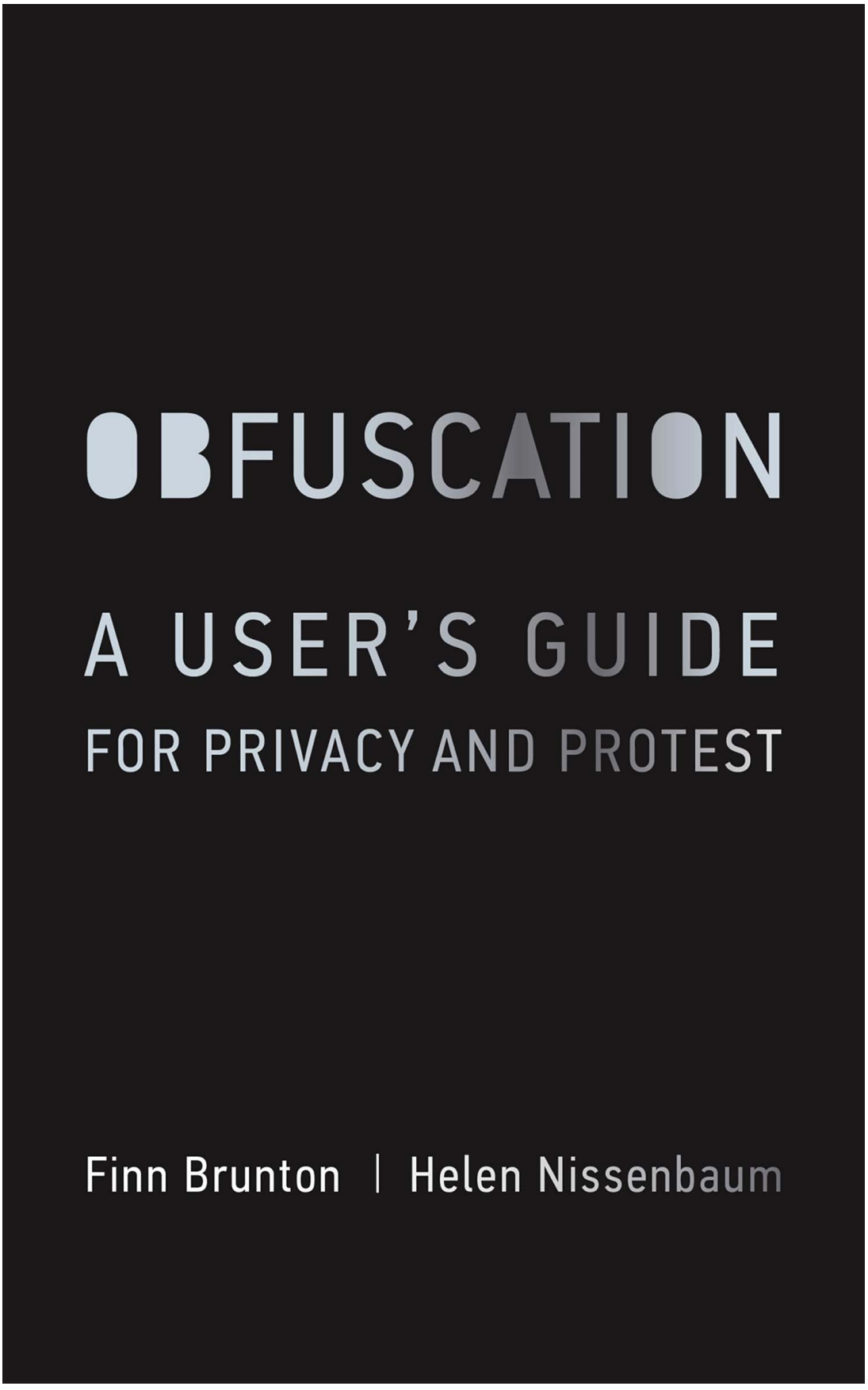
Обфускация. Руководство пользователя по приватности и протесту

Полный русский перевод книги об обфускации как практическом средстве защиты приватности и гражданского протеста: от ложных сигналов и информационного шума до этических ограничений, моделей угроз и оценки эффективности.

Больше крутых материалов в моём телеграм канале @grogrigs

Обфускация. Руководство пользователя по приватности и протесту



Обфускация. Руководство пользователя по приватности и протесту. Финн Брантон и Хелен Ниссенбаум

Обфускация

Руководство пользователя по приватности и протесту

Финн Брантон
Хелен Ниссенбаум

The MIT Press
Кембридж, Массачусетс
Лондон, Англия

Набор гарнитурой PF Din Text Cond Pro выполнен компанией Toppan Best-set Premedia Limited. Напечатано и переплетено в Соединённых Штатах Америки.

Данные каталогизации издания Библиотекой Конгресса доступны.

ISBN: 978-0-262-02973-5

10 9 8 7 6 5 4 3 2 1

Благодарности

Эта книга началась с технологии - проекта TrackMeNot, - и мы выражаем глубочайшую благодарность Дэниелу Хоу, который поставил его на ноги, и Венсану Тубиана, который присоединился к работе, расширил её масштаб и по сей день неустанно поддерживает проект и его пользователей. Отзывы и комментарии сообщества пользователей и сообщества специалистов по приватности в целом, а также совместная техническая статья с Лакшминараянаном Субраманьяном (Венсан Тубиана, Лакшминараянан Субраманьян и Хелен Ниссенбаум, «TrackMeNot: Enhancing the Privacy of Web Search») открыли нам глаза на его возможности и ограничения. Позднее создание и запуск второй системы, AdNauseam, совместно с Дэниелом Хоу и в сотрудничестве с дизайнером Мушоном Зер-Авивом ещё больше расширили наше представление об обфускации и о необходимости глубже и систематичнее осмыслить то, что она предлагает как метод и стратегию.

Когда мы начали работать над общим пониманием обфускации, нам удалось исследовать многие из этих понятий в статье, опубликованной в First Monday, и в главе сборника Privacy, Due Process and the Computational Turn; обе работы чрезвычайно выиграли от рецензий и редакторских отзывов, полученных на этих площадках.

