* [man-to-machine interface], который исследователи создают в надежде, что парализованные в результате несчастного случая люди смогут вновь контролировать свою жизнь. Если эти

системы станут достаточно совершенными, они могут полностью исключить необходимость печати на клавиатуре также и для здоровых людей. В конечном счете такие системы смогут распознавать явно сформулированные мысли или даже хранимые воспоминания.

Моральный долг обязывает пытаться

Итак, суть противоречия в следующем: новые технологии создают потрясающие возможности для экстремистских групп, позволяющие нести смерть и разрушения в общество. В то же время новые технологии дают правоохранительным органам возможность вести всестороннее наблюдение за гражданским населением способами, которые раньше невозможно было себе представить. Могут ли правоохранительные органы заниматься широкомасштабным, всеобъемлющим наблюдением, имея дело с постоянно повышающимся риском мегатеррора?

Чарльз Блэк [Charles Black], один из крупнейших специалистов в области гражданских прав в 1950-х и 1960-х годы XX века, на одном из первых занятий по конституционному праву в Йельском университете задавал слушателям вопрос: «Предположим, что вы нью-йоркский полицейский и у вас имеется задержанный, про которого точно известно, что он установил атомную бомбу с таймером, который должен привести ее в действие на следующий день. Правомерно ли подвергнуть его пытке согласно Конституции? Правомерно ли это вообще?»

Один из бывших студентов Блэка, а ныне профессор права в университете Майами Майкл Фрумкин [Michael Froomkin], хорошо помнит эту задачу. «Непременным является тот факт, что пытки явно запрещены Конституцией», – объясняет Фрумкин. Но, несмотря на это, говорит Фрумкин, если бы *он* был этим полицейским, он бы чувствовал моральный долг применить пытки к преступнику, обезвредить бомбу, после чего уволиться и отвечать за содеянное. «Мы говорим о чрезвычайных обстоятельствах, оправдывающих чрезвычайные действия. Во многом это зависит от уровня вашей моральной интуиции».²¹⁹

Пытки – прекрасная точка отсчета, говорит Фрумкин: если пытка морально оправдана, то, несомненно, прослушивание, видеонаблюдение, снятие отпечатков пальцев и другие современные технологии борьбы с преступностью также оправданы. И конечно, некоторые страны *узаконивали* пытки как средство борьбы с терроризмом. Израиль, например, использовал меры физического воздействия на подозреваемых в терроризме с целью раскрытия деталей планируемых террористических актов. Но многие люди, правительства и ООН протестовали против использования Израилем разрешенных на государственном уровне пыток. Аргумент очень простой: пытки уничтожают моральное доверие к тому, кто их использует. Недавно Верховный суд Израиля вынес определение, что пытки являются неприемлемыми по израильским законам, возможно, положив конец этой практике в Израиле.

Обратимся снова к профессору Луису Рене Бересу из университета Пардью, который считает, что правительству США, возможно, необходимо право на осуществление арестов без ордера, всепроникающего мониторинга и даже убийств для предотвращения в особых случаях, например, ядерных атак террористов, – именно в тех случаях, когда информация достоверна, а времени мало. «Если вы знаете, что определенная группа тайно установила [взрывное] устройство, и единственный способ предотвратить его использование связан с выходящими за рамки закона действиями, готовы ли вы санкционировать их?» – спрашивает Берес.

По мнению Береса, ответ на этот вопрос – безоговорочное «да». Гораздо лучше, аргументирует Берес, временно приостановить гарантированную Конституцией защиту, чем позволить миллионам людей умереть. Для тех, кто не согласен с ним, он говорит: «Если вы

²¹⁹ Интервью автору, 14 мая 1997 года.

считаете, что опасность ареста без ордера выше опасности ядерного уничтожения, то это ваше решение...Томас Джефферсон^[p64] не жил в ядерную эпоху. Он не мог предвидеть такой разрушительной силы».

Лучшее решение

К сожалению, массивное всеохватывающее наблюдение хорошо помогает лишь против химического и ядерного терроризма, но эта методика совершенно бесполезна в борьбе против террористов, использующих биологические агенты. Это происходит потому, что опасные бактерии, вирусы и грибки естественным образом существуют в окружающей среде. «Сибирская язва обнаружена по всему юго-западу Америки, – говорит Кэтлин Бейли [Kathleen C. Bailey], бывший помощник директора Агентства по контролю за оружием и разоружением США [US Arms Control and Disarmament Agency]. – Там она называется „болезнь бараньих стригалей“ [Sheep Shearer Disease], поскольку споры сибирской язвы находятся в овечьей шерсти...Каждый год мы имеем 10, 15 или 20 случаев заболевания».²²⁰

Люди, занимающиеся домашним консервированием мяса и овощей, постоянно подвергаются риску заболеть ботулизмом. Работающий в одиночку потенциальный террорист, прослушавший один или два дополнительных курса по микробиологии в колледже, может создать большой арсенал биологического оружия. Все, что будет нужно этому человеку, по словам Бейли, это оборудование на сумму 10 тысяч долларов и подвальная комната площадью чуть больше 1,5 квадратных метров.

«Если кто-то захочет это сделать, вы не сможете остановить его, – говорит доктор Бейли. – Если это террористическая группа, вы можете выследить ее. Но если это одиночка, очень сложно знать заранее, что он делает у себя в гараже, кладовке или подвале...Не происходит никаких выделений или излучений. Современный уровень развития технологий не позволяет выяснить, кто производит сибирскую язву у себя в подвале».

Даже если конгресс сожжет Конституцию и превратит США в полицейское государство, говорит Бейли, это не избавит общество от угрозы биотерроризма. «Вы действительно думаете, что сможете поймать человека, собирающегося терроризировать население биологическим оружием? Как вы об этом узнаете? Вы не знаете, в какой дом пойти. Или вы хотите иметь по одному полицейскому на каждого жителя Земли, чтобы они контролировали друг друга? Даже если вы сделаете это, вы не гарантированы оттого, что кто-то однажды совершит ошибку».

Вместо этого, говорит Бейли, мы должны готовиться к возможной атаке путем разработки вакцин и лекарств: «Я считаю, что мы должны иметь хорошие лекарства и постоянно быть в курсе того, какие патогены могут быть использованы террористами. И я думаю, что для правоохранительных органов чрезвычайно важно знать, что происходит в террористических группах».

Более того, мы должны постоянно контролировать окружающую среду на предмет появления первых признаков биологической атаки, говорит доктор Джонатан Такер из Центра исследований проблем нераспространения. Поражение спорами сибирской язвы лечится при помощи антибиотиков, если с момента заражения прошло не более трех дней. Проблема состоит в том, что симптомы заражения сибирской язвой проявляются лишь на третий или четвертый день. Если мы будем ждать, пока люди обратятся за неотложной

p64

Томас Джефферсон [Thomas Jefferson] – (1743–1826), 3-й президент США (1801–1809), основной автор Декларации независимости. Ему, в частности, принадлежат слова из Декларации: «Мы исходим из той самоочевидной истины, что все люди созданы равными и наделены Создателем определенными неотъемлемыми правами, среди которых право на жизнь, свободу и стремление к счастью».

²²⁰ Интервью автору, 11 августа 1997 года.

помощью, они умрут.

Вместо этого Такер предлагает установить недорогое оборудование для контроля воздуха в метро, крупных зданиях, аэропортах и других местах, являющихся привлекательными целями для биологической атаки: «В подземке вы можете установить пробоотборщики воздуха, которые будут постоянно брать пробы. Если они обнаружат присутствие необычной аэрозоли, будет инициирована тревога. В этом случае будет необходимо проанализировать пробу из фильтра». Если аэрозоль окажется сибирской язвой, общественность будет предупреждена.

Более того, говорит Такер, чиновники общественной безопасности нуждаются в тренингах, а также в средствах на приобретение оборудования для борьбы с этой угрозой. В 1997 году Пентагон зарезервировал 42 миллиона долларов на проведение тренировок правоохранительных органов на местах по отработке действий на случай биологической или химической атаки террористов. Но деньги не были потрачены на приобретение оборудования, а тренировки служб были проведены лишь в 24 самых крупных городах.

Аналогичные меры мониторинга и тренировки могли бы помочь в борьбе с угрозой ядерного или химического терроризма. Терроризм также может быть побежден путем внимательного мониторинга существующих ядерных и химических запасов: это предусмотрено для нераспространения ядерной угрозы и конвенцией по химическому оружию. Мы, конечно, могли бы пойти еще дальше этих требований, еще больше усилив безопасность ядерных, химических и биологических объектов.

Но многие борцы за гражданские свободы считают, что правоохранительные органы используют угрозу терроризма для оправдания расширения власти и увеличения бюджета, так же как они использовали угрозу диверсий и саботажа во время Первой и Второй мировых войн для оправдания атак на гражданские свободы.

Харви Сильверглэйт [Harvey Silverglate], адвокат по уголовным делам из Бостона, специализирующийся на проблеме гражданских свобод, формулирует это таким образом:

Я считаю, что угроза терроризма, о которой вы говорите, сильно преувеличена. «...» Я считаю, что она специально преувеличивается правоохранительными органами, желающими расширить свои возможности. Позвольте мне выразить это так: я не могу вспомнить ни одного события в истории, связанного с массовым уничтожением людей и собственности, которое было бы осуществлено частными лицами или группами, а не правительствами. Отдельные люди, группы, банды – нанесенный ими вред бледнеет по сравнению с тем вредом, который нанесли неконтролируемые правительства. В истории нет примеров Холокоста, за которыми не стояло бы государство.²²¹

Конечно, все потенциалы оружия массового уничтожения, обсуждаемые в данной главе, разработаны и улучшены правительствами. «Поэтому, – говорит Сильверглэйт, – я предпочел бы жить в мире, где правительства более ограничены в своих действиях, чем давать правительствам огромные, ничем не ограниченные возможности по обузданию частного терроризма. Я предпочел бы уживаться с некоторым количеством терроризма, чем с правительственным тоталитаризмом».

Даже если Сильверглэйт не прав, очевидно, что демократизация деструктивных технологий вкупе с постоянно уменьшающимся размером террористических ячеек привела к тому, что глобальный мониторинг потенциальных экстремистов и террористов является обреченной на провал тактикой. Заманчиво думать, что все, что нам нужно, – это пожертвовать своими гражданскими свободами, а именно правом на приватность, и мы навсегда будем защищены от террористических атак. Но такой выбор – глупая сделка, поскольку таких гарантий никто не сможет дать.

²²¹ Интервью автору, 13 мая 1997 года.

Вместо слежки за людьми, гораздо лучше было бы следить за радиоактивными материалами и ограничить доступность химических отравляющих веществ и исходных материалов для них. Вместо того чтобы поступаться приватностью, мы должны увеличить вложения в здравоохранение, создать запасы антибиотиков и активно контролировать окружающую среду на предмет появления первых признаков применения биологического оружия. В конце концов мониторинг появления новых микроорганизмов защитит нас как от микробов, созданных человеком, так и от микробов, существующих в природе.

Наконец, мы должны сконцентрироваться на построении общества, более устойчивого к разрушению крупных городов, которое почти наверняка может произойти в один не очень прекрасный день. В частности, мы должны начать планировать, что мы будем делать в случае потери Нью-Йорка. [p65]

10

Простите, но человек ли вы?

Я встретил Тенга среди подписчиков одной из электронных рассылок, посвященной вопросам компьютерных технологий и гражданских свобод. В то время я работал как внештатный журналист и писал материалы о компьютерной революции для нескольких газет и журналов. Тенг работал системным аналитиком и отвечал за работоспособность компьютерных сетей в одном из крупных банков Сингапура. Он заинтересовался одной из моих публикаций и послал мне электронное письмо, в котором рассказал о жизни в его офисе. В течение следующих нескольких месяцев мы стали обмениваться посланиями по электронной почте чаще и вскоре стали «электронными друзьями».

В течение двух лет мы обменивались с Тенгом электронными письмами как минимум два-три раза в неделю. Он рассказывал мне, что собой представляет жизнь в Сингапуре, какие вещи он покупает в магазинах, о влиянии американской культуры, о том, как его банк «борется» с новыми технологиями. Тенг, в свою очередь, задавал мне множество вопросов. Я рассказал ему о жизни в США, какие виды товаров я предпочитаю покупать, какие фильмы мне нравятся и о покупке какой модели автомобиля я подумываю. Иногда вопросы Тенга были несколько бестактны, но я считал, что он просто интересуется американской культурой. Иногда возникало впечатление, что он не понял смысла отправленного мною письма, иногда он вновь спрашивал что-то, о чем я ему уже рассказывал несколько недель назад. Я всегда списывал эти несуразицы на языковой барьер.

Но однажды судьба дала мне шанс: один нью-йоркский журнал предложил мне отправиться в Сингапур, чтобы написать репортаж о взрывном развитии высоких технологий в этой стране. Я послал Тенгу электронное письмо с вопросом, не хочет ли он встретиться лично, и если да, то когда ему будет это удобно. Но Тенг проигнорировал это письмо; он ответил мне обычным сообщением, в котором рассказал, чем он занимался в последнее время, и поинтересовался, что нового произошло в моей жизни. Я послал ему второе письмо, затем третье, с вопросом о возможности нашей встречи. Наконец он прислал мне ответ, в котором говорилось, что как раз во время моего визита его не будет в городе и встретиться нам нет никакой возможности.

Не знаю почему, но у меня возникли подозрения в отношении Тенга. Я вдруг осознал, что практически ничего о нем не знаю. В одном из писем я спросил его домашний адрес и номер телефона, но он не ответил. Я связался с банком, в котором, по его словам, он работал. Но там никогда не слышали о таком человеке. Наконец, я обратился к одному своему другу, который работал в *New York Times*. Через репортеров сингапурского бюро *Times* он навел

справки. Получение информации заняло около недели, но когда я узнал правду, я не мог в нее поверить!

Банк, в котором работал Тенг, заключил контракт с американской фирмой, занимающейся исследованиями рынка. Компания создала группу вымышленных личностей, которые «вылавливали» в Интернете американцев, устанавливали с ними дружеские отношения и вытягивали из них ценную для заказчика информацию. Тенг не был реальным человеком, это была компьютерная программа!

Смоделированному человеку нельзя доверять

К счастью для пользователей Интернета, история с Тенгом вымышленная. Хотя я часто завожу «электронные знакомства» с людьми, которых встречаю в списках электронной рассылки по профессиональной тематике, у меня есть достаточно оснований полагать, что мои корреспонденты, находящиеся в Англии, Индии или Японии, являются существами из крови и плоти, а не компьютерными программами, посланными собирать интимные подробности моей жизни.

Между тем многие технологии, необходимые для создания Тенга, существуют уже сегодня. Конечно, Тенг не может быть создан как полноценная модель человеческого интеллекта. Однако он и еще тысячи подобных моделей могут быть созданы путем использования шаблонов, на основе стереотипности мышления, предсказуемости ответов и большого количества средств автоматизированной обработки текста.

Тенг представляет угрозу основам, на которых строятся человеческие отношения. Доверие, честность, уникальность и юмор – ценные качества. Ложь не одобряется ни в одном человеческом обществе. Люди понимают, что это неправильно, и очень часто чувствуют вину, обманывая других. Эти проблемы встают каждый раз, когда люди общаются друг с другом. Правда, всегда найдутся те, кто не захочет играть по правилам, но их достаточно легко вычислить через некоторое время. Общество даже наказывает таких людей, когда они слишком заходят за рамки этики.

Смоделированный человек не может испытывать чувство раскаяния. Он не понимает языка обычных эмоций, созданного человеческим сообществом. Маскирующийся под человека компьютер, который пытается строить человекоподобные отношения и никогда не откроет, что он машина, может быть применен только для использования в неких целях реальных людей, с которыми он вступает в контакт.

ELIZA и ее потомки

Первой компьютерной программой, имитирующей человека, была ELIZA, разработанная Джо Вейценбаумом [Joe Weizenbaum] из Лаборатории искусственного интеллекта Массачусетского технологического института. ELIZA представляла собой простейшую модель человеческого интеллекта. Вейценбаум создал программу в начале 1960-х, когда остальной персонал Лаборатории ИИ бился над созданием компьютера, способного понимать английский язык. Но это было слишком сложно. Вместо того чтобы пытаться создать *разумный* компьютер, Вейценбаум создал компьютерную программу, поведение которой *выглядело* разумным. «Я взял все свои шутки, собрал их вместе и на этой основе запустил ELIZE», – рассказывал он исследователю-историку искусственного интеллекта Даниелю Кревье [Daniel Crevier].²²²

ELIZA была очень простой программой, изображавшей роджерианского психотерапевта – последователя школы психиатрии, основанной Карлом Роджерсом. Роджерианская техника состоит в побуждении пациента говорить о своих проблемах,

²²² Crevier, *AI: Tumultuous History*, p. 133–140.

отвечая вопросом на вопрос. ELIZA анализировала введенные человеком фразы, находила среди частей речи глаголы и существительные, переворачивала предложение наоборот и выводила его на экран. Вы могли сказать программе: «Мой парень заставил меня прийти сюда», на что ELIZA отвечала: «Почему Ваш парень заставил вас прийти сюда?» Если у нее возникали затруднения, она могла вернуться к более ранним темам разговора или отделаться шаблонной фразой типа: «Почему Вы пришли сюда сегодня?»

На опытного специалиста-компьютерщика или лингвиста ELIZA не производила впечатление сложной и умной программы. Но для неподготовленного пользователя ее способность поддерживать разговор казалась удивительной. Даже люди, которые знали, что ELIZA – всего лишь компьютерная программа, увлекались этой игрой. Они доверяли ей свои личные секреты и проблемы. «Секретарь Вейценбаума, которая наблюдала в течение нескольких месяцев работу над программой, попросила, однако, выйти его из помещения на время ее первого „терапевтического“ сеанса с программой», – пишет Кревье.

Шокированный поведением своего детища, Вейценбаум вскоре пришел к выводу, что «основная идеология развития искусственного интеллекта – искусственный разум – безнравственна».

После того как ELIZA была написана, этот «подвиг» повторили десятки тысяч программистов. Хью Лебнер [Hugh Loebner], изобретатель и богатый филантроп, спонсирует ежегодный конкурс по написанию программ, имитирующих человека. Автора программы, поведение которой невозможно будет отличить от поведения реального человека из плоти и крови, ожидает приз в размере 100 тысяч долларов и медаль из чистого золота весом 14 карат.²²³ Пока это не удалось никому. Большинство представленных на конкурс программ «срезались» из-за недостаточного владения английским языком и отсутствия доступа к огромному количеству знаний, являющихся для всех нас само собой разумеющимися.

Однако в менее формальных условиях программы, подобные ELIZA, могут быть приняты за человека. Первое описание такой ситуации, наиболее ярко демонстрирующее проблему приватности применительно к искусственному интеллекту, относится к 1989 году. Речь идет об общении программы MGonz, запущенной в Ирландии, и старшекурсника университета Дрейк в Айове. MGonz была создана Марком Хамфрисом [Mark Humphrys], старшекурсником университетского колледжа в Дублине. Программа отличалась от ELIZA тремя важными моментами. Во-первых, вместо того чтобы общаться на классическом английском языке, MGonz часто обращалась к сленгу, используемому малолетними хакерами. Во-вторых, автор провел «стажировку» программы в сети BITnet, позволяя ей обмениваться короткими сообщениями с участниками сети по всему миру. Наконец, MGonz вела журнал всех своих переговоров.

Во вторник вечером, 2 мая 1989 года, Хамфрис оставил программу запущенной и ушел домой. В 20:12 по ирландскому времени студент из Дрейка начал посылать сообщения программе. Программа отвечала ему. В течение последующего часа и двадцати минут программа выудила из дрейковского студента подробности его сексуальной жизни. К концу сеанса, не осознавая, что ведет диалог с машиной, студент поведал программе, что он потерял девственность в 17 лет, а прошлой ночью занимался сексом в спальне своей подружки. «Войдя в систему на следующий день, я был немало удивлен, что программа успела натворить в мое отсутствие», – вспоминает Хамфрис, поместивший позже запись этой сессии в Интернет (предварительно удалив из текста, по понятным соображениям, имя студента из Дрейка).²²⁴ Хамфрис сказал мне:

²²³ Для получения дополнительной информации о премии Лебнера, я рекомендую обратиться к прекрасной статье Чарльза Платта [Charles Platt] «What's It Mean to Be Human, Anyway?», опубликованной в *Wired Magazine* в апреле 1995.