Обфускация превратилась в книгу благодаря поддержке и обстоятельным советам рецензентов, а также Маргерит Эйвери, Гиты Манакталы, Сьюзен Бакли, Кэти Хелке и Пола Бетге из MIT Press. Мы благодарим их всех. Эмили Голдшер-Даймонд провела скрупулёзную работу в качестве ассистента-исследователя, а также организовала многие другие стороны этого проекта. Работа над всеми вариантами рукописи книги велась при поддержке грантов Национального научного фонда (ITR-0331542: Sensitive Information in a Wired World), программы EAGER (CNS-1355398: Values in Design for Future Internet Architecture - Next Phase), Управления научных исследований Военно-воздушных сил США (MURI-ONR BAA 07-036: Collaborative Policies and Assured Information Sharing) и Научно-технологического центра Intel по социальным вычислениям. Поддержка по этим грантам предоставила время, технологии и коллегиальную среду, необходимые для работы над проектом и его успешного завершения.

Два крупных события помогли сформировать и уточнить наши представления об обфускации. Первым был Симпозиум по обфускации (15 февраля 2014 года), совместно организованный факультетом медиа, культуры и коммуникации Нью-Йоркского университета и Институтом информационного права при совместной поддержке Научно-технологического центра Intel по социальным вычислениям. За то, что это событие стало возможным, мы хотели бы поблагодарить Николь Арцт, Эмили Голдшер-Даймонд, Дав Хелену Педлоски, Мелиссу Лукас-Людвиг, Эрику Роблес-Андерсон и Джейми Шулер - и прежде всего Седу Гюрсес, которая в значительной мере организовала, структурировала и сформировала программу этого дня. Каждый без исключения докладчик непосредственно повлиял на нашу рукопись. Вторым событием стал продолжающийся диалог в Исследовательской группе по приватности Нью-Йоркского университета, на еженедельных семинарах которой мы представляли этот материал на нескольких этапах работы. Без обсуждений в PRG книга не обрела бы своей окончательной формы; мы с теплотой благодарим всех участников.

Другие возможности представить и проверить отдельные стороны этой работы также оказались чрезвычайно плодотворными, а отклики сторонников, критиков, убеждённых приверженцев и скептиков значительно улучшили наши идеи. В число таких мероприятий вошли совместный коллоквиум Центра гражданских медиа MIT и программы сравнительных исследований медиа; конференция аспирантов Новой школы социальных исследований 2014 года; New Media Salon в Тель-Авиве; кафедральный семинар по коммуникациям и журналистике Еврейского университета в Иерусалиме; научно-исследовательские лаборатории IBM в Хайфе; Центр искусства и технологий Eyebeam; HotPETS 2013; конференция Computers, Privacy and Data Protection в Брюсселе; а также конференция по исследованиям наблюдения в Университете Куинс.

Мы глубоко благодарны друзьям и коллегам, с которыми могли обсуждать обфускацию по мере развития этой идеи и которые делились отзывами, критическими замечаниями, поддержкой и новыми мыслями. В особенности мы хотели бы поблагодарить Джулию Энгвин, Солона Барокаса, дану бойд, Клаудию Диас, Синтию Дворк, Кэти Дуайер, Тарлтона Гиллеспи, Мирей Хилдебрандт, Ари Джуелса, Ника Монтфорта, Дейдре Маллиган, Арвинда Нараянана, Мартейна ван Оттерло, Айру Рубинштейна, Иэна Спиро, Люка Старка, Кэтрин Стрэндберг, Мэтью Тирни, Джо Туроу, Джанет Вертези, Тала Зарски, Мальте Цивица и Итана Цукермана.

Наконец, эта книга не появилась бы без поддержки нашего профессионального дома - факультета медиа, культуры и коммуникации Нью-Йоркского университета. Спасибо вам всем!

Введение

Этой книгой мы намерены начать революцию. Но не большую революцию - по крайней мере, не сразу. Наша революция не опирается на масштабные реформы, на всеобъемлющее переустройство общества с «нулевого года» или на беспрепятственное и совершенно единообразное принятие новой технологии. Она строится из уже существующих компонентов - того, что философ назвал бы подручными средствами, а инженер - серийным оборудованием, - доступных в повседневной жизни, в кино, в программах, в детективах и даже в животном мире. Хотя её словарь методов могут использовать и уже использовали тираны, авторитарные правители и тайная полиция, наша революция особенно хорошо подходит малым игрокам, незаметным людям, тем, кто оказался в тупике, кто не может отказаться, выйти из системы или установить контроль над исходящими от него данными. Наша ограниченная революция сосредоточена на ослаблении и преодолении современной цифровой слежки. Мы добавим новые понятия и приёмы к существующему и расширяющемуся набору средств уклонения, неподчинения, прямого отказа, намеренного саботажа и использования на наших собственных условиях. В зависимости от противника, целей и ресурсов мы предлагаем методы исчезновения, затягивания времени и затруднения анализа, озорного неповиновения, коллективного протеста, больших и малых действий по индивидуальному восстановлению справедливости. Мы очерчиваем целую область как уже сложившихся, так и новых случаев, объединённых общим подходом, который можно обобщить и воплотить в правилах, программах и действиях. Этот контур служит знаменем нашей большой маленькой революции, а обозначенное им пространство называется обфускацией.

Если выразить одним предложением: обфускация - это намеренное добавление двусмысленной, запутывающей или вводящей в заблуждение информации, чтобы помешать наблюдению и сбору данных. Это простая вещь со множеством разных и сложных способов применения. Если вы разработчик или проектировщик программного обеспечения, встроенная в программу обфускация способна защитить данные пользователей - даже от вас самих или от того, кто приобретёт ваш стартап, - пока вы предоставляете социальную сеть, геолокацию или другие службы, требующие сбора и использования личной информации. Обфускация также позволяет государственным учреждениям достигать многих целей сбора данных, сводя к минимуму возможность злоупотреблений. А если вы человек или группа, желающие жить в современном мире, не становясь субъектом повсеместной цифровой слежки (и объектом последующего анализа), обфускация предлагает словарь способов насыпать немного песка в шестерёнки, выиграть время и спрятаться в толпе сигналов. Эта книга даёт отправную точку.

В ходе нашего проекта мы проследили примечательные сходства между совершенно разными областями, где те, кто вынужден оставаться видимым, читаемым или слышимым, отвечали на это, погребая значимые сигналы в облаках и слоях вводящих в заблуждение сигналов. Увлечённые разнообразием обстоятельств, в которых действующие лица обращаются к стратегии обфускации, мы представили в главах 1 и 2 десятки подробных случаев, объединённых этой общей нитью. Эти две главы, составляющие часть I книги, служат путеводителем по разнообразным формам и форматам, которые принимала обфускация, и показывают, как такие случаи проектируют и воплощают с учётом конкретных целей и противников. В социальной сети, за покерным столом или в небе во время Второй мировой войны; перед лицом системы распознавания лиц, правительства апартеида в Южной Африке 1980-х годов или сидящего напротив соперника - правильно применённая обфускация способна помочь защитить приватность и противостоять сбору данных, наблюдению и анализу. Сам размах ситуаций и способов применения, рассмотренных в главах 1 и 2, вдохновляет и подталкивает задать вопрос: какую работу обфускация может выполнить для вас?

Случаи из главы 1 выстроены в повествование, которое знакомит с основными вопросами об обфускации и описывает важные подходы к ней, а затем исследует и обсуждает их в части II книги.

В главе 2 более короткие случаи иллюстрируют широту и разнообразие применений обфускации, одновременно закрепляя лежащие в их основе понятия.

Главы 3-5 углубляют понимание обфускации: в них рассматривается, почему обфускация играет определённую роль в разных способах защиты приватности; какие этические, общественные и политические проблемы порождает применение обфускационных тактик; и как оценить, работает ли или способна ли работать обфускация в конкретных ситуациях. Чтобы оценить действенность того или иного подхода к обфускации, необходимо понять, чем обфускация отличается от других средств, а также разобраться в её особых слабых и сильных сторонах. Названия глав 3-5 сформулированы как вопросы.

Первый вопрос, поставленный в главе 3: «Почему обфускация необходима?» Отвечая на него, мы объясняем, почему полезность обфускации позволяет решать проблемы современной цифровой приватности. Мы показываем, как обфускация может противодействовать информационной асимметрии, которая возникает, когда данные о нас собирают в обстоятельствах, которых мы можем не понимать, ради целей, которых мы можем не понимать, а затем используют способами, которых мы можем не понимать. Нашими данными будут делиться, их будут покупать, продавать, обрабатывать, анализировать и применять, и всё это будет иметь последствия для нашей жизни. Получите ли вы кредит или квартиру, на которые подали заявку? Насколько велик связанный с вами страховой или кредитный риск? Что определяет показываемую вам рекламу? Откуда столь многие компании и службы знают, что вы беременны, боретесь с зависимостью или собираетесь сменить работу? Почему разным когортам, разным группам населения и разным районам выделяют разные объёмы ресурсов? Попадёте ли вы, как гласит зловещая фраза нынешней эпохи антитеррористической деятельности на основе данных, «в список»? Даже безобидная или кажущаяся благожелательной работа в этой области имеет последствия, заслуживающие внимания. Обфускация играет свою роль не как замена государственному управлению, деловой практике или технологическим мерам и не как универсальное решение (повторим: это намеренно малая, распределённая революция), а как средство, входящее в более широкую сеть практик защиты приватности. В частности, это средство особенно хорошо подходит людям, которым в данный момент или вообще недоступны другие способы защиты своих прав, - людям, которые, как бывает, не могут применять оптимально настроенные средства защиты приватности, поскольку находятся на слабой стороне конкретных отношений между информацией и властью.

Контекст сходным образом формирует этические и политические вопросы, связанные с обфускацией. Применение обфускации во множестве областей - от социальной политики и социальных сетей до личной деятельности - вызывает серьёзные опасения. В главе 4 мы спрашиваем: «Оправдана ли обфускация?» Не побуждаем ли мы людей лгать, намеренно сообщать неточные сведения или «загрязнять» потенциально опасным шумом базы данных, используемые в коммерческих и общественных целях? Не пользуются ли обфускаторы коммерческими услугами за чужой счёт, полагаясь на добросовестность честных пользователей, которые платят за таргетированную рекламу (и за сами услуги), предоставляя данные о себе? И если такие практики станут широко распространены, не будем ли мы все вместе напрасно расходовать вычислительные мощности и пропускную способность? В главе 4 мы отвечаем на эти возражения и описываем нравственный и политический расчёт, по которому конкретные случаи обфускации можно оценить и признать приемлемыми или неприемлемыми.

В центре главы 5 находится вопрос о том, чего обфускация может и не может достичь. По сравнению с криптографией обфускация может показаться зависящей от обстоятельств и даже ненадёжной. В криптографии точную степень защищённости от атак полным перебором можно вычислить с учётом длины ключа, вычислительной мощности, времени и других факторов. Для обфускации такая точность возможна редко, поскольку её сила как практического средства зависит от того, чего хотят добиться пользователи и с какими конкретными препятствиями они могут столкнуться в соответствующих обстоятельствах применения. Однако сложность не означает

хаоса, и успех всё равно требует внимательного отношения к систематическим взаимозависимостям. В главе 5 мы выделяем шесть распространённых целей проекта обфускации и связываем их с параметрами проектирования. Среди этих целей - выигрыш времени, предоставление прикрытия, возможность отрицать причастность, уклонение от наблюдения, противодействие профилированию и выражение протеста. К выделенным нами сторонам проектирования относится то, является ли проект обфускации индивидуальным или коллективным, известным или неизвестным, избирательным или общим, краткосрочным или долгосрочным. Например, для некоторых целей обфускация может не сработать, если противник знает о её применении; для других целей - таких как коллективный протест или подрыв достаточных оснований и создание возможности правдоподобно отрицать причастность - лучше, чтобы противник знал о загрязнении данных. Всё это, разумеется, зависит от доступных противнику ресурсов, то есть от того, сколько времени, сил, внимания и денег он готов потратить на выявление и отсеивание обфусцирующей информации. Логика этих взаимосвязей обнадёживает, поскольку позволяет предположить, что рассуждения о конкретных случаях помогут нам совершенствовать обфускацию с учётом её назначения. Будет ли обфускация работать? Да - но только в контексте.

Начнём.