²²⁴ Полную запись «беседы» между студентом из Дрейка и MGonz можно найти по адресу <http://www.compapp.dcu.ie/~humphrys/eliza.html>.

Я всегда слегка беспокоился по поводу этой программы, пока не понял, что она преподавала прекрасный урок. Мне понадобилось шесть лет, чтобы осознать это. Заметьте, что все самые дикие непристойности и обещания всегда исходят от человека, а не от машины, которая отвечает с холодным безразличием и задает немного приводящих в бешенство вопросов.²²⁵

MGonz лишь одна из многих программ искусственного интеллекта, прокладывающих свой путь через киберпространство. Другой робот, вызвавший раздражение многих миллионов людей, носил имя Zumabot. Zumabot сканировал конференции Usenet в поисках публикаций, содержащих слово «Turkey»,^[p66] и отвечал на них агрессивными сообщениями о мнимом массовом убийстве мусульман в Армении во время Первой мировой войны.

По мнению автора статьи, появившейся в *Internet Underground*, создание Zumabot было оплачено турецкими спецслужбами. Программа буквально стала пропагандистской машиной. Ее целью было дискредитировать тех, кто говорил о массовом убийстве турками армян в 1917 году, путем многократного повторения, что все было наоборот. «Zumabot был частью широкомасштабной политики подавления разногласий среди турецких экспатриантов».²²⁶

Виртуальные роботы становятся неотъемлемой частью интерактивных многопользовательских игр [MUD – Multi-User Dungeon games] в Интернете. Программы, подобные ELIZA, часто инициируют общение с одинокими людьми, выдавая себя за женщин, желающих установить приятельские отношения.

Многие электронные сообщества установили правила, по которым компьютер обязан идентифицировать себя. Шахматный клуб Интернета [ICC, Internet Chess Club], позиционирующий себя как «самый активный шахматный клуб в мире», регулярно посещает 20 тысяч пользователей, и в нем ежедневно проходит 60 тысяч шахматных партий. В этом клубе есть специальное правило относительно использования компьютеров: все компьютеры должны быть зарегистрированы. Использование незарегистрированного компьютера приводит к аннулированию регистрационной записи. Компьютерам и людям запрещается совместно использовать одну регистрационную запись. И возможно, самое главное – компьютерным программам запрещено предлагать игру людям, им можно лишь откликаться на приглашение.

«Человек имеет право знать, играет он с компьютером или с человеком». Правила ICC гласят:

Использование компьютера без уведомления администрации, или без соответствующей метки [в профиле учетной записи], или без помещения учетной записи в список «компьютерных» [является нарушением правил системы]. У нас многолетний опыт выявления использования компьютеров, поэтому не пытайтесь нас обмануть. Берегите свое время и время администрации: своевременно подавайте запрос на включение в компьютерный список.²²⁷

²²⁵ Из личной электронной почты, 28 октября 1999.

p66

Слово имеет два перевода: «Турция» и «индюшка».

²²⁶ Michael McCormick, «Invasion of the Internet Imposters», *Internet Underground*, 8 июля 1996. Одной из наиболее забавных (и раздражающих) черт Zumabot была неспособность программы различать слова «Турция» и «индюшка», которые пишутся по-английски одинаково. Это стало очевидным незадолго до Дня благодарения, когда программа начала протестовать против праздничных рецептов приготовления птицы.

²²⁷ См. сайт клуба по адресу <http://www.chessclub.com>.

ИСС имеет два вида проблем с роботами, говорит Мартин Грунд [Martin Grund], директор ИСС по интерактивной деятельности. Первая проблема заключается в том, что некоторые люди создают программы, которые соединяются с клубом, входят в систему и приглашают людей сыграть партию. Вторая, более тонкая проблема, возникает с теми, кто входит в систему сам, но фактически играет за них запущенная на их компьютере шахматная программа (это давняя проблема при игре в шахматы по переписке).

Алан Тьюринг

Многие считают Алана Тьюринга [Alan Turing] отцом искусственного интеллекта. Он действительно является одним из основателей компьютерной науки. Во время Второй мировой войны благодаря усилиям Тьюринга британское правительство смогло вскрыть шифры, при помощи которых нацистский режим держал связь со своими подводными лодками и военачальниками. После войны Тьюринга все больше и больше стала интересовать идея создания компьютера, который мог бы вести себя подобно человеку. Сегодня Тьюринг известен благодаря тесту Тьюринга, простому эмпирическому правилу, позволяющему установить, действительно ли компьютер думает и обладает самосознанием или он имитирует человеческий разум. Суть этого теста заключается в практическом испытании, происходящем приблизительно так: человека помещают в изолированную комнату с компьютером. После этого ему предоставляется возможность общаться с другим человеком и с компьютерной программой, при этом все общение происходит исключительно с помощью клавиатуры и экрана. Если испытатель не может различить машину и человека, то компьютерная программа признается такой же интеллектуальной и разумной, как и человек. [Фотография любезно предоставлена Компьютерным музеем (Бостон, Массачусетс) и Историческим центром (Маунтинвью, штат Калифорния)]



«Играть в шахматы на уровне гроссмейстера при поддержке компьютера – способ удовлетворения своих амбиций, в то время как противник в Чили, Аргентине или Австралии осознает свою слабость перед гроссмейстером и сдается, – говорит Грунд. – Получение удовольствия от сознания, что *ваш компьютер* стал победителем, достаточно странно».²²⁸

ИСС не считает проблемой сам факт подключения к системе компьютеров и роботов, говорит Грунд. Действительно, в системе ИСС всегда есть достаточное количество компьютерных оппонентов готовых сразиться и помочь всем желающим повысить свой уровень. Но эти программы никогда не лгут и не притворяются людьми. Если вы пошлете такой программе сообщение: «Привет», она ответит: «Извините, но я всего лишь компьютер. Это мне Вы сказали „привет“».

«Люди, которые нарушают правила и пытаются выдать свои компьютеры за людей, не правы с точки зрения морали, – говорит Грунд. – Шахматы – честная игра. А обманывать в

²²⁸ Интервью автору, 25 августа 1997.

честной игре по меньшей мере трусость. Это бесчестно».

Шахматный клуб Интернета является хорошей базой для развития межчеловеческих связей с использованием компьютерных технологий, а установленные в нем правила применимы гораздо шире. Люди должны быть юридически защищены от попыток компьютеров выдать себя за людей. Такой маскарад является по сути мошенничеством. Из этого не следует, что надо запретить использовать компьютеры в общении между людьми. Но обязанность пометать все свои сообщения как сгенерированные машиной должна стать законом для всех компьютеров. Более того, все машинные сообщения должны содержать подробную информацию, каким образом можно связаться с человеком, ответственным за данный компьютер, т. е. с оператором. Это единственный способ правомерной интеграции интеллектуальных программ в человеческое общество.

Компьютер как ваш агент

Информационная перегрузка – одна из серьезнейших проблем, с которой сталкиваются сегодня работники умственного труда. Каждый день на нас сваливаются тысячи сообщений по электронной почте, web-страниц и газетных статей. Информация льется на нас со страниц книг и журналов, из радио, с телевидения, из инструкций по использованию, с видеокассет, из новых фильмов, с досок объявлений и даже рекламы в небе.

Один из ключевых механизмов, предлагаемых современными технологиями для борьбы с информационной перегрузкой, – это *интеллектуальный агент*. Идея такой программы состоит в том, что она знает ваши интересы и предпочтения и использует данную информацию для фильтрации огромного потока информации, врывающегося в вашу жизнь таким образом, что вы видите лишь то, что желали бы увидеть. Хотя для создания таких агентов предлагалось использовать самые разные технологии, первой на рынке появилась технология называемая *совместной фильтрацией*.

Идея совместной фильтрации чрезвычайно проста. В реальном мире слишком много газет, записей, книг, фильмов, радио– и телевизионных станций, чтобы можно было уделить внимание всему этому разнообразию. Но вам это и не нужно. Вместо этого, вы спрашиваете своих друзей об их предпочтениях. Рано или поздно вы определяете, с кем из ваших друзей вы сходите во вкусах по части музыки и новостей, а чьи интересы так же далеки от вас, как планета Юпитер. Вы определяетесь, кому доверять. Конечно, такое сотрудничество – процесс двусторонний, и вы тоже будете давать рекомендации своим друзьям. И естественно, когда вы обнаружите, что кому-то из друзей приходится по вкусу ваши советы, вы больше станете доверять его советам. Но до того, как вы узнаете это, вам, возможно, придется организовать собственный список рассылки.

Компьютеризованная совместная фильтрация автоматизирует этот процесс. Рекламщики утверждают, что совместная фильтрация может быть использована для доставки информации потребителю более точно, чем, например, поиск по ключевым словам. Они утверждают, что могут сформировать общественное мнение на безликом в другой ситуации web-сайте.

Известный онлайн-книжный магазин Amazon.com использует разновидность совместной фильтрации, чтобы помочь покупателям в выборе книг. В основе системы лежит теория о том, что если существует книга, которая нравится одновременно двум людям, вероятнее всего, существует и еще целый ряд книг, которые заинтересуют их обоих. Система пытается найти пересечение интересов разных людей, и у нее это неплохо получается. Например, если вы выберете «Практическую безопасность UNIX и Интернета» [*Practical UNIX & Internet Security*], одну из моих книг, Amazon сообщит вам:

Клиенты, которые купили эту книгу, купили также «Построение межсетевых экранов в Интернете» Брента Чапмена и др. [*Building Internet Firewalls* by D. Brent Chapman et al.]; «Основы компьютерной безопасности» Деборы Рассел и Г.Т. Гэнджеми [*Computer Security Basics* by Deborah Russel]; «Администрирование

сетей TCP/IP» Крейга Ханта и Гиджи Эстабрук (редактор) [*TCP / IP Network Administration* by Craig Hunt and Gigi Estrabook (editor)]; «Краткий курс системного администрирования: в помощь системным администраторам UNIX (карманный справочник)» Элин Фриш [*Essential System Administration: Help for UNIX System Administrators (Nutshell handbook)* by Eleen Frish].

После того как вы покупаете на Amazon.com несколько книг, система анализирует ваши покупки и строит огромную матрицу, содержащую корреляции между вами и всеми остальными клиентами. Когда я захожу на web-сервер Amazon, он встречает меня, например, таким приветствием: «Здравствуйте, Симеон Л. Гарфинкель! Мы можем порекомендовать вам книги по темам „Компьютеры и Интернет“, „Документальная литература“, „Развлечения“ и другие». Если я выберу раздел «Документальная литература», система порекомендует мне пять книг:

«Холодный гнев: История о вере и могуществе политиков» Мери Бет Роджерс и Билла Мойерса (введение) [*Cold Anger: A Story of Faith and Power Politics* by Mary Beth Rogers, Bill Moyers (introduction)]; «В поисках приватности: Закон, этика и развитие технологий» Джудит Вагнер Дисью [*In Pursuit of Privacy: Law, Ethics and the Rise of Technology* by Judith Wagner Decew]; «Технология и приватность: Новый ландшафт» Филипа Эгра (редактор), Марка Ротенберга (редактор) [*Technology and Privacy: The New Landscape* by Philip Agre (editor), Marc Rotenberg (editor)]; «Ваше право на приватность: Базовое руководство по законным правам в информационном обществе (сборник Американского союза за гражданские свободы)» Эвана Хендрикса и др. [*Your Right to Privacy: A Basic Guide to Legal Rights in an Information Society (An American Civil Liberties Union Handbook)* by Evan Hendricks, et al.]; «Диалог между классами и другие уроки первичной организации» Линды Стоут и Говарда Зинна [*Bridging the Class Divide and Other Lessons for Grassroots Organizing* by Linda Stout, Howard Zinn].

Совершенно очевидно, что Amazon знает, что я покупал книги по определенной тематике, и хочет помочь мне купить еще!

Другие системы потенциально гораздо более сложны. Когда я был аспирантом МТИ и работал в Лаборатории медиа, там было большое количество различных видов интеллектуальных агентов. Джон Оруэнт [John Orwant], научный сотрудник, разработал программу Doppelganger.²²⁹ «Doppelganger – мистическое чудовище из германского фольклора, которое выбирало невинного человека и подглядывало за ним из тени, наблюдая за его привычками, встречами, эмоциями и особенностями, – объяснял Оруэнт. – Через некоторое время Doppelganger начинал походить на этого человека, вести себя как этот человек, и в конечном счете становился этим человеком незаметно для всех».

Созданный Оруэнтом программный Doppelganger пытался сделать то же самое. Программа наблюдала за действиями человека и пыталась построить его модель: что ему нравится и не нравится, наиболее значимые события его жизни. Чем больше информации о вас могла собрать программа, тем точнее она подстраивалась под вас. После этого Doppelganger делал свою базу данных доступной другим программам на вашем компьютере, отвечая на их запросы. Например, глядя, какие электронные издания вы читаете, Doppelganger строил модель ваших предпочтений: какие статьи вам нравятся, а какие нет. На следующий день программа для чтения электронных газет могла спросить Doppelganger, включать или нет конкретную статью в ежедневную подборку для вас. Чтобы не нарушить личную тайну пользователя, вся конфиденциальная информация при передаче ее по

²²⁹ J. Orwant, «For Want of a Bit the User was Lost: Cheap User Modeling», *IBM Systems Journal*, 35: 3 &4, 1996.

компьютерной сети шифровалась при помощи PGP.^[p67] Другой сотрудник Лаборатории медиа, Макс Метрал [Max Metral] разработал ассистента для электронной почты. Программа наблюдала за действиями пользователя, строила его модель, после чего пыталась ее задействовать. Например, если программа замечала, что вы читаете электронные письма от вашей матери сразу же после их получения, то программе начинала автоматически открывать их для вас сразу после их поступления в почтовый ящик, после чего складывала в отдельную папку.²³⁰

Нет никаких причин, по которым программа останавливалась бы на этом. Умная программа для чтения почты может делать разбор входящей корреспонденции и помещать найденную там информацию в базу данных на естественном языке. После этого вы можете задать программе вопрос, например: «Когда я последний раз получал сообщение из Франции?» или: «Как называется модель нового ноутбука, недавно анонсированная IBM?» Компьютер даст вам ответ при помощи этой базы данных.

Это вовсе не научная фантастика. В 1991–1996 годах Агентство перспективных исследований американского Министерства обороны [US Department of Defense Advanced Research Project Agency, DARPA] спонсировало конкурс «Конференция по распознаванию сообщений» [Message Understanding Conference, MUC]. Целью конкурса было создание компьютерной программы, которая извлекала бы информацию из большого количества текстовых сообщений и облекала ее в машиночитаемую форму. В рамках MUC-6 участники написали программу, которая могла сканировать газетные статьи и искать в них информацию об изменениях среди руководящего персонала. Например, MUC-6 был предоставлен следующий текст:

McCann создал новую, так называемую глобальную систему сотрудничества, состоящую из всемирно известных финансовых директоров и творческих партнеров. Известно, что Питер Ким [Peter Kim] был приглашен в сентябре в WPP Group's & Walter Thompson на должность вице-президента, главного специалиста по стратегическому планированию.

В результате получились следующие данные:

```

«ОЧЕРЕДН_СОБЫТИЕ-940224      0133-3»:=      ОЧЕРЕДН_ОРГ:
«ОРГАНИЗАЦИЯ-94 022 4 0133-1» ПОСТ: «Вице-президент, главный специалист
по стратегическому планированию»
  ВХ_И_ВЫХ:      «ВХ__И_ВЫХ-9402240133-5»      ПРИЧИНА_ВАКАНСИИ:
ПРОЧ_НЕИЗВ
  КОММЕНТАРИЙ: «Ким стал вице-президентом... в McCann» «ВХ И
ВЫХ-9402240133-5»:=
  ВХ/ВЫХ_ЛИЧНОСТЬ: «ЛИЧНОСТЬ-94 022 40 133-5»
  НОВЫЙ_СТАТУС: ВХ
  В_РАБОТЕ: ДА
  ПРОЧ_ОРГ: «ОРГ-9402240133-8»
  ОТН_ПРОЧ_ОРГ: ВНЕШН_ОРГ
  КОММЕНТАРИЙ: «Ким пришел из другой организации (должность не
упомянута)» / «Точно известно, что сейчас он работает, назначен несколько
месяцев назад»
«ОРГАНИЗАЦИЯ-9402240133-1»:=
ОРГ_НАЗ: «McCann-Erickson»

```

p67

PGP (Pretty Good Privacy) – программа для шифрования и цифровой подписи сообщений, разработанная Филом Циммерманом [Phi Zimmermann].

230 Yezdi Lashkari, Max Metral and Pattie Maes «Collaborative Interface Agents» («Агенты совместного интерфейса»), MIT Media Laboratory, 1994 (не опубликовано). Доступно для загрузки по адресу <ftp://ftp.media.mit.edu/pub/agents/interface-agents/generic-agents.ps>.

ОРГ_ПСЕВДОН: «McСапп»
ОРГ_ОПИСАН: «одно из крупнейших мировых агентств»
ОРГ_ТИП: КОМПАНИЯ
«ОРГ-9402240133-8»
ОРГ_НАЗ: «J. Walter Thompson»
ОРГ_ТИП: КОМПАНИЯ
«ЛИЧНОСТЬ-94 022 4 0133-5»
ЛИЧН_ИМЯ: «Питер Ким»

В конечном счете вы можете использовать такую программу для создания большой машиночитаемой базы данных из неструктурированной информации, типа сообщений электронной почты или газетных статей.

Другая система была разработана в рамках проекта START в Лаборатории ИИ Массачусетского технологического института [MIT AI Lab].²³¹ В отличие от MUC, START была спроектирована, чтобы отвечать на вопросы, заданные на английском языке. Например, вы могли задать START вопрос:

«WHAT DOES START STAND FOR? [Для чего предназначена START?]

И получить ответ:

START stands for the Syntactic Analysis Using Reversible Transformations.
[START/p68] предназначена для синтаксического анализа с использованием обратимых преобразований.]

Борис Кац [Boris Katz], научный сотрудник Лаборатории ИИ, дал программе прочитать информацию об институте и поместил ее на web-сервер Лаборатории. Любой человек мог задать программе типовой вопрос и получить адекватный ответ. Например, вы могли спросить: „Где находится Лаборатория ИИ?“ и получить ответ: „Лаборатория искусственного интеллекта Массачусетского технологического института находится в Кембридже. Почтовый адрес лаборатории – MIT AI Laboratory, 545, Technology Square, Cambridge, MA 02139“.

Система также знала, как получить доступ к информации на других компьютерах в Интернете. Например, вы могли напечатать запрос:

= => SHOW ME A MAP OF CAMBRIDGE
[Покажи мне карту Кембриджа]

Система ответила:

Sorry, I don't have a map of Cambridge Massachusetts.
Click on the map of Massachusetts if you want to see it.
(Простите, но я не располагаю картой Кембриджа, штат Массачусетс.
Активируйте ссылку «карта штата Массачусетс», если желаете посмотреть на нее.)

²³¹ Информационный сервер START, называемый «START Natural Language Question Answering System» находится по адресу <http://www.ai.mit.edu/projects/infolab>. Упомянутый «Географический справочник ЦРУ 1999» [русское издание: Географический справочник ЦРУ'2000. Екатеринбург: У-Фактория, 2001.] доступен по адресу <http://www.odci.gov/cia/publications/factbook>.

Щелчок мышью на подчеркнутом тексте вызывал карту штата Массачусетс с сервера Time Warner Pathfinder.

Вы можете задать START вопрос о населении Иордании, и она, проконсультировавшись в «Географическом справочнике ЦРУ», даст ответ, что в июле 1999 года оно составляло 4 561 147 человек. Вы можете спросить ее о времени в Сиэтле, и она, обратившись к базе данных временных зон, а также к значению текущего времени в Кембридже, ответит на ваш вопрос.

Хотя START может показаться похожей на другие понимающие естественные языки программы, засоряющие в последние 30 лет область искусственного интеллекта, у нее есть одна важная особенность. Другие системы используют сложные выражения, написанные на загадочном компьютерном языке, чтобы получить знания, задать вопросы и посмотреть на результат; большая же часть START написана непосредственно на английском языке. Это значит, что огромное количество относительно неподготовленных людей могут вводить в нее информацию. Это также означает, что программа может самообучаться путем чтения информации, которая уже находится в Интернете.

Технология агентов-помощников существует уже сегодня и постоянно совершенствуется. Но кто контролирует агентов?

Агент, который может предвидеть ваши действия и желания может оказать неоценимую помощь человеку в борьбе с информационной перегрузкой. Но такой агент также может стать мощным инструментом в руках того, кто хочет заставить вас приобрести определенный продукт. Прогнозирующий агент может также стать незаменимым и для того, кто желает причинить вам вред.

Извлечение «я»

До своего ухода из Федеральной комиссии по торговле Кристина Варни [Christine Varney] написала для радиостанции National Public Radio следующий маркетинговый сценарий от имени агента:

Предположим, что каждый год на годовщину свадьбы вы посылаете цветы своей жене. Я замечаю, что в этом году вы этого не сделали. Я знаю также, что в настоящее время она находится не в Сан-Франциско, а в отеле Four Seasons в Лос-Анджелесе, и спрашиваю вас, необходимо ли мне послать ей цветы? Ваша реакция, восхищение или раздражение, зависит от одной вещи – вашего согласия.²³²

Действительно, восхититесь вы или испытаете раздражение, зависит от многих факторов. Если вы планировали встретиться с женой в этом отеле, вы останетесь довольны таким советом. Если вы полагаете, что ваша жена отправилась навестить свою больную маму в нью-йоркской провинции, то такое сообщение вполне может привести к разводу. А если ваша жена числится пропавшей, такое сообщение поможет вам найти ее. Согласие не фигурирует явно в этой истории. Вы могли дать согласие программе на это действие, если являетесь владельцем кредитной карты, но сам факт мог вызвать у вас раздражение. С другой стороны, даже если вы не дали такого согласия, программа сообщила вам важную информацию, которую вы не знали, и вы должны быть благодарны ей за это. Утверждение Варни ошибочно по другой причине: для практической реализации этой не слишком футуристической рыночной стратегии с использованием агента согласия не требуется. Вся необходимая для реализации описанного Варни сценария информация доступна сегодня банкам и компаниям, имеющим дело с кредитными картами.

²³² Christine Varney, член комиссии FTC, обращение к John McChesney в передаче national Public Radio «All Things Considered», 10 июня 1997.

Если что и сдерживает появление таких программ, то это вовсе не отсутствие согласия клиентов, а отсутствие строгого рыночного обоснования, что такое программное обеспечение принесет компаниям дополнительную прибыль.

Марк Ротенберг [Marc Rotenberg] из Информационного центра электронной приватности [Electronic Privacy Information Center] полагает, что агенты следующего поколения будут сканировать всю доступную персональную информацию о личности, после чего строить прогнозирующую модель для использования маркетологами и другими заинтересованными лицами. Ротенберг назвал это *извлечением «я»*.

Извлечение «я» – одна из наиболее значимых угроз неприкосновенности частной жизни и личностной уникальности со стороны компьютеров. Ваш профиль будет содержать информацию о каждом документе, который вы когда-либо читали, о каждом человеке, которого вы знаете, о каждом месте, которое вы посещали, о каждом произнесенном когда-либо вами и записанном слове. Ваша уникальность будет теперь существовать не только внутри вас, но и внутри вашей модели. «Она будет знать о вас больше, чем вы сами знаете о себе, – говорит Ротенберг. – С этого момента мы теряем не только индивидуальность, мы теряем индивидуумов».²³³

Фактически первый опыт извлечения «я» уже состоялся. В конце 1980 года Джанет Колоднер [Janet Kolodner], аспирантка одного из пионеров искусственного интеллекта в Йельском университете – Роджера Шенка [Roger Schank], создала программу под названием CYRUS. Программа Колоднер была попыткой моделирования памяти государственного секретаря президента Картера – Сайруса Вэнса [Cyrus Vance]. Вспоминает исследователь-историк искусственного интеллекта Даниэль Кревье:

Программа действительно осознавала себя в качестве Вэнса и получала свою «память» из новостей о Вэнсе, перехватываемых с помощью FRUMP [еще одна программа искусственного интеллекта]. Однажды ей был задан вопрос, встречалась ли жена Вэнса с женой израильского премьер-министра Бегина. CYRUS вспомнила, что Вэнс и Бегин принимали участие в мероприятии, на котором были вместе с женами, и дала точный ответ: «Да, на официальном обеде в январе 1980 года в Израиле».²³⁴

Технологических методов предотвращения извлечения «я» не существует. Но если мы хотим, чтобы неприкосновенность частной жизни сохранилась в будущем, такие технологии должны быть взяты под контроль. Существует целый ряд способов установления такого контроля.

Одним из законных средств противодействия извлечению «я» может стать авторское право. Американское законодательство и международные соглашения предусматривают специальный вид авторского права – *авторское право на компиляцию*. Это право защищает газеты, компакт-диски и другие виды носителей сборной информации, даже если отдельные их элементы не являются объектом защиты авторского права. Доктрина авторского права на компиляцию могла бы быть распространена и на отдельные компоненты жизни человека. Вы можете не претендовать на защиту при помощи авторского права каждого произнесенного вами предложения, названия каждого купленного вами продукта или названий улиц, на которых вы проживали с момента рождения. Но когда эти разрозненные факты объединяются в целое, они могут быть использованы против вас. Физические и юридические лица, уличенные в такой практике, должны быть подвергнуты штрафу или тюремному заключению.

Другим путем борьбы с этой проблемой может стать принятие и исполнение жестких

²³³ Из личной электронной почты, 27 августа 1997.

²³⁴ Crevier, *AI: Tumultuous History*.

законов, запрещающих накопление и обобщение персональной информации без исключительного разрешения субъекта этих данных. Законодатели должны четко придерживаться третьего принципа Кодекса о справедливом использовании информации: недопустимо использовать персональную информацию, полученную с одной целью для другой цели, без разрешения субъекта этой информации.^[p69] Необходимость подтверждающего разрешения на накопление данных и их использование в определенных целях, так же должна быть предметом регулирования закона.

Права воплощения!

Более ста лет назад первый программист – леди Ада Лавлейс [Lady Ada Lovelance, 1815–1852] написала серию писем Чарльзу Бэббиджу [Charles Babbage], изобретателю первого механического компьютера. В одном известном письме Лавлейс предположила, что настанет день, когда изобретенные Бэббиджем машины смогут мыслить самостоятельно, если будут правильно запрограммированы. В 1950 году один из величайших пионеров компьютерной науки Алан Тьюринг написал исследовательское эссе о том, как однажды компьютеры смогут стать разумными, и предложил тест, при помощи которого люди могли бы определить, разумна машина или нет. С тех пор десятки тысяч ученых посвятили свою жизнь созданию искусственного интеллекта, миллиарды долларов потрачены на достижение этой цели. И только несколько прорывов принесли существенную выгоду некоторым удачливым предпринимателям. Несмотря на это, спустя более чем 150 лет совершенствования технологий, искусственный интеллект по-прежнему остается иллюзией.

Сегодня не утихают грандиозные философские дебаты на тему возможно ли создание настоящего искусственного интеллекта. Они чрезвычайно похожи на дебаты о возможности искусственного полета, развернувшиеся в последний год XIX столетия. Некоторые считали, что это возможно, другие полагали, что это невозможно. Научные журналы публиковали неопровержимые доказательства того, что человек никогда не сможет построить летательный аппарат.²³⁵ Но пока шли эти дебаты, изобретатели во всем мире неуклонно продвигались к своей цели. Первые попытки создать орнитоптер – машину с машущими крыльями – потерпели неудачу. Стало очевидно, что создаваемая человеком машина, должна использовать другой принцип, нежели простое повторение природы. Ученые стали конструировать планеры и аэродинамические трубы, чтобы изучить природу подъемной силы. В 1903 году конец дебатам положил первый успешный полет на летательном аппарате тяжелее воздуха, совершенный братьями Райт [Orville и Wilbur Wright].

Очень похожие вещи происходили и с искусственным разумом в следующие 50 лет. Подходы, являющиеся сегодня многообещающими, будут усовершенствованы. Другие уйдут в сторону; будут открыты новые.

Рэй Курцвейль [Ray Kurzweil], один из пионеров искусственного интеллекта, основавший несколько успешных компаний, занимающихся ИИ-технологиями, предполагает, что рождение разумной машины произойдет неожиданно, в результате согласованных попыток создать аналог человеческого мозга для хранения в нем информации в качестве резервной копии. В своей вступительной речи на открытии Ближневосточной конференции по информационным технологиям, проводимой Gartner Group в июне 1995

p69

Необходимость получения разрешения субъекта и соответствия целей использования целям сбора предусмотрена, например, в предложенной Симоной Фишер-Хюбнер [Simone Fischer-Hiibner] модели управления доступом к информации, нашедшей практическую реализацию в проекте RSBAC. См. «From a Formal Privacy Model to its Implementation» (<http://www.rsba.org/niss98.htm>).

²³⁵ Подробная история изобретения самолета и дебаты по поводу возможности искусственного полета можно найти на сервер университета Иллинойса по адресу <http://hawaii.psychology.msstate.edu/invent>.

года, Курцвейль обрисовал следующий возможный вариант развития.²³⁶

- К 1997 году компании, такие как Dragon Systems, выпустят на мировой рынок первую систему распознавания речи с большим словарем – настоящую «голосовую пишущую машинку», которая позволит говорить обычным образом, а компьютеру – записывать сказанное (это уже произошло). В 1998 году компании смогут предложить аналогичную систему, не зависимую от говорящего, и позволят использовать технологию в слуховых аппаратах для глухих (этого пока не произошло).

- К 2005 году «компьютеры смогут влиять на психическое состояние человека, по необходимости помогая справиться с такими расстройствами, как перенапряжение и беспокойство». Люди будут общаться с компьютерами преимущественно устно. Компьютерные дисплеи тем временем уменьшатся до размера очков, которые будет носить подавляющее большинство людей, эти очки будут представлять собой «трехмерный дисплей, перекрывающий обычный визуальный мир».

- К 2011 году компьютеры смогут играть роль людей настолько хорошо, что искусственные люди станут первичным средством обучения: «Вместо того чтобы читать о Конституционном конвенте, студент сможет... подискутировать с моделью Бена Франклина о чрезвычайных полномочиях в военное время, роли судов и других аспектах».

- К 2030 году люди смогут полностью воссоздать структуру нейронной организации человеческого мозга. Технология позволит людям просканировать собственный мозг и использовать «свои персональные компьютеры как персональные устройства резервного копирования».

Курцвейль размышляет далее:

Когда человек будет отсканирован и воссоздан в нейрокомпьютере, человечество задумается: «Кто же этот человек в машине?» Ответ зависит от того, кого спросить. Если спросить человека, находящегося внутри машины, он, несомненно, заявит, что является исходной личностью, прожившей несколько жизней, помещенной в сканер и проснувшейся в компьютере. «Ого! Эта технология действительно работает. Вы должны дать ей попытку!», – скажет он. С другой стороны, исходная личность, подвергнутая клонированию, заявит, что человек внутри машины – самозванец, который просто разделяет с ней память, историю, знакомых, но на самом деле является абсолютно другим человеком.

Тем не менее это происходит, и разумные машины будут созданы в ближайшие 50 лет. А будучи созданными, они поднимут одну не известную доселе проблему. Помещенный в кремниевые пластины разум всегда должен оставаться открытой книгой. Принципиально важно, чтобы этот компьютер ничего не скрывал от своих создателей – ни одного бита данных, ни одного кусочка информации, ни одного варианта расчета. Его память должна быть открыта для просмотра. Человек должен управлять созданными им разумными машинами так же, как Бог управляет людьми.

Не станет ли разум, которому не оставлено ни капли приватности, психически больным? Не получится ли так, что соединение разума и памяти внутри компьютерных банков данных станет настолько сложным, что не сможет быть расшифровано создавшими его людьми без помощи самих разумных машин? Будут ли этичными эксперименты над искусственным разумом, например стирание некоторых участков его памяти и наблюдение за реакцией? Будет ли это действие более этичным, если после его окончания искусственный разум будет возвращен в исходное состояние?

«Аморально или незаконно причинять боль и страдание вашей компьютерной

²³⁶ Ray Kurzweil, «Turing's Prophecy – Machine Intelligence: the First 100 years (1940–2040)», Keynote Address, Gartner Group Middle East Information Technology Conference, Tel Aviv, Israel, 25 июня 1995.

программе? – размышляет Курцвейль. – Законно ли отключать вашу компьютерную программу? Возможно, это незаконно, если вы не сделали резервную копию».

Но эти вопросы – только начало, замечает Курцвейль:

К 2040 году в соответствии с законом Мура²³⁷ обычный серийный персональный компьютер будет в состоянии моделировать разум 10 тысяч человек, каждый из которых будет функционировать в 10 тысяч раз быстрее реального человеческого мозга. Либо он сможет реализовать модель человека с емкостью памяти в 10 тысяч раз больше обычного мозга и работающую в 100 миллионов раз быстрее. Каковы будут последствия такого развития?

Учитывая реальную возможность того, что наши интеллектуальные потомки будут населять описанные Курцвейлем мифические машины в 2040 году, мы должны серьезно подумать о правовом и этическом режиме, в соответствии с которым эти разумные аватары будут функционировать, – если эти аватары действительно являются репликантами человеческого разума, если они думают и сами создают объекты творчества, они должны обладать теми же правами на приватность, что и люди из плоти и крови. С другой стороны, в этом случае произойдет описанный в главе 9 перехват разума. Если же пойти другим путем, то в наших собственных интересах гарантировать права компьютерному разуму: приватность, которую вы сохраняете, однажды может оказаться вашей!

11

Право на личную тайну сейчас!

Преамбула

...Принимая во внимание, что необходимо, чтобы права человека охранялись властью закона в целях обеспечения того, чтобы человек не был вынужден прибегать, в качестве последнего средства, к восстанию против тирании и угнетения...

Статья 12

Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств.

«Всеобщая декларация прав человека».

Принята и провозглашена резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года (Doc A/810 at 71).^[p70]

²³⁷ Закон Мура не является законом в полном смысле этого слова. Это наблюдение, сделанное основателем фирмы Intel Гордоном Муром [Gordon Moore]. В соответствии с законом Мура, производительность компьютеров по скорости удваивается приблизительно каждые 18 месяцев в результате развития полупроводниковых технологий и вложений в научно-исследовательские и опытно-конструкторские работы.

p70

Прцитирован перевод Декларации на русский язык, доступный на сервере ООН в Интернете по адресу <http://www.un.org/russian/documen/declarat/declhr.htm>.

В XXI веке кампания против свободы и независимости личности разворачивается во всем мире, но наиболее явно это происходит в Соединенных Штатах. Эта кампания реализуется совместно правительством, бизнесом и обычными гражданами. Мы все виновны. Приватности наносятся тысячи смертельных ран. Свободные общества поворачиваются спиной к вопросам приватности на свой страх и риск, ведь приватность – одно из фундаментальных прав, из которого происходят все остальные права человека:

- сама жизнь не может существовать без возможности предотвращать или сдерживать вторжения. Простейшие организмы используют клеточную оболочку для защиты своего тела от вторжений. Мы, люди, при защите своей неприкосновенности и приватности полагаемся на нашу кожу, наши дома, заборы и наше оружие;

- без приватности мышления – свободы, позволяющей нам формировать свое собственное мнение, и секретности, дающей нам возможность хранить наше мнение в тайне до тех пор, пока мы сами не решим высказать его, – не может существовать личность и индивидуальность;

- без приватности коммуникаций не может существовать политической жизни и в конечном счете нормальных взаимоотношений. Люди не смогут вести откровенных разговоров друг с другом, зная, что их слова слышит, а возможно, и записывает кто-то еще. Точно так же, как приватность личности является непреложным условием развития собственного «я», приватность в отношениях между людьми является непреложным требованием для создания длительных дружеских отношений.

Эти определения приватности могут показаться доведенными до абсурда аргументами, содержащимися в обсуждаемой в первой главе статье «Право на приватность». В конце XIX века Уоррен и Брэндис не могли представить, что технологии будут представлять опасность для приватности людей на таком фундаментальном уровне. Расстаться с нашей физической целостностью? Открыть свои мысли? Что за вздор! Более того, сегодня нашему праву быть свободными от вмешательств угрожают как террористы с оружием массового уничтожения, так и правительство, стремящееся найти и уничтожить этих террористов. Угроза нашему праву на тайну мыслей и переговоров исходит со стороны правительств, продавцов и неумолимой техногенизации нашей планеты. Наши личные истории лежат открытыми перед страховыми компаниями. Наши мысли однажды могут быть промоделированы или, скорее всего, украдены мощными компьютерами. Очень сложно, взглянув на любой сегмент экономики, *не найти* там новых агрессивных нарушений приватности личности.

Технология не нейтральна

Однажды на конференции я встретил студента МТИ. Со всей искренностью он заявил мне, что технология *нейтральна по отношению к приватности*. «Технологии могут использоваться для нарушения приватности, либо они могут использоваться для защиты приватности», – сказал он.

Этот студент из МТИ во многом напомнил мне себя самого: я говорил практически такие же вещи, когда был студентом этого института. Аргумент «технология нейтральна» очень удобен для людей, привыкших работать с самыми передовыми в мире технологиями. «Проблема не в технологии, – нравится нам думать, – проблема в способах использования этой технологии людьми!»

Тезис «технология нейтральна» очень удобный, но он неправильный. История полна примерами бесчеловечных проявлений технологий.²³⁸ Хотя и возможно использовать технологии для защиты и усиления приватности, тенденция технологического прогресса заключается в обратном. Сложнее, а зачастую и гораздо дороже создавать устройства и услуги, которые защищают приватность людей, чем уничтожать их.

²³⁸ Jacques Ellul, *The Technological Society* (New York: Random House, 1967).

Например, когда я учился на последнем курсе МТИ, институт получил очень дорогую электронную телефонную станцию 5ESS. В течение пяти лет цифровые ISDN-телефоны были установлены в институте повсюду. Каждый телефонный аппарат имел небольшой дисплей, более десятка кнопок, раза в два больше лампочек и встроенный микрофон для громкоговорящей связи. Когда я подробнее изучил устройство аппарата, я выяснил, что каждая кнопка и лампочка на нем являются «программными», т. е. любая кнопка и любая лампочка могут быть запрограммированы 5ESS на выполнение любой функции – это лишь вопрос программного обеспечения.

К сожалению, конструкция этих ISDN-телефонов позволяет использовать их в целях, для которых они никогда не были предназначены: установка жучков в офисах университетского городка. Роль жучка играет встроенный микрофон громкоговорящей связи. Обычно, когда вы делаете звонок, не поднимая трубки, красная лампочка рядом с микрофоном сигнализирует о том, что он включен. Но поскольку телефонный аппарат полностью управляется программой, включение микрофона и включение лампочки являются независимыми операциями. Путем перепрограммирования 5ESS можно включить микрофон, не включая световую индикацию. А между тем аппарат мог быть легко сконструирован по-другому, например, чтобы лампочка всегда загоралась при включении микрофона, безо всякого вмешательства со стороны 5ESS. Телефон не был сконструирован таким образом потому, что разработчики из AT & T не рассматривали обеспечение приватности как одну из основных целей разработки.