Часть I. Словарь обфускации

Существует множество стратегий обфускации. Их определяют цели пользователя (которые могут простираться от выигрыша нескольких минут до постоянного противодействия системе профилирования), то, действуют ли пользователи поодиночке или сообща, цель и те, кто получит пользу, характер обфусцируемой информации и другие параметры, которые мы обсудим в части II. (Части I и II можно читать независимо друг от друга - если у вас есть вопросы о целях обфускации, этических и политических затруднениях или обстоятельствах, которые, по нашему мнению, делают обфускацию полезным дополнением к набору средств защиты приватности, смело переходите вперёд.) Однако прежде мы хотим, чтобы вы поняли, как множество конкретных обстоятельств применения обфускации можно свести к общей закономерности. Мы можем объединить под одним заголовком целое семейство на первый взгляд разрозненных событий, выявить лежащую в их основе преемственность и показать, как сходные методы можно применять в других контекстах и к другим проблемам. Обфускация зависит от обстоятельств: её формируют проблемы, которые мы стремимся решить, и противники, которых мы надеемся обмануть или задержать, однако для неё характерно простое основополагающее условие: не имея возможности отказаться от наблюдения или воспрепятствовать ему, мы создаём множество правдоподобных, неоднозначных и вводящих в заблуждение сигналов, среди которых может затеряться информация, которую мы хотим скрыть.

Чтобы показать обфускацию с тех сторон, которые наиболее важны для её нынешнего применения и развития, и дать материал для обращения на протяжении остальной книги, мы выбрали ряд основных случаев, наглядно демонстрирующих, как работает обфускация и на что она способна. Эти случаи организованы тематически. Хотя они не укладываются в простую типологию, мы расположили их так, чтобы по мере чтения становились ясны различные варианты выбора, присущие обфускации. Помимо этих случаев мы представляем набор кратких примеров, иллюстрирующих некоторые другие способы применения обфускации и некоторые более необычные контексты. Благодаря этим случаям и объяснениям вы получите указатель по обфускации во всех областях, где мы с ней сталкивались. Обфускация - положительная и отрицательная, эффективная и неэффективная, целенаправленная и неизбирательная, естественная и искусственная, аналоговая и цифровая - возникает во многих областях и во многих формах.

Глава 1. Основные случаи

1.1. Дипольные отражатели: как победить военный радар

Во время Второй мировой войны оператор радара следит за самолётом над Гамбургом и наводит прожекторы и зенитные орудия по фосфорной точке, положение которой обновляется с каждым проходом антенны. Внезапно точки, которые как будто обозначают самолёты, начинают множиться и быстро заполняют весь экран. Настоящий самолёт находится где-то среди них, но определить его местоположение невозможно из-за присутствия «ложных эхо-сигналов».[1]

Самолёт выбросил дипольные отражатели - полоски чёрной бумаги с подложкой из алюминиевой фольги, нарезанные до половины длины волны радара-цели. Их выбрасывают фунтами, и, медленно опускаясь в воздухе, они заполняют экран радара сигналами. Дипольные отражатели в точности соответствуют параметрам данных, на поиск которых настроен радар, и дают ему больше «самолётов», рассеянных по всему небу, чем он способен обработать.

Вполне возможно, это самый чистый и простой пример обфускационного подхода. Поскольку обнаружение настоящего самолёта было неизбежным (в то время сделать самолёт невидимым для радара было невозможно), дипольные отражатели создавали слишком много потенциальных целей и тем самым исчерпывали ограничения системы обнаружения по времени и пропускной способности. То, что отражатели действовали лишь недолго, пока опускались к земле, и не давали постоянного решения, в тех обстоятельствах значения не имело. Им требовалось проработать лишь достаточно хорошо и достаточно долго, чтобы самолёт вышел за пределы действия радара.

Как мы обсудим в части II, многие формы обфускации лучше всего работают как одноразовые ходы, позволяющие выиграть время. Они могут дать лишь несколько минут, но иногда несколько минут - это всё время, которое вам нужно.

Пример дипольных отражателей также помогает на самом базовом уровне провести различие между подходами к обфускации. Дипольные отражатели основаны на создании эхо-сигналов - имитаций настоящего объекта, - которые используют ограниченные возможности наблюдателя. (Фред Коэн называет это «стратегией ложных целей».[2]) Как мы увидим, одни формы обфускации создают подлинные, но вводящие в заблуждение сигналы - подобно тому как содержимое одной машины можно защитить, отправив её в сопровождении нескольких других одинаковых машин, или конкретный самолёт можно защитить, заполнив небо другими самолётами, - тогда как другие формы перемешивают подлинные сигналы, смешивая данные ради затруднения извлечения закономерностей. Поскольку разбрасывающие дипольные отражатели точно знают своего противника, им не требуется ни то ни другое.

Если проектировщики системы обфускации обладают конкретными и подробными знаниями об ограничениях наблюдателя, разработанная ими система должна действовать лишь на одной длине волны и лишь в течение 45 минут. Если используемая противником система наблюдения более терпелива или располагает более широким набором возможностей наблюдения, проектировщикам приходится использовать своё понимание внутренних целей противника, то есть того, какую полезную информацию он надеется извлечь из полученных при наблюдении данных, и подрывать эти цели посредством манипулирования подлинными сигналами.

Прежде чем перейти к манипулированию подлинными сигналами, рассмотрим совсем иной пример заполнения канала эхо-сигналами.

1.2. Боты Twitter: заполнение канала шумом

Два примера, которые мы сейчас обсудим, построены на контрастах. Хотя их способом обфускации служит создание имитаций, они переносят нас из Второй мировой войны в современные обстоятельства и от радаров к социальным сетям. Кроме того, они вводят важную тему.

В главе 3 мы утверждаем, что обфускация особенно подходит в качестве средства «слабым» - тем, кто в силу обстоятельств оказался в невыгодном положении, на проигрывающей стороне асимметричных властных отношений. В конце концов, есть основания прибегнуть к этому методу, если вы не можете стать невидимым, не можете отказаться от отслеживания или наблюдения, не можете просто выйти из системы или работать внутри профессионально защищённых сетей. Это не означает, что его не используют и сильные. У угнетающих или принуждающих сил обычно имеются средства лучше обфускации. Однако иногда обфускация становится полезной могущественным участникам - как это произошло во время двух выборов, одних в России и других в Мексике. Поняв, перед каким выбором стояли противоборствующие группы, мы увидим, как можно применять обфускацию такого рода.