Существует и обратный пример. Это небольшая видеокамера, которой производитель компьютеров Silicon Graphics комплектует большинство своих настольных рабочих станций. Камера предназначена для организации видеоконференций, она установлена сверху на мониторе компьютера и направлена на пользователя. Обычно затвор камеры управляется программно: запустите программу, и камера начнет передавать видеоизображение. Остановите программу – и она остановится. Но эта камера имеет также и механический затвор – небольшую пластиковую шторку, которой можно закрыть объектив, заблокировав камере обзор. Конечно, камера с пластиковой шторкой более дорога в производстве, чем дешевые видеокамеры без механического блокирующего устройства. Но если вы сидите перед машиной и опустили шторку перед объективом, вы можете быть абсолютно уверены, что камера не в состоянии следить за вашими действиями. Эта шторка – дополнительный элемент конструкции, про который другие производители – увы! – предпочитают забывать.

Одной из проблем, присущих обеспечивающим приватность технологиям, является то, что очень сложно узнать, правильно ли работает технология. Если ваша приватность нарушена, вы можете заметить сигнализирующие об этом симптомы: непрошенная почта или надоедающие телефонные звонки. Вы можете обнаружить свою персональную информацию опубликованной в Интернете. Вы даже можете обнаружить скрытую видеокамеру у себя в спальне. Но нельзя с абсолютной уверенностью утверждать, что ваша приватность обеспечена. Более того, когда нарушение приватности обнаруживается и исправляется, обычно очень сложно узнать, внесены ли изменения технически корректным способом.

Технологии не являются нейтральными по отношению к приватности. Подавляющее большинство технологий нарушают приватность, это заложено в самой их природе. Развитие технологий позволяет более точно описывать, измерять и систематизировать мир вокруг нас. Оно позволяет нам создать глобальное хранилище информации, в котором очень легко осуществлять поиск. Технологии также позволяют осуществлять лучший контроль за недетерминированными процессами, такими как выбор человеком хлопьев на завтрак или политические выборы. Мы игнорируем эту тенденцию на свой страх и риск.

Повестка дня для правительства на XXI век по обеспечению приватности

Законотворчество и правовое регулирование могут стать одними из лучших методик защиты приватности в XXI веке, так же как в XX веке единственным эффективным способом

защиты окружающей среды стали законы и правовое регулирование. Если правительство не обеспечит защиту права на приватность личности, бизнесу очень легко (и очень выгодно) будет действовать не в наших интересах.

Тридцать лет назад Соединенные Штаты стояли на пути создания государственной системы защиты приватности. К сожалению, Уотергейт^[p71] и ошибки администрации Картера сбили нас с этого курса. В результате мы создали общество, в котором правительственные и бизнес-круги незаинтересованы и не имеют опыта в вопросах обеспечения приватности. Этот недостаток опыта заявляет о себе в первую очередь все возрастающим количеством вопиющих фактов нарушения приватности, которые мы наблюдаем в последние годы. Каждый раз, когда некоторые правительственные агентства или бизнесмены запускают новую программу или услугу, эта программа оказывает косвенное влияние на приватность. Когда общественность узнает об этом, неизменно разражается скандал, иногда сопровождаемый слушаниями в конгрессе или массовыми протестами потребителей. А мы, похоже, не извлекаем уроки из собственного опыта.

Гораздо более правильный подход заключается в создании постоянно действующего федерального контролирующего агентства, основной обязанностью которого стала бы защита приватности. Такое агентство могло бы:

- сдерживать правительство в его постоянном стремлении приносить приватность людей в жертву другим целям и осуществлять на правительственном уровне проверку новых федеральных программ на предмет возможных нарушений приватности до их реализации;
- претворять в жизнь немногочисленные существующие в США законы в области приватности;
- быть хранителем неприкосновенности и свободы личности в мире бизнеса; демонстрировать бизнесменам, как можно одновременно обеспечивать приватность и получать прибыль;
- быть омбудсменом^[p72] американской общественности, пытающимся обуздать самые худшие крайности, созданные нашим обществом.

Подсчитано, что создание такого агентства сегодня обойдется менее чем в 5 миллионов долларов – капля в федеральном бюджете.²³⁹

Некоторые активисты приватности высмеивают идею использования правительства для обеспечения гарантий приватности. Правительства, говорят они, повинны в самых крупных нарушениях приватности! Это правда, и именно по этой причине необходимо использовать законодательное решение. В конце концов правительство США было одним из самых крупных загрязнителей окружающей среды. Но это было до того, как конгресс принял множество законов по защите окружающей среды, заставившей правительство сделать свою деятельность более чистой. Законодательный подход эффективен, поскольку правительство США, как правило, выполняет свои законы. Сегодня правительство США является фактически национальной природоохранной полицией, одинаково внимательно контролирующей деятельность как частного бизнеса, так и самого правительства.

Правительства могут сделать чрезвычайно позитивные подвижки в области

p71

Уотергейт [Watergate] – политический скандал, в который оказалась вовлечена администрация республиканцев в 1973–1974 годах. Во время предвыборной кампании в помещении Демократической партии в отеле «Уотергейт» были задержаны взломщики, пытавшиеся установить подслушивающую аппаратуру. По данным некоторых источников они были связаны с комитетом по переизбранию на второй срок президента-республиканца Р. Никсона.

p72

Лицо, назначаемое правительством для разбора жалоб частных лиц на государственные структуры.

²³⁹ Прогноз Эвана Хендрикса [Evan Hendricks], председателя Совета по приватности США; издателя *Privacy Times*.

приватности. В частности правительства могут изменить разработку технологий, влияющих на приватность, как это уже сделано правительствами в Европе. Рассмотрим следующий аспект: все большее количество европейских компаний предлагают бесплатные телефонные звонки, предоставляемые после того, как вызывающий абонент прослушает короткую рекламу. Эта услуга экономит деньги потребителей, даже если представляется как мягкая форма промывания мозгов. Но эти услуги предоставляются по-разному. В Швеции рекламу вынуждены прослушивать как вызывающий, так и вызываемый абоненты, и новые рекламные объявления звучат прямо во время разговора. Однако в Италии омбудсмен по вопросам приватности постановил, что слушать рекламу должен только вызывающий, но не вызываемый абонент.²⁴⁰

В Соединенных Штатах имеет место мощная общественная поддержка мер государственного контроля, в частности, по таким ключевым вопросам, как защита медицинских данных. Например, проведенный в 1993 году Harris-Equifax опрос по вопросам обеспечения конфиденциальности медицинской информации показал, что 56 % американской общественности за «комплексный закон, устанавливающий режим конфиденциальности для индивидуальных медицинских данных» как часть общенациональной реформы законодательства в области здравоохранения. Среди сторонников нового федерального закона о конфиденциальности данных 96 % считают, что закон должен четко установить, кто может иметь доступ к медицинским данным; 96 % считают, что люди должны иметь право проверять свои медицинские данные и должна быть установлена процедура, позволяющая им корректировать и пополнять свои медицинские записи; 94 % опрошенных считают, что вся персональная медицинская информация должна быть отнесена к критичной, а 69 % – считают, что «должен быть создан независимый Национальный медицинский комитет по вопросам приватности [National Medical Privacy Board], который будет проводить слушания, издавать инструкции и претворять в жизнь стандарты».²⁴¹ Достаточно интересно, что 65 % главных администраторов медицинских учреждений, которым были заданы аналогичные вопросы, также высказались за федеральное регулирование.

Но даже без федеральной комиссии по приватности мы многое можем сделать.

Преобразование американского «Закона о точной отчетности по кредитам» в «Закон о защите данных»

«Закон о точной отчетности по кредитам» (FCRA) был хорошим законом для своего времени (1970), но он требует изменений. FCRA был написан в те времена, когда для принятия решения о кредитоспособности клиента использовался очень ограниченный набор данных. Сегодня в бизнесе решение о выдаче кредита принимается на базе гораздо более широкого спектра информации. Таким образом собирающие информацию о кредитоспособности потребителей фирмы вторгаются в области, про которые при написании FCRA никто и подумать не мог.

К сожалению, Федеральная комиссия по торговле и суды очень узко интерпретируют FCRA. Первое, что необходимо сделать, – это законодательно распространить действия FCRA на новые области.²⁴² А именно:

- фирмам, собирающим информацию о потребителях, необходимо запретить включение

²⁴⁰ John Tagliabue, «Europe Offering Free Calls, but First, a Word from...», *New York Times*, 28 сентября 1997, р. А1.

²⁴¹ Harris-Equifax, *Health Information Privacy Survey*, 1993.

²⁴² Кое-что из этого уже имеется в своде законов штата Калифорния, раздел CC1785.13-1785.26.

в отчет информацию об арестах, кроме случаев, когда человек действительно был признан виновным. Это необходимо потому, что не каждая запись об аресте указывает на виновность: множество арестованных людей никогда не оказываются в суде, поскольку их арестовывают по ошибке – полицейский намеревался арестовать кого-то другого. В других случаях полицейский арестовывает человека, но впоследствии его признают невиновным.

Невзирая на это, кредитор или потенциальный работодатель могут рассматривать арест как признак потенциальной вины. Если обвинение против человека снято или он признан в суде невиновным, собирающему информацию о потребителях агентству должно быть запрещено включать информацию об аресте или обвинении в отчет о потребителе;

- фирмам, собирающим информацию о потребителях, необходимо запретить сообщать информацию о лишении жилья в пользу домовладельца или кондоминиума, за исключением случаев, когда это произошло по решению суда и обе стороны (арендодатель и наниматель) согласны с тем, что этот факт может быть включен в отчет. Соображения аналогичны: арендодатели часто подают иск о выселении людей, являющихся хорошими арендаторами, но знающими свои права и пытающимися заставить домовладельцев исполнять свои законные обязанности;²⁴³

- американским компаниям необходимо запретить обмен медицинской информацией о конкретных клиентах или предоставлять медицинскую информацию как часть клиентского отчета без явного разрешения клиента. Разрешение должно быть получено на каждый отчет и должно указывать, какая конкретно информация будет передана и для каких целей она будет использована.

Нам также необходимо законодательно расширить базовые права, данные потребителям согласно FCRA. FCRA должен быть преобразован из закона, регулирующего сбор кредитной информации, в закон США о защите информации с широкими полномочиями. Вот некоторые ключевые элементы, которые должны быть включены в закон:

- когда в кредитное бюро сообщается негативная информация, ее поставщик обязан уведомить субъекта информации (т. е. потребителя) в письменной форме. В настоящее время потребители даже не знают о неблагоприятной информации в своих досье до тех пор, пока не получают отказ при поиске работы или намерении получить ипотечный кредит. На исправление или удаление ошибочной информации могут потребоваться недели, месяцы или даже годы;

- в случае совместной задолженности, например, в случае банкротства дебитора, за которого поручились, все стороны должны быть извещены до того, как негативная информация будет включена в отчет;

- закон должен быть уточнен, чтобы в случае, если собирающая информацию о кредитоспособности клиентов компания не исправляет ошибочные данные или они повторно появляются в отчетах после удаления, клиент мог подать иск о возмещении прямых убытков, уплате штрафа и оплате судебных издержек. Наказания должны быть прописаны в законе;

- потребитель должен быть извещен каждый раз, когда о нем запрашивается и отсылается информация. Уведомление должно включать причину предоставления отчета – в связи с рассмотрением заявления о приеме на работу, выдаче кредита или т. п.;

- потребители должны получать компенсации, когда их кредитная информация предоставляется кредитору или работодателю;

- люди должны иметь право знакомиться со всей собранной о них информацией. Эти отчеты должны предоставляться бесплатно и не реже одного раза в полгода;

- люди должны иметь право исправлять любую некорректную информацию в своих

²⁴³ В Калифорнии есть подобный закон, но он очевидно нарушает Первую поправку к Конституции США. См.: *UD Registry v. California*, 34 Cal. App. 4th 107 (1995). (Первая поправка ратифицирована 15 декабря 1791 года и гарантирует гражданские свободы. В частности, она запрещает принятие конгрессом законов, ограничивающих свободу слова, вероисповедания и т. п. – Примеч. перев.)

досье, будь то кредитные отчеты, медицинские записи, личные, деловые и другие данные. Если потребитель и фирма не могут прийти к общему мнению, то потребитель должен иметь право поместить в записи о себе *подробное* разъяснение спорного факта. Все больший интерес вызывают технологии сокрытия данных и другие методики, позволяющие людям работать с машиночитаемой информацией. Все шире используются штрих-коды, магнитные полоски, смарт-карты и машиночитаемые чипы. Люди должны иметь полное право знать, какие данные о них находятся в этих устройствах. И, по аналогии с кредитной информацией, люди должны иметь право корректировать эти данные, если они ошибочны.

Переосмысление разрешения

Разрешение является основой современного права. Чтобы дать разрешение, лицо должно достигнуть определенного возраста и быть вменяемым; человек в состоянии опьянения или недееспособный по другой причине не может дать юридически значимое разрешение. Но возможно, наиболее важно то, что человек должен быть четко проинформирован, на что именно он дает разрешение.

Разрешение превратилось в злую шутку. Медицинские учреждения и страховые компании требуют от пациентов подписания бланка разрешения, в котором просто написано: «Я даю вам разрешение делать с моей информацией что угодно и сколько угодно». Эти бланки зачастую подписываются под давлением обстоятельств, например в реанимации. В супермаркетах покупатели подписывают бланки на участие в дисконтных программах, до конца не понимая, что магазин будет делать с информацией об их покупках.

Разрешение – замечательная идея, но регулирующее его законодательство должно быть переписано с целью ограничения видов соглашений, которые можно заключать с потребителями. Соглашение должно стать больше похожим на улицу с двусторонним движением, когда запрашивающие разрешение организации формулируют условия четко и ясно. Всеобщие и бессрочные разрешения должны быть запрещены.

Важность компьютерной безопасности

В этой книге неоднократно поднимался вопрос о важности компьютерной безопасности для защиты информации и обеспечения приватности. К сожалению, требования к надежности и безопасности компьютеров зачастую упускаются из виду как производителями, так и пользователями компьютерных систем.

Например, в 1980-е годы Соединенные Штаты активно развивали сотовые и пейджинговые сети связи, хотя обе эти технологии были абсолютно незащищенными. Обе системы передавали информацию в эфир незашифрованной: при помощи радиоприемника любой мог перехватить сигнал и узнать содержимое сообщения. Вместо разворачивания безопасных систем производители пролоббировали закон, который просто запрещал прослушивание этих сигналов. Результат был предсказуем – десятки случаев, когда радиосигнал был подслушан.

Закон – важный элемент любого режима обеспечения приватности. Но сам по себе закон не может заменить базовые технические меры. Технологии и закон должны быть согласованными, чтобы сохранить свободу и обеспечить приватность. Для защиты приватной информации нам необходимы безопасные компьютеры и сети, соответствующие поставленной задаче.

Возвращение ОТА

В октябре 1972 года президент Ричард Никсон подписал документ 92-484 – «Закон о Бюро оценки технологий» [Office of Technology Assessment, ОТА]. Приняв закон, конгресс признал тот факт, что многие правительственные решения принимаются под воздействием

передовых технологий, но при этом технологии развиваются настолько быстро, что конгресс не успевает их отслеживать. Закон гласил:

Федеральные агентства, непосредственно подчиняющиеся конгрессу в настоящее время, не предназначены для предоставления законодательной ветви власти независимо от собранной адекватной и своевременной информации, касающейся потенциальных последствий технологических приложений. Имеющиеся в распоряжении конгресса механизмы не предназначены для предоставления законодательной власти такой информации.²⁴⁴

Согласно закону было создано независимое Бюро оценки технологий со следующими полномочиями.

1. Выявлять существующие и потенциальные последствия внедрения технологий и технологических программ.
2. По возможности устанавливать причинно-следственные связи.
3. Определять альтернативные технологические методы реализации определенных программ.
4. Определять альтернативные программы для достижения поставленных целей.
5. Осуществлять прогнозирование и сравнение последствий реализации альтернативных методов и программ.
6. Представлять результаты аналитических исследований соответствующим органам законодательной власти.
7. Определять сферы, в которых для осуществления прогнозов и оценок, перечисленных в параграфах 1–5, требуется проведение дополнительных исследований и сбор данных.
8. В соответствии с подразделом (d) осуществлять по поручению соответствующих уполномоченных органов сопутствующую деятельность.

ОТА не имело полномочий на создание законов и выпуск инструкций. Все, что оно могло, это публиковать отчеты по темам, которые конгресс попросил его изучить. ОТА выпустило отчеты по таким важным проблемам, как кислотные дожди, международное управление технологиями здравоохранения, пассивное курение на рабочем месте и мировые запасы нефти. В общей сложности ОТА опубликовало 741 отчет, когда в 1995 году оно было расформировано вновь избранным конгрессом, большинство в котором составляли республиканцы и который уничтожил свою возможность прогнозировать будущее в погоне за экономией 20 миллионов долларов в двухмиллиардном бюджете.

Я упоминаю здесь ОТА, поскольку ОТА, более чем любое другое федеральное агентство, было в высшей степени компетентно в вопросах влияния технологий на персональную приватность. Из 741 выпущенного ОТА отчета 175 касались вопросов приватности. Выпущенный в 1988 году отчет ОТА «Системы электронных данных и приватность личности» [*Electronic Record Systems and Individual Privacy*] непосредственно рассматривал многие вопросы, касающиеся банков данных (обсуждаемые во второй главе этой книги), и проводил параллели между приватностью и компьютерной безопасностью. ОТА рассматривало вопрос наблюдения за сотрудниками, как, например, в отчете «Электронный надсмотрщик: новые технологии, новая напряженность» [*The Electronic Supervisor: New Technology, New Tensions*]. Кроме того, ОТА обеспечивало компромисс между требованием выполнения закона и гражданскими свободами, в частности применительно к прослушиванию, наблюдению за базами данных и системам дистанционного наблюдения.

Это настоящая трагедия, что народ Соединенных Штатов позволил своим выборным представителям уничтожить ОТА. Любой серьезный план по обеспечению приватности в

²⁴⁴ Section 471 U.S. Code Title 2.

XXI веке должен включать в себя воссоздание этого национального достояния.

Купите вашу собственную приватность

Закон может лишь установить минимально необходимый уровень приватности, но люди, которые чувствуют себя некомфортно с этим уровнем – и которые имеют необходимые ресурсы, – всегда имели возможность купить для себя дополнительную приватность. Неудивительно, что люди, обладающие количеством денег выше среднего, нуждаются в повышенном уровне приватности. Таким образом идея покупки приватности является неким призывом к равноправию: те, кто нуждается в этом, как правило, могут себе это позволить.

В XXI веке криптографические средства, преобразующие информацию таким образом, что никто, кроме ее владельца и указанных им получателей, не сможет ее расшифровать, станут одним из основных путей, при помощи которых располагающие деньгами люди будут покупать себе приватность.

Точно так же, как существуют различные уровни конфиденциальности, существуют и различные виды криптографической защиты. Некоторые криптографические средства защищают информацию в момент ее передачи, но не информацию, которая уже дошла до места назначения. Другие криптографические средства защищают хранимую информацию. Различные области применения криптографии включают защиту деталей финансовых транзакций или сокрытие личности участников в электронных сообществах.

Одним из интересных средств обеспечения конфиденциальности является система Freedom,^[p73] разработанная канадской корпорацией Zero-Knowledge Systems.²⁴⁵ Система Freedom предназначена для анонимного просмотра страниц в Интернете, обмена электронной почтой и участия в конференциях Usenet (группах новостей). Система функционирует на базе специальных серверов, разбросанных по всему миру. Когда кто-либо хочет послать сообщение в Интернет, просмотреть web-страницу или принять участие в другой электронной транзакции, зашифрованное сообщение посылается с компьютера этого человека на один из серверов Freedom. Первый сервер пересылает сообщение на второй сервер, который в свою очередь пересылает его на третий, который наконец отправляет его по назначению. Каждое отправляемое сообщение зашифровано три раза, с последовательным использованием ключей серверов. Устройство системы не дает возможности человеку, перехватывающему сообщения (или имеющему контроль над одним из серверов Freedom), одновременно узнать и личность отправителя сообщения и содержимое сообщения.^[p74] Фактически Zero-Knowledge разместила серверы по всему миру, чтобы максимально затруднить для отдельно взятого правительства возможность изъятия содержимого всех трех серверов, задействованных в пересылке конкретного сообщения.

Как мы увидели на примере системы Freedom, криптография может быть мощным средством контроля над распространением персональной информации. Некоторые

p73

Freedom (англ.) – свобода.

245 Web-сайт Zero-Knowledge Systems находится в Интернете по адресу <http://www.zks.net>.

p74

Действительно, первый сервер знает личность отправителя (точнее, адрес его компьютера), но не имеет доступа к содержимому сообщения, которое после приема остается зашифрованным на ключах второго и третьего серверов. Второй сервер «снимает» второе шифрование, также не имея доступа к тексту и уже не зная отправителя сообщения, так как получает его не непосредственно, а от первого сервера. Наконец последний сервер получает после расшифрования исходное сообщение, но не имеет возможности получить информацию об отправителе.

преданные поклонники криптографии утверждают, что эта технология является панацеей в области приватности, решая практически все рассматриваемые в этой книге проблемы. Они говорят, что, используя криптографию, мир может более не опасаться подслушивания. Используя электронную наличность^[p75] для деперсонализации покупки информации, люди смогут читать энциклопедии или загружать порнографию полностью конфиденциально. В то же время цифровые подписи избавят нас от обмана и мошенничеств.

Эта аргументация имеет внутреннее противоречие, заключающееся в том, что криптография не обеспечивает приватность, она лишь защищает информацию. Сегодня многие банки и компании требуют от своих клиентов применения криптографических средств при пересылке финансовой информации через Интернет. Криптография гарантирует конфиденциальность этой пересылки. Но если прокурор постановит изъять эту информацию с web-сайта, находящегося на другом конце линии передачи, после чего обнародует названия приобретенных вами книг, ваша приватность все-таки будет нарушена, хотя сама по себе информация была надежно зашифрована во время передачи.

Криптография – чрезвычайно мощная технология, и будущее электронной экономики зависит от ее благоразумного использования. Но криптография сама по себе гарантирует нам приватность в будущем не больше, чем крепкие замки на дверях. Кроме того, криптография создает дополнительную нагрузку на пользователя. Человек, использующий систему Freedom, может, например, добровольно (или случайно) раскрыть свою настоящую личность в тексте сообщения. А поскольку криптография является лишь одним из средств обеспечения конфиденциальности, то чья-то конфиденциальность оказывается нарушенной и секрет разглашается, и уже никакая криптография не сможет восстановить конфиденциальность.

На протяжении всей этой книги я подразумевал, что криптография будет обязательной частью электронной реальности XXI века, но я не стал отвлекаться, чтобы написать об этом более подробно. Причина этого в том, что я неуютно чувствую себя с «шифропанковским»^[p76] видением электронного криптографического будущего. Защита приватности при помощи криптографии аналогична идее защиты приватности при помощи бумажных мешков. Конечно, люди в Нью-Йорке могут ходить с бумажными мешками на голове, чтобы их изображение не записывали видеокамеры, но это неприемлемо, например, в университетской среде.

Переломный момент

Мы находимся на очень опасной точке в эволюции приватности. На фоне того, что все больше и больше людей осознает важность приватности, правительства все меньше и меньше занимаются регулированием этой проблемы. Для состоятельных людей ничего не стоит обеспечить свою приватность собственными средствами. Но если правительство не будет этим заниматься и люди не будут обеспечены необходимым им уровнем приватности, кто-нибудь в конечном счете возьмет этот вопрос в свои руки.

Повсюду в мире мы видим результаты деятельности защитников приватности радикального толка. Эти люди преступают закон и социальные нормы, пытаясь привлечь внимание мировой общественности к проблеме приватности. Их нападки имеют целью придать гласности недостаток приватности и смехотворность правительственной политики ее обеспечения. Они пытаются кричать: «А король-то – голый!». Рассмотрим следующие

p75

Электронная наличность [digital cash] – термин, применяемый для обозначения «безликих» электронных денег. Обычный электронный платеж похож на чек, который идентифицирует плательщика, а электронная наличность является аналогом распространенных в реальном мире банкнот и монет.

p76

От англ. «сypher» – шифр и «punk» – панк.

события.

- В конце 1992 года в Северной Калифорнии была сформирована слабо организованная группа под названием Cypher-punks.²⁴⁶ Шифропанки посвятили себя распространению высоконадежного криптографического программного обеспечения и публичным нападкам на программное обеспечение, которое якобы обеспечивает приватность, а на самом деле не использует надежное шифрование.^[p77] За прошедшие годы шифропанкам приписывались многочисленные незаконные действия, включая незаконный экспорт из Соединенных Штатов криптографического программного обеспечения и публичное раскрытие ранее секретных алгоритмов шифрования. Список рассылки шифропанков использовался также для распространения информации об обнаруженных в коммерческом программном обеспечении ошибках в части безопасности, даже если распространение этой информации могло подвергнуть опасности финансовую информацию.

- Журналист Джеффри Ротфедер [Jeffrey Rothfeder] в своей книге «Приватность на продажу» [*Privacy for Sale*] решил, что наиболее эффективным способом демонстрации недостатка приватности был бы выбор наиболее ценящих свою приватность людей и публикация всего, что можно узнать об этом человеке.

«Я выбрал для проверки Дэна Ратера [Dan Rather], поскольку, как мне говорили, этот мужественный и молчаливый репортер CBS предпринял многочисленные меры для защиты своей персональной информации. С учетом этого он был наиболее подходящей кандидатурой для оценки масштабов [информационного] андеграунда».²⁴⁷

- Радикальные борцы за приватность появляются даже в средних школах. Когда администрация средней школы в Растоне, штат Луизиана, ввела обязательное ношение каждым учащимся идентификационной карточки учащегося, на которой были нанесены его имя, логотип Pepsi и штрих-код, учащиеся Рейчел Уинчел [Rachel Winchel] и Джонатан Вашингтон [Jonathan Washington] воспротивились этому. Они заявили, что штрих-код легко декодируется (он был основан на широкораспространенном алгоритме, известном под названием Code 39) и раскрывает номер социального страхования учащегося, что является нарушением Family Educational Rights and Privacy Act^[p78] 1974 года и Privacy Act^[p79] 1974 года.²⁴⁸ Ученики прошли по школе, показывая другим, как можно прочесть Code 39, после чего убедили своих товарищей вырезать штрих-код со своих карточек в знак протеста. Хотя

²⁴⁶ Simson Garfinkel, *PGP: Pretty Good Privacy* (Sebastopol: O'Reilly & Associates, 1995).

(Описание программы PGP на русском языке и освещение вопросов приватности в Интернете можно найти по адресу <http://www.geocities.com/SoHo/Studios/1059/pgp2x-ru-Volumel.html>. – *Примеч. перев.*)

^{p77}

Имеется в виду программное обеспечение, в котором из-за экспортных ограничений применяется урезанная длина ключа, и программы, в которых используются самодельные и никем не апробированные криптографические алгоритмы.

²⁴⁷ Rothfeder, *Privacy for Sale*.

^{p78}

Закон, гарантирующий конфиденциальность данных, связанных с обучением.

^{p79}

Закон об охране прав личности. Запрещает учреждениям разглашать информацию, касающуюся частных лиц, а также гарантирует этим лицам право на доступ к своей информации и ее корректировку.

²⁴⁸ David M. Bresnahan, «Tagged Students Defy Big Brother», *World Net Daily*, 23 сентября 1999. Доступно в Интернете по адресу http://www.worldnetdaily.com/bluesky_bresnahan/19990923_xex_tag-ged_stude.shtml.

администрация школы утверждала, что не нарушает закон и имеет право требовать носить карточки со штрих-кодами, 30 сентября 1999 года школьная администрация смягчилась и позволила учащимся убрать штрих-коды. Заглянув в будущее, легко себе представить борцов за приватность, повторяющих шаги других радикальных организаций, таких как бойцы группы экологического терроризма Earth First! и группа активистов борьбы со СПИДом АСТ UP!. Хотя эти активисты, несомненно, будут избегать официально зарегистрированных организаций по защите приватности, их действия, возможно, могут помочь добиться реальных изменений на политической арене. Уже сейчас некоторые защитники приватности потихоньку обсуждают необходимость создания подпольного фронта.

Этот подпольный фронт вряд ли нанесет ущерб своими действиями. Люди уже всю практикуют искажение информации, например при заполнении опросников для бесплатной подписки на журналы. Подпольные борцы за приватность могут лишь подлить масла в огонь, проводя кампании по убеждению людей переставлять цифры в своих номерах социального страхования, «случайно» делать ошибки в написании своих имен, т. е. глобально снижать качество информационного потока до тех пор, пока не будут приняты существенные меры по обеспечению приватности.

В последнее десятилетие большое количество групп, отстаивающих права гомосексуалистов, взяли на вооружение практику «утечек» – выставления политиков и бизнесменов как скрытых гомосексуалистов. Подпольные борцы за приватность могут воспользоваться «утечкой данных», т. е. публикацией имен, адресов, номеров домашних телефонов, номеров социального страхования, доходов и покупательских привычек людей, возглавляющих организации, активно нарушающие сегодня нашу приватность. Только представьте, как будет дергаться от телефонных звонков за обедом президент фирмы, специализирующейся на рекламе по телефону, или поток непрошеной почты в адрес главы компании, занимающейся прямым маркетингом!

Наконец, после этой точки может начаться информационный терроризм. В качестве протеста против практики недостаточного обеспечения приватности информационные террористы могут начать взламывать компьютеры и шифровать находящуюся в них информацию, либо они могут «освободить» корпоративные банки данных, организовав утечку информации из них в Интернет.

Хотя лично я полагаю, что право на приватность может быть обеспечено при помощи цивилизованного диалога и законодательных мер, а не информационного насилия, я опасаясь, что пострадавшие в конечном счете могут удариться в ярый активизм, использовать «утечки» и информационный терроризм, если все другие пути окажутся безнадежными.

Предсказание будущего всегда было рискованным делом. Существует слишком много непредвиденных обстоятельств, которые могут в корне изменить даже самое продуманное и правдоподобное предсказание того, что нас ждет впереди. Когда я был ребенком, моя мама кратко объясняла этот факт при помощи старинной еврейской поговорки: «Человек предполагает, а Бог располагает».^[p80]

Тем не менее предсказание будущего и строительство планов является для людей обязательным условием выживания. Тысячелетиями мы готовились к тяжелым зимним месяцам, сея семена весной и собирая урожай осенью. Мы планируем и создаем крупные гражданские объекты для предотвращения наводнений в сельской местности и обеспечения водой наших городов. Мы обучаем нашу молодежь, хотя отдача от этого не очевидна и возможна лишь в будущем. Кто не планирует будущее, не имеет ничего.

Уже более ста лет представление о приватности тесно переплетено с видением будущего. Когда Сэмюэль Уоррен и Луис Брэндис написали свою статью «Право на приватность», их главной заботой было не состояние приватности в Бостоне в 1890 году, но

потенциальные угрозы приватности в грядущем. Когда в 1947 году Джордж Оруэлл написал свой роман о Большом Брате, его волновало не состояние приватности в послевоенной Великобритании или России, а то, что может произойти с гражданскими свободами в какой-то момент в будущем, скажем, в 1984 году. Когда Алан Уэстин давал показания перед конгрессом в 1968 году, он подверг критике существовавшую в то время в кредитной индустрии США практику, но его наиболее серьезные предупреждения относились к тому, как пострадает наше будущее, если кредитная индустрия не будет поставлена на место.

Памятуя об этом, пять лет назад я взялся за написание книги о приватности в XXI веке. На первоначальном этапе я решил выбрать год в середине 100-летнего периода, год 2048. Частично это была игра, подсказанная Джорджем Оруэллом, но это также и веха на нашем пути в будущее. Сегодня само понятие «приватность» связано с множеством вопросов, которые, я думаю, обязательно будут решены к 2048 году. Сегодня многие проблемы с приватностью являются результатом использования технологий, базирующихся на неверных допущениях относительно приватности и свободы личности, которым сотни лет. Я убежден, что к середине XXI века этих допущений останется совсем мало. Человечество наконец лицом к лицу столкнется с проблемой абсолютной идентификации, дистанционного считывания, отслеживания, генной инженерии и угрозой со стороны искусственного интеллекта. Если к 2048 году человечество не позволит уничтожить себя одиночке-сумасшедшему или покорить сверхактивным полицейским силам, сказал я себе, то мы выйдем на новый уровень, который позволит нам выжить в следующие тысячелетия.

Но чем дольше я работал над книгой «2048», тем более ясным становилось, что меня больше всего должно заботить не какое-то устоявшееся футуристическое общество будущего. Моя борьба должна происходить здесь, в начале XXI столетия. Единственный способ преодолеть мост, отделяющий нас от некоего утопического будущего, заключается в том, чтобы начать принимать правильные решения уже сегодня.

Приватность действительно находится на распутье. Уже сегодня очень легко представить мир, в котором у нас будет отнята цифровая независимость, мир, где все наши действия отслеживаются, все наши секреты становятся известными и поэтому возможность выбора ограничена. Это мир, описанием которого я открыл свою книгу. Это мир, в котором я не желаю жить. Но единственный способ, при помощи которого мы сможем избежать такого антиутопического будущего, заключается в том, чтобы уже сегодня начать строить другое будущее.

Вместо создания нации баз данных мы должны изменить наше мышление, наши законы и наше общество. Мы должны построить свободное общество, которое уважает независимость и конфиденциальность личности. И мы должны начать прямо сейчас.

Эпилог Год спустя

Через год после того как эта книга увидела свет, приватность стала одним из ключевых вопросов, волнующих жителей Соединенных Штатов. Правительственные деятели и бизнесмены теперь осознают, что боязнь клиентов потерять контроль над своей персональной информацией является наиболее важным фактором, сдерживающим развитие электронной коммерции. Вопросы сохранности и обращения персональной информации стали одной из главных проблем в отношениях между Соединенными Штатами и Евросоюзом. В течение того года я получил сотни электронных писем от людей, чья приватность пострадала в результате действий компаний.

Большинство этих писем пришло от людей, ставших жертвами «кражи личности», описанной в главе 2. Оценки очень разнятся, но согласно им в 2000 году зарегистрировано от 500 до 750 тысяч различных случаев кражи личности. Кража личности стала настолько распространенным преступлением, что единичные случаи больше не привлекают внимание

прессы: ее внимание занимают промышляющие этим шайки – группы преступников, похищающие имена, номера социального страхования и кредитные истории одновременно десятков тысяч людей. Группы мошенников были обнаружены в Управлении социального страхования, подразделениях по работе с персоналом набирающий обороты фирм Силиконовой долины и даже в многонациональных телефонных компаниях. Например, правоохранительные органы обезвредили в Детройте шайку преступников, занимавшихся кражей личности, обманувших за 18 месяцев 1200 человек и похитивших более 2 миллионов долларов. Информация «уходила» непосредственно с компьютеров расположенной в Эдисоне, штат Техас, компании Aegis Communication, в которой работал один из членов шайки. Aegis^[p81] обрабатывает информацию о пользователях системы кредитных карт American Express; будучи похищенной, эта информация использовалась для получения поддельных карточек социального страхования, свидетельств о рождении, водительских прав и карт для банкоматов.²⁴⁹

Электронное письмо другого рода я получил от женщины, жившей в многоквартирном доме и начавшей нервничать, когда менеджер здания начал отпускать замечания по поводу одежды, которую она надевает на ночь. В конечном счете она обнаружила, что в ее спальне установлена скрытая видеокамера. Женщина обратилась в местную полицию, но там ей сказали, что это не нарушает закон об ограничении подслушивающих устройств, поскольку он касается лишь звукозаписывающей аппаратуры. Ей посоветовали просто найти новое жилье.

Атаки на приватность продолжаются

Это был тяжелый год для приватности. Когда в ноябре 1999 года эта книга вышла из печати, рекламное интернет-агентство Doubleclick как раз закончило процесс слияния с занимающейся маркетинговыми исследованиями фирмой Abacus Direct. Doubleclick планировало скомбинировать свою собственную базу данных по предпочтениям пользователей Интернета, – полученную путем обработки статистики посещения и регистрационных форм web-серверов, – с базой данных Abacus, содержащей имена, адреса и демографические сведения о потребителях. Сообщение об этом вызвало бурю протестов со стороны клиентов и групп по защите приватности, которые заявили, что планы Doubleclick резко увеличивают возможности корпораций по неправомерному использованию персональной информации, поскольку предоставляемая Doubleclick услуга позволит любому web-сайту получить имя, адрес и номер телефона практически любого человека, зашедшего на web-сайт или просмотревшего баннерную рекламу.

Мы стали свидетелями того, как многочисленные ошибки, недочеты в безопасности, просто небрежность и банкротства превратили радужные перспективы Интернета в информационное болото, в котором практически не оказывается внимания и уважения приватности личности. Рассмотрим следующие факты.

- Консультант по вопросам компьютерной безопасности Ричард Смит [Richard Smith], основатель и бывший президент Phar Lap Software, превратил поиск web-сайтов, нарушающих приватность, в некий вид домашнего бизнеса. Смит специализируется на анализе кода, используемого для создания web-страниц, с целью нахождения кода, передающего информацию между различными организациями. Например, в марте 2000 года Смит обнаружил, что web-сайт Intuit по неосторожности допускает передачу рекламодателям

p81

По иронии судьбы, «aegis» по-английски означает «эгида», «покровительство», «защита».

²⁴⁹ Martindale, Mike, «Feds shut down identity-theft ring: network stole credit cards, driver's licenses to ring up millions», *Detroit Morning News*, 26 апреля 2000. См.: <http://detnews.com/2000/metro/0004/26a01-44171.htm>.

информации, вводимой пользователями на странице финансового калькулятора.²⁵⁰ Эта утечка дает рекламодателю возможность узнать, что пользователь ищет возможность получить кредит в сумме 30 тысяч долларов на приобретение машины или 500 тысяч долларов на приобретение дома. Intuit заявила, что утечка данных была случайной и исправила ошибку сразу же, как только она была обнаружена.

• Несмотря на то что жалобы на непрошеную электронную почту являются самыми распространенными среди пользователей Интернета, компании, собирающие адреса электронной почты, не защищают их. Например, в марте 2000 года программная ошибка привела к тому, что Trans World Airlines разгласила электронные адреса 80 % подписчиков своего списка рассылки *Dot Com Deals*. В сентябре 2000 года компания DigitalConvergence столкнулась с проблемой в безопасности, приведшей к тому, что были разглашены имена и электронные адреса всех клиентов, установивших выпускаемый компанией сканер штрих-кодов и зарегистрировавших продукт. Компании заявили, что воспринимают происшедшее со всей серьезностью: «Мы сожалеем о причиненных неудобствах. Мы устранили проблему и приняли дополнительные меры предосторожности во избежание появления подобных проблем в дальнейшем», – сказал технический директор DigitalConvergence Дуг Дэвис [Doug Davis] в выпущенном компанией пресс-релизе.²⁵¹ Но если компании действительно воспринимают эти угрозы серьезно, они в первую очередь должны тратить больше времени и денег на проверку своих систем для предотвращения подобных проблем.

• Многие компании продолжают сталкиваться с хорошо подготовленными проникновениями в их банки данных с кредитными картами. В январе 2000 года хакер под псевдонимом Максус связался с онлайн-магазином CD Universe, заявив, что похитил 350 тысяч имен и номеров кредитных карт с web-сайта компании. Хакер запросил 100 тысяч долларов за возврат информации и в подтверждение серьезности своих слов опубликовал несколько тысяч имен и номеров в Интернете.²⁵² На Максуса началась облава, но результат был неутешительным. В марте 2000 года с web-сайта розничной торговли Salesgate.com было похищено около 20 тысяч записей о клиентах, включая номера кредитных карт и другую персональную информацию.²⁵³ В сентябре 2000 года Western Union сообщила о хищении с ее сайта подробной информации о кредитных картах 15 700 клиентов.