Во время протестов из-за проблем, возникших на парламентских выборах 2011 года в России, значительная часть обсуждений вбросов бюллетеней и других нарушений первоначально проходила на LiveJournal - блоговой платформе, которая возникла в Соединённых Штатах, но наибольшую популярность получила в России: россияне составляли более половины её пользовательской базы.[3] Хотя LiveJournal довольно популярен, его пользовательская база очень мала по сравнению с различными социальными системами Facebook и Google: у платформы менее 2 миллионов активных учётных записей.[4] Поэтому злоумышленникам сравнительно легко отключить LiveJournal с помощью распределённой атаки типа «отказ в обслуживании» (DDoS), то есть компьютеры, разбросанные по всему миру, отправляют такой объём запросов к сайту, что обеспечивающие его работу серверы оказываются перегружены, а законные пользователи утрачивают к нему доступ. Подобная атака на LiveJournal в сочетании с арестами блогеров-активистов на протестной акции в Москве представляла собой прямолинейный способ цензуры.[5] Когда и почему в таком случае понадобилась обфускация?

Обсуждение российских протестов переместилось в Twitter, и заинтересованные в его срыве силы столкнулись с новой трудностью. У Twitter огромная пользовательская база, которой соответствуют его инфраструктура и знания в области безопасности. Вывести его из строя так же легко, как LiveJournal, было невозможно. Поскольку Twitter находился в Соединённых Штатах, он был гораздо лучше способен противостоять политическим манипуляциям, чем материнская компания LiveJournal. (Хотя обслуживание LiveJournal осуществляет учреждённая для этой цели в США компания, владеющая им SUP Media находится в Москве.[6]) Для полной блокировки Twitter потребовалось бы прямое вмешательство государства. Атака на LiveJournal была проведена независимо хакерами-националистами, которые могли иметь, а могли и не иметь одобрение и помощь администрации Путина/Медведева.[7] Поэтому стороны, заинтересованные в прекращении политического обсуждения в Twitter, столкнулись с трудностью, которая будет не раз возникать по мере изучения способов применения обфускации: времени было мало, а традиционные механизмы действий были недоступны. Прямой технический подход - блокировка Twitter внутри страны или всемирная атака типа «отказ в обслуживании» - был невозможен, а политические и правовые направления атаки нельзя было использовать. Поэтому вместо прекращения обсуждения в Twitter злоумышленники могут перегрузить его шумом.

Во время российских протестов обфускация приняла форму тысяч внезапно заговоривших учётных записей Twitter, пользователи которых публиковали твиты с теми же хештегами, что и протестующие.[8] Хештеги служат механизмом группировки твитов; например, если я добавлю к твиту #obfuscation, символ # превратит слово в активную ссылку: щелчок по ней покажет все остальные твиты с меткой #obfuscation. Хештеги полезны для превращения потока твитов в

связные обсуждения конкретных тем, и #триумфальная (отсылка к Триумфальной площади, где проходила протестная акция) стал одним из нескольких тегов, с помощью которых люди могли выплеснуть гнев, выразить мнение и организовать дальнейшие действия. (Хештеги также играют роль в том, как Twitter определяет «актуальные» и важные темы сайта, которые затем могут привлечь дополнительное внимание к обсуждению под этим тегом: список Trending Topics на сайте часто получает освещение в новостях.[9])

Если бы вы следили за #триумфальная, то видели бы один твит за другим от российских активистов, которые распространяли ссылки на новости и строили планы. Но эти твиты начали перемежаться сообщениями о величии России или твитами, которые казались шумом, бессмыслицей либо случайными словами и фразами. В конце концов такие твиты настолько захватили поток #триумфальная и потоки других связанных с протестами тем, что относящиеся к теме сообщения по существу затерялись в шуме: они уже не могли привлечь внимание или положить начало связному обмену с другими пользователями. Этот поток новых твитов исходил от учётных записей, которые большую часть своего существования бездействовали. С момента создания до начала протестов они публиковали очень мало, но теперь каждая выдавала десятки сообщений в час. Некоторые предполагаемые пользователи этих учётных записей носили благозвучные имена вроде imelixyvyq, wyqufahij и hihexiq; у других были имена, казавшиеся более обычными и построенные по схеме имя_фамилия, например latifah_xander.[10]

Очевидно, эти учётные записи Twitter были «ботами Twitter» - программами, которые выдавали себя за людей и автоматически создавали целевые сообщения. Многие учётные записи были созданы примерно в одно время. Благодаря количеству и частоте такие сообщения могут легко захватить обсуждение и вследствие чрезмерного использования фактически разрушить платформу для конкретной аудитории, то есть выполнить обфускацию посредством создания ложных, бессмысленных сигналов.

Использование ботов Twitter становится надёжным приёмом подавления обсуждений в Twitter. Ещё один, причём более совершенный, пример практического применения этой стратегии дают крайне ожесточённые выборы 2012 года в Мексике.[11] Противники лидировавшего кандидата Энрике Пеньи Ньето и Институционно-революционной партии (Partido Revolucionario Institucional, PRI) использовали #marchaAntiEPN как организационный хештег для объединения обсуждения, структурирования призывов к действию и подготовки протестных мероприятий. Группы, желавшие помешать организации протестующих, столкнулись с трудностями, сходными с российским случаем. Однако вместо тысяч ботов было достаточно сотен; более того, когда этот случай исследовала американская испаноязычная телесеть Univision, действовало лишь около тридцати таких ботов. Их подход состоял как в противодействии работе по продвижению #marchaAntiEPN, так и в чрезмерном использовании этого хештега. Многие твиты целиком состояли из вариантов строки «#marchaAntiEPN #marchaAntiEPN #marchaAntiEPN #marchaAntiEPN #marchaAntiEPN #marchaAntiEPN». Подобное повторение, особенно со стороны учётных записей, уже проявлявших подозрительно похожее на ботов поведение, активирует внутренние системы Twitter, которые выявляют попытки манипулировать системой хештегов, а затем удаляют соответствующие хештеги из списка Trending Topics. Иными словами, поскольку элементы Trending Topics становятся достойными новостей и привлекают внимание, спамеры и рекламодатели пытаются посредством повторения протолкнуть хештеги в это пространство, поэтому Twitter разработал механизмы выявления и блокировки такой деятельности.[12]