• Наконец, банкротство Интернет-магазина Toysmart.com показало, что так называемая «добровольная» политика защиты приватности просто не может ее защитить. Еще в то время, когда Toysmart.com была процветающей фирмой, она приобрела уважение многих клиентов, заявив, что никогда не продаст список своих клиентов – мера безопасности, очень важная для родителей малолетних детей. Но когда дело дошло до аукциона, Toysmart объявила, что на продажу выставляется все ее имущество, включая базу данных по клиентам.²⁵⁴ С предложением о приобретении списка выступила компания Disney – один из

²⁵⁰ Junnarkar, Sandeep, «Intuit plugs leak Doubleclick», CNET News.com, 2 марта 2000. См.: <http://news.cnet.com/news/0-1007-200-1562341.html>.

²⁵¹ «DigitalConvergence Experiences Electronic Security Breach», Digital Convergence, 15 сентября 2000. См.: <http://www.digitalconvergence.com/news/20000915.html>.

²⁵² Wolverton, Troy, «FBI probes extortion case at CD store», CNET News.com, 10 января 2000. См.: <http://news.cnet.com/news/0-1007-200-1519088.html>.

²⁵³ Borland, John, «E-commerce site breached by credit card thieves», CNET News.com, 1 марта 2000. См.: <http://news.cnet.com/news/0-1007-200-1562239.html>.

²⁵⁴ Farmer, Melanie Austria, «39 states object to sale of Toysmart's customer list», CNETNews.com, 21 июля 2000. См.: <http://news.cnet.com/news/0-1007-200-2307727.html>.

крупнейших инвесторов Toysmart. Лишь после того как Федеральная комиссия по торговле начала расследование, Toysmart смягчилась и пообещала, что продаст список своих клиентов только той компании, которая согласится следовать первоначальной политике Toysmart – маленький триумф борцов за приватность.

Где же ответ?

Неразбериха с приватностью продолжается, поскольку американский бизнес и правительственные круги испытывают нехватку формальных руководств и советов экспертов по методикам обеспечения надлежащего уровня защиты приватности. Такого нет в других странах. Например, после того как публичная библиотека Ванкувера (Британская Колумбия) установила сеть из 30 камер видеонаблюдения для предотвращения хищений и вандализма, специальный уполномоченный по вопросам приватности Британской Колумбии провел инспекцию здания. После он предоставил отчет, в котором показал, как сеть наблюдения может быть изменена, чтобы лучше выполнять свое предназначение по предотвращению краж и одновременно меньше нарушая приватность личности.²⁵⁵ Но, в отличие от Канады, Европы и Гонконга, Соединенным Штатам не достает как законодательных актов, устанавливающих минимальные стандарты обеспечения приватности, так и занимающихся регулированием этих вопросов агентств, которые могли бы консультировать компании и правительственные учреждения по вопросам создания приемлемой политики защиты приватности.

Конечно, правительство США продолжает настаивать на том, что нет необходимости в создании законодательных актов, всесторонне регламентирующих защиту приватности личности, поскольку вполне достаточно добровольно устанавливаемой политики, несмотря на тот факт, что Федеральная комиссия по торговле докладывала конгрессу США о неотложной необходимости принятия новых законодательных актов в области приватности.²⁵⁶

Вместо того чтобы сопротивляться принятию законодательных актов в области приватности, индустрия США должна сфокусироваться на разработке набора правил и методик по соблюдению приватности, которые были бы приемлемы как для Интернета, так и для обычной жизни. Эти методики должны учитывать как директиву Евросоюза о персональной информации [European Union's Directive on Personal Information], так и выпущенное ОЭСР в 1980 году Руководство по контролю над защитой приватности и перемещением через государственные границы персональных данных. (ОЭСР – Международная организация по экономическому сотрудничеству и развитию, объединяющая 29 стран-членов и занимающаяся обсуждением, развитием и работами по улучшению экономической и социальной политики.) В конце концов, американские компании ведут бизнес в Европе, Канаде и многих других странах, уже имеющих соответствующие законы в области приватности, базирующиеся на этих принципах. Эти компании лицемерят, когда говорят, что законодательные акты по защите приватности могут стать неприемлемой преградой их бизнесу.

История с MetroCard

Через день после того, как я начал свой «книжный тур»^[p82] с этой книгой, в

²⁵⁵ Подробности отчета можно найти по адресу <http://www.oip-cbc.org/investigations/reports/invrptl2.html>.

²⁵⁶ Mariano, Gwendolyn, «FTC to recommend stronger privacy legislation to Congress», CNET News.com, 22 мая 2000. См.: <http://news.cnet.com/news/0-1005-200-1926088.html>.

Нью-Йорке состоялось мое радиоинтервью репортеру «Голоса Америки» Ларри Фройнду [Larry Freund]. Фройнд передал мне опубликованную в *New York Post* статью, описывающую, как полиция Нью-Йорка получает доступ к данным из компьютеров системы метрополитена. Похоже, что администрация метрополитена [Metropolitan Transit Authority, МТА] запрограммировала компьютеры на запоминание времени и места каждого использования всех карточек MetroCard в городе. Полиция прослушала об этой базе данных и взяла за практику получать данные о проходе через турникеты метро задержанных ею людей: один звонок в управление метрополитена, и полиция получала подробную распечатку, с указанием всех станций метро, где была использована карточка задержанного.

Согласно статье из *Post*, полиция уже неоднократно пользовалась этой возможностью для опровержения алиби. В одном из случаев человек был задержан по подозрению в совершении кражи в магазине. Подозреваемый заявил, что не покидал Стейтен Айленд в день преступления, но, согласно данным компьютера, его MetroCard была использована через пять минут после совершения преступления на станции метро, находящейся рядом с магазином. Автор статьи в *Post* рассказывал еще о нескольких случаях, когда система опровергла алиби, и об одном случае, когда алиби было доказано (что заставило полицию искать другого подозреваемого).

Однако наибольшее беспокойство вызывало то, что статья в *Post* была написана совершенно спокойным тоном, без тени критики. Когда администрация метрополитена анонсировала внедрение новой системы MetroCard, она ничего не говорила гражданам Нью-Йорка о том, что устанавливает широкомасштабную систему слежки, которая будет запоминать маршруты их перемещений. Автор статьи не поинтересовался у МТА, кто имеет доступ к этой базе данных: только полиция или любой частный детектив, которому заплатил клиент? Что если служащий МТА захочет отследить перемещения своей подруги, чтобы узнать, не ездила ли она в Бронкс, на станцию подземки, находящуюся недалеко от квартиры ее бывшего приятеля? Есть ли какие-нибудь средства обнаружения несанкционированного просмотра базы? И конечно, автор статьи не акцентировал внимание на том, что система наблюдения на самом деле отслеживает не передвижение людей в системе метрополитена, — она отслеживает передвижение карточек.

Чтобы прояснить ситуацию, я позвонил в МТА. Менеджер по рекламе МТА был ошарашен моими вопросами: они не могли предоставить мне письменную копию инструкции, определяющей, что можно и что нельзя делать с информацией из системы MetroCard, поскольку этой инструкции не существовало. Правоохранительным органам доступ был предоставлен в порядке любезности; не существует формализованного процесса контроля и защиты гражданских прав, определяющего порядок предоставления полиции информации и какой именно информации. Служащим не разрешается просматривать записи в базе данных, но не принято никаких мер по предотвращению просмотра. С другой стороны, МТА создало систему, в которой люди могут получить доступ к своей информации: просто пошлите нам номер своей карточки MetroCard, сказали мне, и мы вышлем вам распечатку перечня станций, на которых вы были. Я думаю, что несомненно это существенно упрощает жизнь частным детективам и ревнивым супругам: все, что нужно сделать, это стащить ненадолго карточку — и все данные по ней будут доступны для запроса.

Взгляд за границу

Четыре месяца спустя после выхода в свет этой книги правительство Канады приняло всеобъемлющий пакет законов, защищающих право граждан на приватность. Названный С-6 и известный также под названием «Закон о защите персональной информации и электронных документах» [Personal Information Protection and Electronic Documents Act], этот законодательный акт устанавливает ряд правил, которые канадские компании обязаны

выполнять при сборе и обработке персональной информации. В настоящее время закон распространяется только на канадские компании, находящиеся под федеральным регулированием, такие как банки и страховые компании, но через три года действие закона будет распространено также и на компании, регулирование деятельности которых находится в ведении провинций.²⁵⁷

За последний год больше всего внимания было уделено вопросам обеспечения приватности в Интернете. Но канадский закон касается всей деятельности по сбору информации, независимо от того, онлайн она или нет. Именно так и должно быть, сказал член канадского парламента Джон Кэннис [John Cannis], один из авторов закона. Выступая этой весной непосредственно перед принятием закона, Кеннис, являющийся также парламентским секретарем министра промышленности, сказал:

Для того чтобы Канада смогла стать лидером в интеллектуальной экономике и электронной коммерции, потребители и бизнесмены должны спокойно чувствовать себя с новыми технологиями и влиянием, которое эти технологии будут оказывать на их жизнь. Канадцы хотят знать, что их сделки конфиденциальны и безопасны, что существуют правовые и финансовые схемы поддержки сделок и что информационная инфраструктура работает.²⁵⁸

Закон создает условия, в которых все канадские компании будут придерживаться одинаковых правил защиты персональной информации, говорит Кеннис:

Индустрия прямого маркетинга, IT-компании, телекоммуникационные компании, банки – все понимают, что Канаде необходима инфраструктура законов в области приватности. Они понимают также, что гибкое, но эффективное законодательство поможет потребителям перейти на электронные способы ведения бизнеса и будет для компаний менее затратным, чем самостоятельное создание правил.²⁵⁹

Положенные в основу C-6 принципы базируются на модельном стандарте приватности под названием «Свод правил по защите персональной информации» [Code for the Protection of Personal Information], который Канадская ассоциация стандартов [Canadian Standards Association, CSA] приняла в сентябре 1995 года. Свод правил обеспечения приватности CSA [CSA Privacy Code] стал для организаций пошаговой инструкцией по защите приватности личности. Эти шаги включают, в первую очередь, определение целей сбора информации, получение разрешения от людей, ограничение сбора, обеспечение точности и принятие адекватных мер против случайного разглашения (см. краткое изложение этих шагов в рамке).

Краткое изложение канадских принципов

Модельный «Свод правил по защите персональной информации», выпущенный Канадской ассоциацией стандартов, базируется на десяти независимых принципах.²⁶⁰

²⁵⁷ Копия текста закона C-6 может быть найдена по адресу http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/90052bE.html.

²⁵⁸ Speaking Примечания for John Cannis, M.P. (Scarborough Centre), Parliamentary Secretary to the Minister of Industry, Senate Amendments to Bill C-6, Check Against Delivery, February 14, 2000, Ottawa, Canada. См.: <http://www.ecom.ic.gc.ca/english/speeches/42d9.html>.

²⁵⁹ Ibid.

²⁶⁰ Выдержки из приложения к положениям C-6. Полный текст закона доступен по адресу

1. *Подотчетность.* Организация несет ответственность за находящуюся в ее ведении персональную информацию и должна назначить одного или нескольких сотрудников, отвечающих за выполнение организацией настоящих принципов.

2. *Определение целей.* Цели, с которыми осуществляется сбор персональной информации, должны быть определены до начала сбора информации.

3. *Разрешение.* Информирование человека и получение разрешения от него являются обязательными для сбора, использования или раскрытия персональной информации, за исключением случаев, когда это невозможно.

4. *Ограничение сбора.* Сбор персональной информации должен быть ограничен в соответствии с целями сбора, определенными организацией. Информация должна собираться честными и законными методами.

5. *Ограничения на использование, раскрытие и хранение.* Персональная информация не должна использоваться или раскрываться в целях, отличных от тех, для которых она собрана, кроме как по разрешению человека или в связи с требованиями закона. Персональная информация не должна храниться дольше, чем это необходимо для достижения заявленных целей.

6. *Точность.* Персональная информация должна быть настолько точной, полной и актуальной, насколько это необходимо для целей ее использования.

7. *Меры безопасности.* Персональная информация должна быть защищена при помощи мер безопасности, уровень которых соответствует уровню ее конфиденциальности.

8. *Открытость.* Организация должна предоставлять людям свободный доступ к информации о принятой в ней политике и методиках использования персональной информации.

9. *Обеспечение доступа.* По запросу, каждый человек должен быть проинформирован о существовании, использовании и раскрытии своей персональной информации, и ему должен быть предоставлен доступ к ней. Он должен иметь возможность оспорить точность и полноту информации, а также внести соответствующие поправки.

10. *Обработка жалоб.* Каждый человек должен иметь возможность направить ответственному сотруднику (или сотрудникам) организации жалобу по факту невыполнения изложенных принципов.

Свод правил обеспечения приватности CSA во многом похож по духу на Стандарт качества ISO 9001 Международной организации по стандартизации, ставший очень модным среди некоторых компаний США. Так же как ISO 9001, стандарт приватности CSA является добровольным. Канадские компании, которые желают следовать требованиям стандарта CSA, могут использовать его для усовершенствования служб по работе с клиентами и внутренних процессов. Они могут также объявить принципы взаимоотношений с общественностью. (Попытки Канады в 1997 году добиться принятия ее стандарта приватности ISO потерпели неудачу; эта деятельность в значительной степени блокировалась Соединенными Штатами.)

С-6 явился эффективным преобразованием свода правил в форму закона. Для «хороших корпоративных граждан», которые следовали этим принципам с 1995 года, изменения будут чисто номинальными, говорит специальный уполномоченный по вопросам информации и приватности провинции Онтарио Энн Кавукян [Ann Cavoukian]. По словам Кавукян, «хорошие корпоративные граждане» уже защищают приватность своих клиентов. Для компаний, которые ничего не делали, это повлечет огромный объем работ на начальном этапе: в первую очередь они должны будут обдумать основную цель сбора данных, а затем получить разрешение своих клиентов на использование этой информации в других целях.²⁶¹

Но воздействие С-6 на рядовых граждан Канады будет значительным. С-6 послужит

http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/90052bE.html.

²⁶¹ Из личной переписки (электронная почта), 28 апреля 2000.

выравниванию шансов канадских компаний, заставив их в конечном счете раскрыть, что они делают с персональной информацией своих клиентов. Компании, имеющие несоответствующие политику и процедуры, больше не смогут избегать общественного надзора, просто оставаясь в тени.

Пришло время и США обдумать аналогичное законодательство. Действующая в США политика обеспечения приватности клиентов практически целиком основывается на саморегулировании. Но этот подход работает, только если «часть компаний публично дает обязательство» защищать приватность, говорит Кавукян. Глядя через южную границу своей страны на Соединенные Штаты, она говорит: «Я не видела этого».

Это в наших руках

Уже более двадцати лет правительство Соединенных Штатов не имеет целостного законопроекта по защите приватности своих граждан. Такому плачевному положению дел существует масса объяснений, начиная от мощного воздействия бизнеса на политику и заканчивая отсутствием событий, которые заставили бы общественность сплотиться. Многие политологи связывают повышенный интерес Европы к вопросам приватности с преступлениями Гитлера, который использовал персональную информацию для поиска, изоляции и уничтожения евреев, либералов и политических врагов. К счастью, США не сталкивались с подобным.

Но настроения общественности меняются. Прошлым летом Федеральная комиссия по торговле опубликовала заявление, в котором говорится о том, что защита приватности потребителей при помощи самостоятельно создаваемых индустрией политики и правил оказалась неработоспособной и что для конгресса настало время принять всесторонний законодательный акт по этой проблеме. Это произошло в то время, когда комитет сената США по вопросам коммерции, науки и транспорта предложил не один, а целых три билля, которые должны были установить различные уровни защиты приватности в Интернете. Билль, определяющий некоторые аспекты приватности в Интернете, скорее всего, будет принят в ближайшее время.

Сегодня многие люди живут в двух мирах: в онлайн-мире и в реальной жизни. Но эта двойственность быстро разрушается. Всепроникающие технологии стирают многие традиционные отличия между онлайн-миром и оффлайн-миром, и взаимное проникновение двух миров происходит с огромной скоростью. Жизненно важно, чтобы правительство США приняло национальный закон о защите информации, который защищал бы всю персональную информацию как в Интернете, так и вне его. Однако в отсутствие такого закона конгресс должен, по крайней мере, обратиться к проблеме онлайн-приватности.

Есть только одна причина, по которой конгресс США наконец всерьез взялся за изучение проблемы приватности. Эта причина, конечно, протесты общественности. Каждый год происходит все больше и больше случаев кражи личности, в общественных местах появляются новые камеры наблюдения, еще более всеохватным становится наблюдение за нами властью имущих, все более глубоко проникающим становится мониторинг ненасытного бизнес-сообщества. И постепенно общественность начинает говорить: «Хватит!» Но если мы хотим видеть существенные подвижки нашего общества к лучшему, мы должны сделать так, чтобы наши голоса были услышаны: мы должны требовать обеспечения нашей приватности, и мы должны потребовать это прямо сейчас.

Где получить помощь

Ниже перечислены организации, которые могут помочь вам при решении проблем с приватностью и могут помочь сделать ваш голос услышанным.

Горячая линия по вопросам «кражи личности» Федеральной комиссии по торговле [Federal Trade Commission's Identity Theft Hotline]

С 1992 по 1997 год в Соединенных Штатах интенсивность краж личности возросла в 16 раз. За прошедшее время частота этого вида преступления подскочила еще больше. К концу 2000 года насчитывалось более 700 тысяч жертв кражи личности. Прошедшим летом Trans Union сообщила, что она получает по 3 тысячи звонков в день по поводу краж личности. Согласно прогнозу длительное время занимающегося вопросами защиты приватности Алана Уэстина, в ближайшие годы с проблемой кражи личности столкнется каждая четвертая семья. Но на горизонте не предвидится федерального законодательного акта, который мог бы существенно повлиять на корни проблемы: на простоту, с которой банки и занимающиеся кредитными картами компании выдают кредиты без идентификации личности, и на полное безрассудство, с которым эти компании отправляют ошибочные и вводящие в заблуждение отчеты агентствам, занимающимся сбором кредитной информации.

Недавно Федеральная комиссия по торговле создала горячую линию по вопросам кражи личности, которая собирает статистику по этой проблеме и старается помочь потребителям. Если вы стали жертвой кражи личности, пожалуйста, позвоните по этой горячей линии.

Federal Trade Commission's Identity Theft Hotline
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20 580
Voice: 877-IDTHEFT (438-4338)
TDD: 202-326-2502
<http://www.consumer.gov/idtheft>

Информационный центр электронной приватности [Electronic Privacy Information Center, EPIC]

С 1991 года Марк Ротенберг [Marc Rothenberg] и Информационный центр электронной приватности работают в Вашингтоне, федеральный округ Колумбия, чтобы защитить приватность нации в цифровую эпоху. Они свидетельствуют перед многочисленными комитетами и комиссиями о возрастающей угрозе нашей приватности; они успешно возбудили дело и заставили федеральное правительство предать гласности тысячи документов, описывающих планы посягательства на приватность всех американцев; они успешно организуют акции протеста потребителей против компаний вроде Lexis/Nexis и Intel. EPIC издает электронный информационный бюллетень и поддерживает web-сайт, являющийся поистине кладовой информации по вопросам приватности.

The Electronic Privacy Information center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009
Voice: 202-483-1140
Fax: 202-483-1248
E-mail: info@ecip.org
<http://www.epic.org>

Центр обмена информацией о праве на приватность [Privacy Rights Clearinghouse]

Располагающийся в Калифорнии и возглавляемый Бет Гивенс [Beth Givens] Privacy

Rights Clearinghouse обладает большим количеством информации для потребителей, столкнувшихся с нарушением приватности. В Центре функционирует горячая линия, по которой всегда готовы дать ответы на вопросы по таким темам, как домогательства на рабочем месте, преследования, искаженная информация и кредитные вопросы. Privacy Rights Clearinghouse обладает также обширными ресурсами для жертв кражи личности.

The Privacy Rights Clearinghouse
1717 Kettner Ave. Suite 105
San Diego, CA 92101
Voice: 619-298-3396
Fax: 619-298-5681
E-mail: prc@privacyrights.org
<http://www.privacyrights.org>

Фонд электронного фронта [Electronic Frontier Foundation, EFF]

Фонд электронного фронта изначально был основан как некая разновидность фонда по защите гражданских прав хакеров. Спустя годы после своего основания организация сосредоточилась на трех целях: сохранении свободы слова в онлайн-мире, защите цифровой приватности и обеспечении того, что новые технологии создаются с учетом «уважения человеческих прав, таких как свобода слова, приватность и справедливое использование». EFF — членская организация, которая стремится как обучать общественность, так и влиять на общественную политику.

Electronic Frontier Foundation
1550 Bryant Street, Suite 725
San Francisco CA 94103
Phone: 415-436-9333
Fax: 415-436-9993
E-mail: info@eff.org
<http://www.eff.org>

Аннотированный список использованных источников

Annas, George J. *Standard of Care: Laws of American Bioethics*. London, New York: Oxford University Press, 1993.

Написанная ведущим специалистом по биоэтике, *Standard of Care* исследует взаимодействие медицины, общества и законов путем изучения важных прецедентов в области биоэтики, закончившихся судебным разбирательством. Освещенные в этой книге вопросы включают аборты, СПИД, эвтаназию, трансплантацию органов и генетические исследования.

Bertillion, Alphonse (глава службы судебной идентификации [Judicial Identification Service] Франции). *Signaletic Instructions, Including the Theory and Practice of Anthropometrical Identification*. Перевод с последнего французского издания со 132 рисунками, иллюстрациями и таблицами. Под редакцией майора Р. В. Макклаффри [Major R. W. McClaghry], в прошлом главы полиции Чикаго. Chicago: The Werner Company, 1896.

В этой книге описана система идентификации Бертильона, первой биометрической системы идентификации, разработанной и внедренной в недавнее время.

Brin, David. *Earth*. New York: Bantam, 1990.

Брин описывает будущее Земли, в котором нет места приватности. Мир находится в состоянии политического кризиса и кризиса окружающей среды. Действие происходит в середине XXI века, где повсюду установлены видеокамеры, вся информация в мире легко доступна через информационную сеть, а стукачи используют самые разные пагубные

технологии. Превосходное чтение, хотя описание технологии и не совсем убедительно.

Brin, David. *The Transparent Society*. Reading, MA: Perseus Books, 1998.

Вместо того чтобы цепляться за иллюзию анонимности, Брин утверждает, что мы должны сфокусироваться на защите наиболее важной формы приватности и сохранить взаимную подконтрольность. Самая большая угроза нашей свободе, предупреждает Брин, заключается в том, что технологии будут использоваться не массово, а очень ограниченным кругом людей.

Burnham, David. *The Rise of the Computer State: A Chilling Account of the Computer's Threat to Society*. New York: Random House, 1983.

Книга Бернхама стала классической книгой о приватности и компьютерной безопасности 1980-х. В ней он рассказывает о возрастающей угрозе компьютерных служб слежения, кредитных агентств, служб отбора арендаторов и слежения за работниками. Печально, но большинство проблем, поднимаемых Бернхамом в книге, стало еще острее, а недостаток юридической защиты, о котором он сожалеет, стал наносить еще больший вред общественному устройству.

Calvin, William H. *Conversations with Neil's Brain: The Neural Nature of Thought and Language*. Reading: Addison-Wesley, 1994.

В этой книге подробно описывается современный уровень развития нейробиологии и микроанатомии, которые однажды сделают возможным прослушивание мозга.

Cavoukian, Ann, and Don Tapscott. *Who Knows? Safeguarding Your Privacy in a Networked World*. Toronto: Random House of Canada, 1995.

Написанная одним из специальных уполномоченных по защите данных Канады, эта книга является прекрасным пособием по защите информации в США и Канаде.

Cranor, Carl R, ed. *Are Genes Us? The Social Consequences of the New Genetics*. New Brunswick: Rutgers University Press, 1994.

Прекрасный учебник по генетике, со специальной главой о технологиях генетической идентификации.

Crevier, Daniel. *AI: The Tumultuous History of the Search for Artificial Intelligence*. New York: Basic Books, 1993.

Исчерпывающая история искусственного интеллекта, в которой особое место уделено буму и последующему спаду в исследованиях искусственного интеллекта в 1980-х.

Cummins, Harold, and Charles Midlo. *Finger Prints, Palms and Soles: An Introduction to the Dermatoglyphics*. Philadelphia: The Blakiston Company, 1943.

Учебное пособие по отпечаткам пальцев, написанное в середине XX века. Особенный интерес вызывает история отпечатков пальцев и обсуждение их генетической составляющей, замеченной еще до того, как была осознана генетическая природа наследственности.

Cushman, Robert E. *Civil Liberties in the United States: A Guide to Current Problems and Experience*. Ithaca: Cornell University Press, 1956.

Исследует современные проблемы гражданских свобод в Соединенных Штатах, уделяя особое внимание расовой и половой дискриминации, но оставляя за бортом проблемы приватности.

Eaton, Joseph W. *Card-Carrying Americans: Privacy, Security, and the National ID Card Debate*. Totowa: Rowman & Littlefield, 1986.

Итон утверждает, что Соединенные Штаты должны принять национальную систему идентификационных карт, чтобы исключить нелегальную иммиграцию и обеспечить подконтрольность людей, вносящих изменения в компьютерные данные. Карта должна содержать биометрическую информацию для опознания владельца. Но чего Итон не учел, так это широкого внедрения информационных сетей, особенно беспроводных сетей передачи данных, которые делают такие карты ненужными.

Etzioni, Amitai. *The Limits of Privacy*. New York: Basic Books, 1999.

В этой спорной книге Этциони утверждает, что у нас не недостаток, а переизбыток приватности. Если речь идет о тестировании на ВИЧ, реестре сексуальных преступников,

криптографии и идентификационных картах, Этциони утверждает, что право общества знать факты о своих членах перевешивает право отдельных личностей на приватность. Интересно, но единственная область, в которой, по мнению Этциони, приватность недостаточна – это медицинская информация. Но здесь, говорит Этциони, угроза исходит не от Большого Брата, а от Большого Бизнеса.

Finn, James, and Leonard R. Sussman, eds. *Today's American: How Free?* New York: Freedom House, 1986.

Эта книга представляет собой интересную подборку эссе, изучающих проблему свободы в современном обществе. Особого внимания заслуживает, написанная президентом Diebold Group Джоном Дайболдом [John Diebold] глава, изучающая влияние компьютеров на приватность и свободу.

Flaherty, David H. *Privacy in Colonial New England*. Charlottesville: University Press of Virginia, 1972.

В тезисах докторской диссертации Флаэрти рассматриваются истоки осмысления американцами приватности путем исследования состояния этого вопроса в Бостоне и других городах Новой Англии.

Garson, Barbara. *The Electronic Sweatshop: How Computers Are Transforming the Office of the Future into the Factory of the Past*. New York: Simon & Schuster, 1988.

В книге Гарсон изучается введение компьютеров и передовых телекоммуникационных технологий в деловую жизнь американцев в середине 1980-х. Она демонстрирует, что эти технологии, разработанные изначально для повышения производительности труда, быстро стали средством слежения за работниками, даже если такое слежение было неэффективным и даже приносило вред. Гарсон сопоставляет американский опыт с европейским, где приняты строгие законы, ограничивающие слежку за тем, какие кнопки нажимают служащие на компьютере.

Givens, Beth and the Privacy Rights Clearinghouse, with Dale Fetherling. *The Privacy Rights Handbook: How to take Control of Your Personal Information*. New York: Avon Books, 1997.

Книга Гивенс основана на теории и практике. Используя в качестве примера информацию, полученную от тысяч людей, обратившихся по горячей линии ее организации в Калифорнии, Гивенс объясняет, что движет компаниями, нарушающими нашу приватность и что с этим делать. Книга разделена на шесть частей, освещающих вопросы борьбы с агрессивной коммерцией; защиту персональных данных; подводные камни телекоммуникаций; приватность на работе; личную безопасность и активизм.

Lalonde, Peter, and Paul Lalonde. *The Mark of the Beast: Your Money, Computers, and the End of the World*. Eugene: Harvest House Publishers, 1994.

Лалонды рисуют апокалиптическую картину, навеянную Откровением о том, что глобальная экономика и нумерация жителей Земли специальными метками на руках и лбу приведут к концу света. Несмотря на то что он многими подвергается осмеянию, этот аргумент часто используется против глобальной переписи.

Long, Senator Edward V. *The Intruders: The Invasion of Privacy by Government and Industry*, with a Foreword by Vice President Hubert H. Humphrey. New York: Praeger, 1966.

Сенатор Эдвард Лонг возглавлял подкомитет сената США по нарушениям приватности. Книга подробно рассказывает о нарастающем стремлении к электронной слежке со стороны правительства и бизнеса в 60-х годах XX века. Очень подробно освещена тема мониторинга почты. Особенно интересен рассказ об проведенном Администрацией по контролю за продуктами и лекарствами прослушивании, которое осуществлялось с помощью электронного слежения с целью получения доказательств против продавцов не одобренных пищевых добавок, и Налоговом управлении, которое использовало прослушивание для поиска скрываемых доходов. Читателей также развлекут фотографии различных шпионских подслушивающих устройств, таких как оливка со встроенным микрофоном, пистолет, стреляющий дротиками с микрофонами и «шокер», который можно смонтировать на спине «молодой женщины», чтобы помочь в азартной игре.

Miller, Arthur R. *The Assault on Privacy: Computers, Data Banks, and Dossiers*. Ann Arbor: University of Michigan Press, 1970.

Прекрасная история политических интриг и событий, приведших к принятию «Закона о точной отчетности по кредитам».

Murphy, Paul L. *World War I and the Origin of Civil Liberties in the United States*. New York: W. W. Norton & Co., 1979.

Мерфи утверждает, что перед началом Первой мировой войны нарушения гражданских свобод были достаточно распространены, но с ними в известной степени мирились. Но во время войны было столько нарушений гражданских свобод и они были так широко распространены, что это привело к появлению движения американцев за гражданские свободы.

Orwell, George. 1984. New York: Harcourt Brace Jovanovich, 1949.

Спустя пятьдесят лет после публикации многие люди забыли, что обрисованная Джорджем Оруэллом классическая антиутопия не столько о приватности, сколько о тоталитаризме. Большой Брат управлял обществом на основе контроля прошлого и вселения страха в сердца в настоящем.

Русский перевод книги доступен на <http://lib.rus.ec/b/76207> (прим. составителя FB2)

Packard, Vance. *The Naked Society*. New York: David McKay Co., 1964.

Эта монументальная работа Паккарда посвящена приватности и слежке в 1960-х годах XX века. Паккард рассматривает атаки на приватность дома и на работе, со стороны правительства и бизнеса. Он рассматривает экономические и политические факторы, приведшие нас к новой эре тотальной слежки, и дает конкретные рекомендации о том, что должно быть сделано.

Philips, John Aristotle, and David Michaelis. *Mushroom: The Story of the A-bomb Kid*. New York Morrow, 1978.

Джон Аристотель Филипс был студентом, обнаружившим, что может создать подробный план изготовления атомной бомбы, пользуясь только общедоступными источниками. Он доказал, что «ядерные секреты» гораздо менее секретны, чем думают многие.

Ramberg, Bennett. *Nuclear Power Plants as Weapons for the Enemy: An Unrecognized Military Peril*. Berkley: University of California Press, 1984.

Рамберг демонстрирует, что для атомной катастрофы совсем не надо обладать ядерными секретами: все, что для этого нужно, это грузовик с взрывчаткой и ближайшая атомная электростанция.

Robin, Leonard. *Money Troubles: Legal Strategies to Cope with Your Debts*, 4th ed. Berkley: Nolo Press, 1996.

В книге обсуждается как получить кредитные отчеты и что делать с некорректной информацией в банках данных кредитных бюро.

Rosenberg, Jerry M. *The Death of Privacy*. New York: Random House, 1969.

Книга Розенберга рассказывает о влиянии электронной обработки данных на приватность личности в конце 1960-х годов. Это еще одна книга, призывающая к принятию Соединенными Штатами законов для защиты людей от сохранения в компьютерных банках данных неверной или неточной информации о них.

Rothfeder, Jeffrey. *Privacy for Sale: How Computerization has Made Everyone's Private Life an Open Secret*. New York: Simon & Schuster, 1992.

В 1990 году журналист Джеффри Ротфедер, работая в журнале *Business Week*, получил доступ к кредитному отчету вице-президента Дэна Куэйла [Dan Quayle]. После ухода из *Business Week* Ротфедер написал «Приватность на продажу», обзор вопросов приватности, в котором особое внимание уделено занимающимся сбором информации фирмам так называемым «супербюро». Эта книга стала известной частично еще и потому, что в нее включено подробное описание личной жизни журналиста Дэна Ратера [Dan Rather], описание, которое было составлено и опубликовано без разрешения мистера Ратера.

Schwartz, Paul, and Joel Reidenberg. *Data Protection law: A Study of United States Data Protection*. Dayton: Michie, 1996.

Пространный обзор законодательства в области защиты информации и распространенных в настоящее время в промышленности практик.

Smith, H. Jeff. *Hanging Privacy: Information Technology and Corporate America*. Chapel Hill: University of North Carolina Press, 1994.

Тезисы Смита из Гарвардской школы бизнеса являются исследованием того, как крупные корпорации США обрабатывают персональную информацию. По сути, это лишь общий обзор.

Smith, Robert E., and Eric Siegel. *War Stories: Accounts of Persons Victimized by Invasions of Privacy*. Available from *Privacy Journal* (P.O. Box 28577, Providence, RI 02908; 401-274-7861), 1994.

Описывается более 500 случаев нарушения приватности, в том числе нарушения в кредитных отчетах, медицинских данных, кражи личности, электронное наблюдение, использование Интернета, правительственную информацию, навязчивые предложения по телефону и многое другое. Опубликовано редактором *Privacy Journal*.

Smith, Robert E., and Eric Siegel. *War Stories II*. Available from *Privacy Journal* (P.O. Box 28577, Providence, RI 02908; 401-274-7861), 1997.

Описывает дополнительные случаи из *Privacy Journal*.

Stephenson, Neal. *Snow Crash*. New York: Bantam, 1992.

Роман Стивенсона переносит нас в начало XXI столетия, заполненное вездесущими видеокамерами, носимыми камерами, с напичканным жучками виртуальным окружением, повсеместной демократизацией деструктивных технологий и настоящим прослушиванием и контролем мозга. «Лавина» предсказывает появление многих технологий, обсуждаемых в этой книге, что в сочетании с живым изложением делает роман одновременно и приятным, и заставляющим задуматься.

Русский перевод книги доступен на <http://lib.rus.ec/b/54414> (прим. составителя FB2)

Turkington, Richard C, George B. Trubow, Anita L. Allen. *Privacy: Cases and Materials*. Houston: The John Marshall Publishing Co., 1992.

Серьезное учебное пособие для изучения истории и современного состояния законодательства в области приватности как в Интернет, так и вне его.

Twain, Mark. *Pudd'nhead Wilson: A Tale*. London: Chatto & Windus, 1894.

Новелла Твена познакомила многих американцев с идеей использования отпечатков пальцев для идентификации и расследования преступлений.

Русский перевод книги доступен на <http://lib.rus.ec/b/57097> (прим. составителя FB2)

Wayner, Peter. *Disappearing Cryptography*. Boston: AP Professional, 1996.

В книге Уэйнера изучается стеганография – техника сокрытия зашифрованных данных в других видах информации, чтобы скрыть сам факт наличия зашифрованных данных. Стеганография напрямую связана со скрытым маркированием и обеспечением законности.

Westin, Alan R, Project Director, Michael A. Baker, Assistant Project Director. *Databanks in a Free Society: Computers, Record-Keeping and Privacy*. New York: Quadrangle Books, 1972.

Книга представляет результаты проведенного National Research Council исследования развития электронных банков данных и их влияния на американское общество. Книга содержит подробный рассказ о компьютерах, работавших в федеральном правительстве, штатах, коммерческих организациях, учебных заведениях и других некоммерческих организациях в 1970–1971 годах. Читателям будет особенно интересно описание компьютеров Управления социального страхования, Национального центра информации о преступности ФБР [FBI's National Crime Information Center]; Bank of America; TRW's Credit Data Corporation; Управления почтовыми списками R. L. Polk and Company; Массачусетского технологического института и мормонской церкви. Книга также обобщает результаты посещения 55 передовых компьютерных систем, расположенных в Соединенных Штатах. Она прогнозирует будущие направления развития компьютерных технологий и

рассматривает влияние компьютеров на общественную политику. По соображениям обратной совместимости, многие системы в описанных Уэстином и его соавторами организациях продолжают функционировать и сегодня, что делает книгу актуальной и спустя 28 лет после ее публикации.

Wilson, Thomas R, and Paul L. Woodard. *Automated Fingerprint Identification Systems: Technology and Policy issues*. U.S. Department of Justice, Bureau of Justice Statistics, April 1987. Pub. No. NCJ-104342.

Этот отчет, резюмирующий впечатляющий успех систем AFIS, отмечает начало широкомасштабного принятия и внедрения AFIS-технологий в Соединенных Штатах.

Web-сайты

Следующие web-сайты помогут получить дополнительную информацию по вопросам, обсуждаемым в этой книге.

<http://www.chessclub.com>

Домашняя страница Шахматного клуба Интернета.

http://lists.essential.org/cgi-bin/listproc_search.cgi?listname=med-privacy

Архивы с механизмом поиска в электронном списке рассылки MED-PRIVACY, посвященном вопросам медицинской приватности.

<http://members.aol.com/victcrdrpt/index.html>

Домашняя страница «жертв кредитной отчетности». Этот web-сайт посвящен людям, пострадавшим от агентств, собирающих кредитную информацию. Содержит информацию о «Законе о точной отчетности по кредитам», методиках корректировки кредитных отчетов и некоторую предварительную информацию о методиках борьбы.

<http://www.american-adoption-cong.org>

Домашняя страница American Adoption Congress.

<http://www.atcc.org>

Домашняя страница American Type Culture Collection.

<http://www.ball.com/aerospace/index.html>

Домашняя страница Ball Aerospace, производящей спутники-наблюдатели QuickBird. Для более подробной информации о спутнике см.: <http://www.ball.com/aerospace/qbird.html>.

<http://www.consumer.gov/idtheft>

Домашняя страница горячей линии по вопросам кражи личности Федеральной комиссии по торговле.

<http://www.eds.dofn.de>

Домашняя страница Earth Observation Data Services. Содержит онлайн-хранилище с более чем 21 000 доступных для загрузки спутниковых изображений.

<http://www.epic.org>

Домашняя страница Информационного центра электронной приватности.

<http://www.eff.org>

Домашняя страница Фонда электронного фронта.

<http://www.loebner.net/Prizef/loebner-prize-bkup.html>

Домашняя страница проекта «Приз Лебнера», который достанется первому компьютеру, чьи ответы и поведение будут неотличимы от человеческого.

<http://www.nationalcpr.org>

Домашняя страница Национальной коалиции прав пациентов, некоммерческой организации, посвятившей себя идее, что пациенты имеют право на приватность, когда получают консультацию врача или другого специалиста в области здравоохранения. Организация считает, что ни работодателям, ни страховщикам, ни правительственным агентствам, ни полиции не должно быть позволено нарушать это базовое право.

<http://www.ncfa-usa.org>

Домашняя страница Национального совета по усыновлению.

Совет является некоммерческой организацией, предоставляющей информацию по внутреннему и международному усыновлению, поддерживающей развитие законодательства в области усыновления и предоставляющей ссылки на агентства-члены.