Боты Twitter на мексиканских выборах намеренно вели себя плохо, чтобы вызвать автоматическое исключение из списка и тем самым не допустить появления влияния #marchaAntiEPN «на радарах» крупных средств массовой информации. Они делали хештег непригодным для использования и лишали его потенциальной значимости для СМИ. Это была обфускация как разрушительное действие. Хотя подобные усилия основаны на той же базовой тактике, что и дипольные отражатели для радаров (то есть на создании множества имитаций, настроенных так, чтобы скрыть настоящую

вещь), цели у них совершенно иные: не просто выиграть время, например в преддверии выборов и в период последовавших за ними волнений, а сделать определённые термины непригодными для использования и даже, с точки зрения алгоритма сортировки, токсичными посредством манипулирования свойствами данных с помощью ложных сигналов.

1.3. CacheCloak: службы определения местоположения без отслеживания местоположения

CacheCloak применяет подход к обфускации, подходящий службам на основе местоположения (location-based services, LBS).[13] Этот случай показывает два новых поворота в использовании ложных эхо-сигналов и имитаций для обфускации. Первый состоит в обеспечении возможности для пользователя по-прежнему извлекать нужные данные; второй - в попытке найти подход, способный работать постоянно, а не служить временной стратегией выигрыша времени.

Службы на основе местоположения используют возможности мобильных устройств по определению местоположения для создания разнообразных сервисов: социальных (например, FourSquare, превращающий посещение мест в соревновательную игру), прибыльных (например, реклама с учётом местоположения) и совершенно практичных (например, карты и поиск ближайших объектов). Здесь проявляется классическая риторика уравновешивания приватности и полезности, в которой полезность часто представляют как нечто наносящее ущерб приватности. Если вам нужна ценность LBS, например вы хотите находиться в той же сети, что и ваши друзья, чтобы встретиться с одним из них, когда окажетесь рядом, придётся пожертвовать частью приватности и привыкнуть к тому, что поставщик услуги знает, где вы находитесь. CacheCloak предлагает иначе устроить этот компромисс.

«Если другие методы пытаются скрыть путь пользователя, пряча отдельные его части, - пишут создатели CacheCloak, - мы скрываем местоположение пользователя, окружая его маршрутами других пользователей»[14], то есть распространяем неоднозначные данные. В стандартной модели ваш телефон отправляет службе своё местоположение и в ответ получает запрошенную информацию. В модели CacheCloak телефон прогнозирует ваши возможные пути, а затем заранее получает результаты для нескольких вероятных маршрутов. По мере движения вы пользуетесь преимуществами знания местоположения - получаете доступ к тому, что ищете, в форме данных, заранее помещённых в кеш до возможных запросов, - а противник остаётся перед множеством возможных путей, не имея возможности отличить начало маршрута от конца или определить, откуда вы пришли, куда намерены направиться и даже где находитесь сейчас. С точки зрения наблюдателя, значимые данные - те, которые мы хотим оставить при себе, - погребены в пространстве других, столь же вероятных данных.

1.4. TrackMeNot: смешивание подлинных и искусственных поисковых запросов

TrackMeNot, разработанный в 2006 году Дэниелом Хоу, Хелен Ниссенбаум и Венсаном Тубиана, служит примером программной стратегии сокрытия деятельности с помощью имитирующих сигналов.[15] Назначение TrackMeNot - помешать профилированию пользователей по их поисковым запросам. Он был разработан в ответ на запрос Министерства юстиции США о предоставлении журналов поиска Google и на удивительное открытие журналиста New York Times: некоторые личности и профили можно было установить даже по опубликованным AOL Inc. обезличенным журналам поиска.[16]

Наши поисковые запросы в конечном счёте превращаются в перечни мест, имён, интересов и проблем. Независимо от того, включены ли в них наши полные IP-адреса, по этим перечням можно установить наши личности и выявить закономерности в наших интересах. Отвечая на требования подотчётности, поисковые компании предложили способы развеять опасения людей по поводу сбора и хранения поисковых запросов, хотя продолжают собирать и анализировать журналы таких запросов.[17] Не допустить, чтобы какой-либо поток запросов неуместно раскрывал интересы и деятельность конкретного человека, по-прежнему трудно.[18]

Решение TrackMeNot состоит не в том, чтобы скрывать запросы пользователей от поисковых систем (это непрактичный метод, учитывая необходимость получать ответы на запросы), а в обфускации посредством автоматического создания запросов из «начального списка» терминов. Первоначально отобранные из RSS-лент, эти термины развиваются таким образом, что у разных пользователей формируются разные начальные списки. Точность имитации постоянно повышается: начальный список пополняется новыми терминами, полученными из результатов поисковых запросов. TrackMeNot отправляет запросы так, чтобы попытаться имитировать поисковое поведение настоящих пользователей. Например, пользователь, искавший «хорошее кафе с wi-fi челси», мог также искать «питомники саванна», «свежевыжатый сок майами», «азиатская компания недвижимости», «физические упражнения замедляют деменцию» и «телескопический галогенный светильник». Действия человека маскируются действиями множества призраков, отчего закономерность становится труднее различить и уже гораздо сложнее утверждать, что конкретный запрос возник вследствие человеческого намерения, а не был автоматически создан TrackMeNot. Тем самым TrackMeNot расширяет роль обфускации и в некоторых ситуациях обеспечивает возможность правдоподобно отрицать причастность.

1.5. Загрузки на сайты утечек: как похоронить важные файлы

WikiLeaks применял различные системы для защиты личностей как посетителей, так и авторов материалов. Однако существовал демаскирующий признак, способный подорвать безопасность сайта: загрузка файлов. Если бы соглядатаи могли отслеживать трафик WikiLeaks, они могли бы выявлять действия по отправке материалов на защищённый сервер WikiLeaks. В особенности если бы они могли обоснованно предположить сжатый размер различных впоследствии опубликованных наборов данных, то задним числом смогли бы сделать выводы о том, что, когда и кем было передано (учитывая недочёты в других областях технической и операционной безопасности). Столкнувшись с этой совершенно особой трудностью, WikiLeaks разработал сценарий для создания ложных сигналов. Он запускался в браузерах посетителей и порождал действия, похожие на загрузки на защищённый сервер.[19] Поэтому соглядатай видел бы огромную толпу предполагаемых информаторов (подавляющее большинство которых в действительности лишь читало или просматривало уже опубликованные документы), и некоторые из них действительно могли быть информаторами. Сценарий не стремился предоставить какие-либо определённые данные для противодействия интеллектуальному анализу данных или рекламе; он просто имитировал и скрывал действия некоторых пользователей.