<http://www.nci.org/nci/index.htm>

Домашняя страница Института ядерного контроля. Основанный в 1981 году, институт стал исследовательским и пропагандистским центром по предотвращению распространения ядерного оружия. Являясь независимой некоммерческой организацией, институт играет роль защитника в сложной и опасной области.

<http://www.novaspace.com>

Домашняя страница NovaGraphics. Продает постер «Земля ночью» и другие, изготовленные при помощи изображений со спутников Landsat (800-727-NOVA).

<http://www.privacyrights.org>

Домашняя страница Privacy Rights Clearinghouse.

<http://spaceimage.com/index.htm>

Домашняя страница Space Imaging Corporation.

<http://www.spot.com>

Домашняя страница Spot Imaging.

<http://www.terraserver.com>

Домашняя страница TerraServer, на которой можно приобрести как спутниковые фотографии с американского спутника Landsat, так и спутников SPIN-2 советских времен. Изображения могут быть куплены и загружены с web-страницы; можно также заказать большие фотооттиски Kodak. Интуитивно-понятный интерфейс пользователя TerraServer дает возможность определить интересующую вас точку указанием адреса, координат или щелчком мыши на изображении земного шара.

<http://www.the-dma.org>

Домашняя страница Ассоциации прямого маркетинга США.

<http://www.worldsat.ca>

Домашняя страница WorldSat International, Inc, производителя самых сложных в мире постеров со спутниковыми изображениями, для создания которых требуются очень сложные расчеты (800-387-8177).

Благодарности

Впервые я официально столкнулся с вопросами приватности в 1986 году, когда слушал курс по науке, технологии и общественной политике у доктора Гэри Маркса [Dr. Gary Marx] в Массачусетском технологическом институте. Одной из изучаемых нами книг была книга Дэвида Бернхэма «Рассвет компьютерного государства: страшная правда об угрозе компьютеров обществу» [David Burnham, *The Rise of the Computer State: A Chilling Account of the Computer's Threat to Society*]. Несмотря на то что я более десяти лет был программистом и всегда с удовольствием работал с машинами, я знал о существовании некоторых компьютерных аспектов, которые легко могли быть использованы злонамеренно. Маркс и Бернхэм открыли мне глаза на масштабы этих проблем, и с тех пор оба играют важную роль в моем образовании.

В 1986 году я начал читать дайджест Питера Ньюмана [Peter G. Neumann] *RISKS* – форум, посвященный рискам, которым общество подвергается со стороны компьютерных и сопутствующих систем в Интернете. Добровольные помощники со всего мира присылали статьи для *RISKS*. Среди них были истории, анекдоты и наблюдения о том, как люди совершают тяжелейшие ошибки при внедрении и использовании компьютерных систем. В течение более десяти лет форум Питера был постоянным источником материалов, а его доброжелательность, остроумие и мудрость были источником вдохновения. После многих лет общения в сети я наконец получил шанс встретить Питера лично, и мы стали друзьями.

Когда однажды летом Питер побывал в на Мартас-Виньярд, [\[p83\]](#) он посмотрел несколько глав этой рукописи и дал мне очень ценные наставления – он даже приглашал меня на обед и в кино!

Стив Росс [Steve Ross] с факультета журналистики Колумбийского университета преподавал мне урок о том, что мало иметь хорошую историю, не менее важно хорошо ее написать. Стив также посоветовал мне не пытаться делать много за один присест. Когда мне нужно было написать тезисы на тему «Угроза номеров социального страхования», Стив обратил мое внимание на одну специфичную проблему с приватности – вред, наносимый службами по отбору нанимателей. Затем он научил меня, как можно продавать вариации одной и той же истории снова и снова в составе разных публикаций – очень полезный навык для любого, кто зарабатывает на жизнь писательством.

Роберт Эллис Смит [Robert Ellis] приобрел одну из статей, основанных на моих тезисах, и напечатал ее в *Privacy Journal*, который он неустанно издает уже более 25 лет. Когда я окончил школу журналистики, Боб всегда был рад приобрести все, что я писал на тему приватности. Он подвигнул меня изучить вопрос и написать о супербюро – системе автоматического распознавания отпечатков пальцев, системах генетической идентификации, проблемах медицинской приватности и «прогрессе» в торговле. Выпускаемый Бобом ежемесячный информационный бюллетень, его подборку «военных историй» и его многочисленные книги об угрозах приватности необходимо прочесть каждому, кто интересуется угрозой приватности. Боб также способствовал организации Privacy Summit, проходящей каждые полгода встречи активистов приватности. Он является «электростанцией», питающей приватность.

Материалы Марка Ротенберга [Marc Rotenberg], Дэвида Банисара [David Banisar] и Дэвида Собеля [David Sobel] из Информационного центра электронной приватности были авторитетным источником, из которого я мог цитировать информацию, касающуюся угроз приватности со стороны правительств и большого бизнеса. Выдвинутый ЕРІС в соответствии с «Законом о свободе информации» [\[p84\]](#) судебный иск против ФБР и других правительственных организаций извлек на свет огромное количество информации о планах правительства принести приватность в жертву сразу на двух алтарях: укрепления законности и национальной безопасности. Марк, в частности, оказался крупным специалистом в вопросах теории приватности, его голос в пользу законодательства по защите приватности является одним из самых мощных в Вашингтоне (и, хотя это несколько неловко говорить, он имеет склонность к антиправительственным либертарианским настроениям, как и многие сторонники киберправ). Он также стал для меня «путеводной звездой приватности», разъясняя мне проблемы, по которым мы были не согласны. Почти всегда Марку удавалось убедить меня в моих ошибках.

Фил Эгр был аспирантом в Лаборатории искусственного интеллекта Массачусетского технологического института, когда я учился в этом институте. С тех пор он стал профессором в UCLA, где специализируется на проблемах приватности. Публикации и выступления Фила о технологиях, укрепляющих приватность, социальной теории и роли бизнеса оказали неоценимую помощь в формировании многих моих убеждений, изложенных в этой книге. Фил также сделал ценные критические замечания по многим моим книгам, темам и статьям.

Многие прочитанные мною книги включают длинный список людей, с которыми автор общался во время работы над книгой. Мне всегда было интересно читать этот раздел и

p83

Мартас-Виньярд – остров недалеко от Бостона, штат Массачусетс.

p84

Freedom of Information Act (FOIA) году. Вступил в силу в 1967 году. Согласно закону, все федеральные ведомства обязаны обеспечивать свободный доступ граждан ко всей информации, которой они располагают.

находить в нем знакомые имена, но мне было грустно смотреть на неизвестные мне имена. Чем занимаются эти люди? Откуда автор знает их? Чем они ему помогли?

За пять лет работы над этой книгой я беседовал с несколькими сотнями людей. Они отвечали на мои вопросы, на мою электронную почту и выкраивали в своем плотном расписании время, чтобы поговорить со мной. Каждый из них внес большой вклад в конечный результат. Хотя я не решаюсь перечислить их всех из-за боязни пропустить кого-либо, я хотел бы выразить особую благодарность:

- Ами Брукману [Ami Bruckman], разработавшему искусственные миры MediaMoo и MooseCrossing в Лаборатории медиа Массачусетского технологического института [MIT Media Laboratory] и работающему в Комитете приватности MIT [MIT Privacy Committee],

- Рэму Аврахами [Ram Avrahami], который попытался сразиться с индустрией прямого маркетинга и проиграл,

- Джону Берджесу [John Burgess], служащему отдела информации посольства США в Лондоне, который уделил мне время и рассказал о видеокамерах в Великобритании,

- Джейсону Кэтлиту [Jason Catlett], основателю Junkbusters,

- Дороти Деннинг [Dorothy Denning], профессору Джорджтаунского университета [Georgetown University], специалисту в области шифрования,

- Дэну Эллису [Dan Ellis], которого я знал как аспиранта Лаборатории медиа, и который всегда интересовался проблемами приватности,

- Карлу Эллисону [Carl Ellison], экстраординарному криптографу, работающему в настоящее время в Intel,

- Майклу Фрумкину [Michael Froomkin], одному из самых известных в США адвокатов в области интернет-права, который в настоящее время преподает в университете Майами во Флориде,

- Роберту Джелману [Robert Gellman], эксперту-аналитику по вопросам приватности, консультирующему в Вашингтоне, федеральный округ Колумбия,

- Джону Гилмору [John Gilmore], основателю Electronic Frontier Foundation и настоящему знатоку криптографии, еще одному человеку, который убежден, что сильная криптография является решением многих проблем приватности,

- Бет Гивенс [Beth Givens], руководителю проекта Privacy Rights Clearinghouse из Калифорнии,

- Дженлори Голдману [Janlori Goldman], который занимался проблемами приватности, работая в ACLU, EFF и CDT,

- Ламонту Грэнквисту [Lamont Granquist], действительно выдающемуся компьютерному специалисту, обитающему в Вашингтонском университете в Сиэтле,

- Майклу Гранту [Michael Grant], моему дорогому другу, который очень интересуется проблемами приватности и который рассказал мне много интересных историй,

- Эвану Хендриксу [Evan Hendricks], издателю информационного бюллетеня *Privacy Times* из Вашингтона, федеральный округ Колумбия,

- Эрику Хьюзу [Eric Hughes], одному из истинных киберпанков, который всегда убеждал меня, что только хорошая криптография может сохранить свободу и независимость личности,

- Джеймсу Колстрому [James Kallstrom], возглавлявшему офис ФБР в Нью-Йорке и убедившему меня в том, что он действительно заботится о гражданских свободах,

- Стиву Манну [Steve Mann], которого я знал как аспиранта Лаборатории медиа и который знаменит тем, что расхаживает повсюду с видеокамерой на голове,

- Клиффорду Мейеру [Clifford M. Meyer], менеджеру по коммуникациям в магистратуре общественных отношений Вашингтонского университета, который помог мне обосноваться в Сиэтле и организовать там группу по изучению технологий и демократии [Technology and Democracy Study Group],

- Джону Оруэнту [Jon Orwant], еще одному аспиранту Лаборатории медиа, проделавшему фундаментальный труд по моделированию пользователей, до того как он стал

издателем журнала,

- Дамселу Плюму [Damsel Plum], *not de plume* [p85] координатора публикаций *Bastard Nation*,
- Памеле Самюэльсон [Pamela Samuelson], эксперту в области авторского и интеллектуального права,
- С. Б. Роджерсу-мл. [C. B. Rogers, Jr.], главному администратору Equifax,
- ПитеруТарши-Хорночу [Peter Tarczy-Hornoch], детскому неонатологу, который уделил мне время в Сиэтле, чтобы рассказать о медицинской информатике, медицинской приватности и других не менее важных проблемах,
- Брэду Темплтону [Brad Templeton], старожилу Интернета, который всегда интересовался взаимодействием технологии и политики,
- Брюсу Уайлдеру [Bruce Wilder], врачу из Питтсбурга, взявшему на себя труд по сокрытию медицинской информации от страховщиков,
- Россу Степлтону-Грею [Ross Stapleton-Gray], рассказавшему мне о своем опыте в роли объекта Internet Hunt и продолжавшему затем работать со мной в большом количестве других проектов.

Часть этой книги была написана весной 1997 года, когда я стажировался в Вашингтонском университете в Сиэтле. Профессор Алан Борнинг [Alan Borning] с факультета компьютерных наук устроил меня на должность; Марго Гордон [Margo Gordon] разместила меня. Вашингтонский университет – одно из самых любимых мною учебных заведений в мире. У него исключительно живописный университетский городок, большое количество студентов и впечатляющий выбор курсов. Будучи там, я смог в полной мере воспользоваться библиотечной системой университета, особенно библиотекой Suzzallo and Allen и Odegaard Undergraduate. Я посетил множество дневных и вечерних лекций; студенты, бывшие там весной 1997 года, могут увидеть прямую связь между некоторыми главами этой книги и событиями в университете в тот период. Многие преподаватели весьма великодушно уделяли мне время; интервью с ними вошли в эту книгу. Я также получал помощь от очень эффективной службы общественной информации университета. Во время пребывания в этом университете мне было позволено присутствовать на занятиях по медицинской информатике на медицинском факультете UW, за что я также очень благодарен. Факультет общественных отношений также был очень великодушен, предоставив мне помещение для вечерних встреч созданной мной дискуссионной группы Technology and Democracy Study Group; многие из изложенных в этой книге идей впервые прозвучали там.

Фрагменты рукописи этой книги прочитали Хал Абельсон [Hal Abelson], Ами Брукман, Джейсон Кэтлитом, Ришаб Айер Гош [Rishab Aiyer Ghosh], Шин Грэмэтс [Sian Gramates], Эван Хендрикс, Бернард Гринберг [Bernard Greenberg], Эндрю Листфилд [Andrew Listfield], Марк Ротенберг, Джин Спаффорд [Gene Spafford] и Хал Варьян [Hal Varian]. Все они дали очень ценные комментарии и советы. Как и все остальные свои книги, O'Reilly пропустило данную рукопись через процесс формального рецензирования. Эта прекрасная практика редко встречается сегодня в издательском мире. Алекса Чемпион [Alexa Champion], Шин Грэмэтс, Оскар Ганди [Oscar Gandy], Бернард Гринберг и Марк Ротенберг прочитали эту рукопись полностью и дали множество полезных рекомендаций, сделавших конечный продукт гораздо лучше. Особенно ценными были комментарии Марка: часто единственное замечание заставляло меня переделывать целые страницы!

Работая над этой книгой, я очень зависел от онлайн-услуги доступа к энциклопедии «Британика». У меня никогда не было денег, чтобы купить полный комплект «Британики», но платя 5 долларов в месяц за онлайн-доступ, мне это было и не нужно. Когда я только начал работу над книгой, Британика взимала 14,95 доллара в месяц и не имела на своем сайте опубликованных положений о приватности. Сегодня у них есть

положение, в котором жирными буквами написано: «Британика не продает, не сдает в аренду, не использует для обмена и не раскрывает каким-либо другим образом персональную информацию». Далее политика подробно объясняет, какая именно информация накапливается на web-сайте, как используются «ключики»^[p86] и для каких целей «персональная информация» используется внутри организации. Это очень впечатляющее положение, и мне приятно думать, что я в некотором роде способствовал его появлению, поинтересовавшись в 1997 году, почему на web-сайте отсутствует такое уведомление. Мораль этой истории в том, что организации можно обучить правильным вещам.

Те вещи, которые я не мог отыскать в «Британике» или на просторах Паутины, были найдены моим верным исследователем Джейн Станкавейдж [Jayne Stancavage]. Джейн гораздо более быстрый работник, чем я, и я боюсь, что она часто неделями размышляла, не забросил ли я проект. Конечно, я этого не сделал, она, к счастью, тоже.

Моя работа над книгой то начиналась, то прерывалась с 1989 года, но серьезно я занялся ею с 1995 года. Дебби Рассел [Debby Russel] из O'Reilly знала о проекте все эти годы, и в 1998 году решила отредактировать и опубликовать книгу. Именно благодаря ей эта книга появилась на свет. Эта книга отмечает 10-летний юбилей нашей совместной деятельности с Дебби; это шестая книга, которую мы сделали вместе.

Ханна Дайер [Hanna Dyer] создала замечательную обложку для этой книги; Алисия Сеч [Alicia Cech] сделала большую работу по внутреннему дизайну; Эди Фридман [Edie Freedman] и вся дизайнерская группа O'Reilly сделали прекрасную и творческую работу, создав методом мозгового штурма общий дизайн книги. Майкл Сноу [Michael Snow] делал фотомонтаж в Adobe Photoshop, Эди Фридман придумал замочную скважину, а Джон Фейнгерш [John Feingersh] из Stock Market сделал фотографию глаза. Для издания в мягкой обложке Мелани Уэнг [Melani Wang] придумала дополнительные элементы на базе оригинального внутреннего дизайна, и Эмма Коулби [Emma Colby] создала обложку.

Крис Рейли проделал огромную работу, иллюстрируя эту книгу, особенно если учесть качество некоторых исходных материалов. Сара Уиндж [Sara Winge], Кэти Рекорд [Cathy Record] и Марк Брокеринг [Mark Brokering] провели огромную работу по предыздательскому маркетингу этой нетрадиционной для O'Reilly книги – будем надеяться, что их старания окупятся!

Производственный редактор Мэдлейн Ньюелл [Madelein Newell] обнаружила буквально тысячи опечаток и неточностей и милостиво дала нам с Дебби время их исправить. Анна Ким Сноу [Anna Kim Snow], Коллин Горман [Colleen Gorman], Дэвид Футато [David Futato], Джефф Холкомб [Jeff Holcomb], Нэнси Коутри [Nancy Kotery] и Абби Майерс [Abby Mayers] осуществили неоценимый контроль качества и производственную поддержку. Рейчел Уэллер [Rachel Wheller] осуществляла контроль качества и производственную поддержку для данного издания в мягкой обложке. Майк Сьерра [Mike Sierra] реализовал внутренний дизайн с использованием Adobe FrameMaker 5.5. Роберт Романо [Robert Romano] помог организовать размещение иллюстраций. Эллен Трутман Цайг [Ellen Troutman Zaig] составила индекс. Дэн Эплман [Dan Appleman] подверг эту рукопись тщательной проверке в процессе издания и, к счастью, не нашел никаких накладок.

Наконец, я хотел бы поблагодарить моего агента Лью Гримса [Lew Grimes], который поддерживал этот проект в течение долгих пяти лет, и мою жену Бет Розенберг [Beth Rosenberg], чья любовь, поддержка, понимание и мудрость давали мне силы и время для работы над этим произведением.

Кембридж, Массачусетс, и Мартас-Виньярд

p86

Cookies (англ.) – переменные, записываемые web-сервером в браузер клиента для сохранения некоторых промежуточных данных: имени пользователя, даты последнего посещения, идентификатора текущего сеанса и др.

октябрь 1999 декабрь 2000

От переводчика

Симсон Гарфинкель как автор одновременно и сложен, и легок в переводе. Очень ясное и иллюстративное изложение делает перевод приятным занятием. С другой стороны, разносторонние интересы и глубокие познания автора в различных отраслях требуют изучения дополнительных материалов для адекватного перевода.

Самым сложным оказалось перевести вынесенное в англоязычное название книги слово «privacy». Это очень емкое понятие, и в русском языке отсутствует единственное слово, которое в одиночку могло бы передать все грани смысла понятия «privacy». «Приватность», «секретность», «личная тайна», «право побыть одному», «независимость» – далеко не полный список вариантов, из которых приходилось выбирать в каждом конкретном контексте. Искренне надеюсь, что мне удалось правильно передать оттенки смысла.

Насколько актуальна книга С. Гарфинкеля для России? На первый взгляд может показаться, что рассматриваемые в ней проблемы нас мало касаются – наша жизнь еще не настолько связана с компьютерами и современными технологиями. Но именно поэтому нам необходимо осознать существование описываемых в книге проблем и попытаться не допустить их возникновения. США *уже создали* «нацию баз данных», мы же *пока стоим на пороге* ее создания. В чем-то мы уже начали повторять ошибки американцев: история создания и развития Social Security Numbers (SSN) невольно вызывает аналогию с введением ИНН. Наверное, не стоит делать своих ошибок – лучше учесть чужие. Я хочу поблагодарить всех, без кого работа по переводу этой замечательной книги была бы очень сложной. Наталья Головина терпеливо объясняла мне встречавшиеся в книге специальные термины из области психологии и помогала подобрать их адекватный перевод. К Павлу Покровскому всегда можно было обратиться с вопросами по химии и биологии, а также получить помощь в выборе более благозвучного варианта перевода. С Дмитрием Леоновым и Антоном Чувакиным всегда можно было обсудить перевод сложных фраз и получить ценную страноведческую информацию. Этот список далеко неполный, не буду перечислять всех, чтобы кого-нибудь не пропустить. И конечно, особая благодарность моей семье за понимание и поддержку – во время работы я общался с близкими гораздо меньше, чем с компьютером.

Владислав Мяснянкин