Однако даже зашифрованные и сжатые данные содержат существенные метаданные, и проект OpenLeaks - в конечном счёте неудачного варианта WikiLeaks, разработанного некоторыми разочаровавшимися участниками первоначальной системы WikiLeaks, - включал дальнейшее усовершенствование.[20] Проведя статистический анализ материалов, отправленных в WikiLeaks, OpenLeaks разработал модель поддельных загрузок, которая сохраняла те же соотношения размеров файлов, что обычно встречались во входящем трафике сайта утечек. Размер большинства файлов составлял от 1,5 до 2 мегабайт, хотя несколько выбросов превышали 700 мегабайт. Если противник способен отслеживать трафик загрузки, форма может быть не менее

показательной, чем содержание, и не менее полезной для отделения настоящих сигналов от поддельных. Как показывает этот пример, механизмы обфускации могут значительно выиграть, если определить все параметры, которыми можно манипулировать, и выяснить, что ищет противник, чтобы предоставить ему искусственно изготовленную версию искомого.

1.6. Ложные теллсы: создание закономерностей для обмана подготовленного наблюдателя

Рассмотрим, как ту же базовую схему обфускации можно поставить на службу в контексте более лёгком, чем сокрытие работы информаторов: в покере.

Значительная часть удовольствия и трудности покера состоит в том, чтобы по выражениям лица, жестам и языку тела научиться определять, блефует ли человек (то есть делает вид, будто у него на руках более слабая комбинация, чем на самом деле) в надежде, что соперник уравняет ставку. Центральное место в изучении соперников занимает «телл» - неосознанная привычка или нервное движение, которые противник проявляет при сильной или слабой комбинации: например, потеет, тревожно поглядывает или наклоняется вперёд. Теллсы настолько важны в информационной экономике покера, что игроки порой используют ложные теллсы, то есть создают особенности поведения, которые могут показаться частями более широкой закономерности.[21] Согласно распространённой покерной стратегии, ложный телл лучше приберечь для решающего момента турнира, иначе другие игроки успеют понять, что он недостоверен, и в свою очередь воспользуются этим против вас. Терпеливый анализ множества игр позволил бы отделить настоящие теллсы от ложных, но в ограниченном по времени контексте игры с высокими ставками момент обмана может оказаться очень действенным. Сходные приёмы применяются во многих видах спорта, где присутствует видимая коммуникация. Один из примеров - подача сигналов в бейсболе; как объяснил тренер газетному репортёру: «Иногда вы подаёте знак, но он вообще ничего не означает».[22]

1.7. Групповая идентичность: множество людей под одним именем

Один из простейших и самых запоминающихся примеров обфускации, который к тому же знакомит с ролью группы в обфускации, - сцена из фильма «Спартак», где римские солдаты требуют от восставших рабов назвать своего предводителя, которого солдаты намерены распять.[23] Когда Спартак (в исполнении Кирка Дугласа) уже собирается заговорить, окружающие один за другим произносят: «Я Спартак!», пока вся толпа не заявляет об этой идентичности.

Множество людей, принимающих одну и ту же идентичность ради защиты группы (например, Капитан Свинг во время восстаний английских сельскохозяйственных рабочих 1830 года; вездесущий «Жак», имя которого берут радикалы в «Повести о двух городах» Диккенса; или маска Гая Фокса из графического романа «V - значит вендетта», теперь связанная с хактивистской группой Anonymous), к настоящему времени стало почти клише.[24] Марко Дезериис исследовал применение «несобственных имён» и коллективных идентичностей для стирания индивидуальной ответственности и умножения действий.[25] Одни формы обфускации можно осуществлять в одиночку; другие зависят от групп, команд, сообществ и сообщников.

1.8. Одинаково выглядящие сообщники и предметы: множество людей в одинаковой одежде

Существует множество примеров обфускации, при которой члены группы сообща создают подлинные, но вводящие в заблуждение сигналы, скрывающие подлинный значимый сигнал. Запоминающийся пример из массовой культуры - сцена в ремейке фильма «Афера Томаса Крауна» 1999 года, где главный герой в приметном костюме, вдохновлённом Магриттом, внезапно оказывается среди тщательно организованной массы других мужчин в таких же костюмах, которые ходят по музею и обмениваются одинаковыми портфелями.[26] План ограбления банка в фильме «Не пойман - не вор» 2006 года основан на том, что все грабители одеты в рабочие комбинезоны маляров, перчатки и маски и точно так же одевают заложников.[27] Наконец, вспомним находчивость Роджера Торнхилла, главного героя фильма Альфреда Хичкока «К северу через северо-запад» 1959 года: чтобы ускользнуть от полиции по прибытии поезда в Чикаго, он подкупает носильщика и берёт его приметную форму, зная, что толпа носильщиков на станции даст полиции слишком много конкретных целей для поиска.[28]

Одинаковые предметы как средство обфускации встречаются достаточно часто и достаточно понятны, чтобы вновь и вновь возникать в воображении и действительности. Примером служат анцилии Древнего Рима. Согласно легенде, во время правления Нумы Помпилия, второго царя Рима (753-673 годы до н. э.), с неба упал щит (ancile), который истолковали как знак божественного благоволения, священную реликвию, владение которой гарантировало продолжение римского господства.[29] Его повесили в храме Марса вместе с одиннадцатью точными копиями, чтобы потенциальные похитители не знали, какой щит взять. Ещё один пример дают шесть гипсовых бюстов Наполеона, от которых получил название рассказ о Шерлоке Холмсе. Злодей помещает чёрную жемчужину в мокрый гипс предмета, у которого не только есть пять копий, но который к тому же относится к более широкому классу предметов (дешёвых белых бюстов Наполеона), настолько повсеместных, что они становятся невидимыми.[30]

Случай из реального мира связан с так называемым грабителем с Craigslist. Во вторник 30 сентября 2008 года в 11 часов утра мужчина, одетый как дезинсектор (синяя рубашка, защитные очки и противопылевая маска) и нёсший распылитель, подошёл к бронированному автомобилю у банка в Монро, штат Вашингтон, вывел охранника из строя перцовым аэрозолем и скрылся с деньгами.[31] Прибывшая полиция обнаружила поблизости тринадцать мужчин в синих рубашках, защитных очках и противопылевых масках: они надели эту форму по указаниям из объявления на Craigslist, которое обещало хорошую оплату за технические работы, начинавшиеся в 11:15 по адресу банка. Чтобы установить, что ни один из подённых рабочих не был грабителем, понадобилось бы лишь несколько минут, но несколько минут - это всё время, которое требовалось грабителю.

Есть и яркая история, которую часто пересказывают, хотя фактически она неверна: король Дании и множество датчан-неевреев надели жёлтую звезду, чтобы оккупационные немецкие власти не могли отличить и депортировать датских евреев. Хотя датчане мужественно защищали своё еврейское население другими способами, нацисты не применяли жёлтую звезду в оккупированной Дании, опасаясь вызвать усиление антинемецких настроений. Однако «существуют документально подтверждённые случаи, когда неевреи носили жёлтые звёзды в знак протеста против нацистского антисемитизма в Бельгии, Франции, Нидерландах, Польше и даже в самой Германии».[32] Эта легенда даёт идеальный пример совместной обфускации: неевреи носят жёлтую звезду как акт протеста, создавая группу населения, с которой могут слиться отдельные евреи.[33]

1.9. Избыточное документирование: как сделать анализ неэффективным

Продолжая рассматривать обфускацию, действующую посредством добавления подлинных, но вводящих в заблуждение сигналов, обратимся к избыточному созданию документов как форме обфускации, например к чрезмерному раскрытию материалов в судебном процессе. Такова была стратегия Огюстена Лежёна, начальника Общего полицейского бюро Комитета общественного спасения, одного из главных орудий эпохи Террора Французской революции. Лежён и его писцы составляли отчёты, закладывавшие основу для арестов, интернирований и казней. Позднее, пытаясь оправдать свою роль в Терроре, Лежён утверждал, что скрупулёзное, подавляюще подробное качество отчётов его ведомства было намеренным: он поручил писцам создавать избыточный объём материалов и сообщать «самые незначительные подробности», чтобы замедлить подготовку разведывательной информации для Комитета, не создавая видимости мятежа. Сомнительно, что утверждения Лежёна полностью точны (приводимые им количества подготовленных отчётов ненадёжны), но, как отмечает Бен Кафка, он придумал бюрократическую стратегию создания задержек посредством избыточного предложения: «Он, по-видимому, пусть и с опозданием, понял, что умножение документов и подробностей открывает возможности как для сопротивления, так и для подчинения».[34] В ситуациях, когда нельзя сказать «нет», открываются возможности для хора бесполезных «да»: например, в ответ на запрос отправляйте не папку, а палету с коробками папок, содержащих потенциально относящиеся к делу бумаги.

1.10. Перестановка SIM-карт: внесение неопределённости в выбор мобильной цели

Как показали недавние журналистские материалы и некоторые раскрытые Эдвардом Сноуденом сведения, аналитики, работающие на Агентство национальной безопасности, используют сочетание источников радиоэлектронной разведки - прежде всего метаданные мобильных телефонов и данные систем геолокации, - чтобы выявлять и отслеживать цели для уничтожения.[35] Метаданные (показывающие, на какие номера и когда звонили) создают модель социальной сети, которая позволяет установить определённые телефонные номера как принадлежащие интересующим лицам; благодаря геолокационным свойствам мобильных телефонов эти номера можно с разной степенью точности привязать к конкретным местам, по которым затем могут наносить удары беспилотники. Иными словами, эта система способна пройти путь от идентификации к установлению местоположения и убийству, ни разу не проведя визуальную идентификацию человека лицом к лицу. Самое близкое к возможности увидеть человека, что может получить оператор беспилотника, - это наружный вид здания или силуэт садящегося в машину человека. Разумеется, учитывая непоследовательные результаты программы АНБ по сбору метаданных мобильных телефонов и ударов беспилотников, точность вызывает серьёзные опасения. Беспокоят ли человека угрозы национальной безопасности, которые остаются в безопасности и продолжают действовать, несправедливо отнятые жизни невинных людей или и то и другое, потенциальные изъяны такого подхода увидеть нетрудно.

Однако перевернём ситуацию и рассмотрим её более абстрактно с точки зрения целей. Большинство целей АНБ вынуждены всегда иметь при себе или рядом с собой устройство слежения (только самые высокопоставленные фигуры в террористических организациях могут обходиться без технологий, создающих сигналы), как и практически все люди, с которыми они контактируют. Звонки и разговоры, поддерживающие работу их организаций, одновременно предоставляют средства для их идентификации; структура, делающая возможной их деятельность, также заманивает их в ловушку. Противнику не приходится координировать зенитные орудия ради

поиска цели где-то в небе: он обладает полным господством в воздухе и способен доставить ракету к машине, перекрёстку или дому. Однако у противника имеется и тесно связанный с этим набор системных ограничений. Как бы ни поражала эта система своим масштабом и возможностями, в конечном счёте она опирается на SIM-карты (модули идентификации абонента) и физическое владение мобильными телефонами - своего рода узкую полосу пропускания, которую можно использовать. Бывший оператор беспилотника Объединённого командования специальных операций сообщил, что поэтому цели принимают меры для смешивания и запутывания подлинных сигналов. В обращении находится множество SIM-карт, связанных с личностями некоторых людей, и эти карты случайным образом перераспределяются. Один из подходов состоит в проведении встреч, на которых все участники складывают SIM-карты в сумку, а затем наугад вытаскивают их, чтобы осталось неясным, кто в действительности связан с каждым устройством. (Этот подход ограничен во времени: если анализ метаданных достаточно развит, аналитик в конце концов сможет снова разделить людей по прежним закономерностям звонков, однако нерегулярное повторное перемешивание усложняет эту задачу.) Повторное перемешивание может происходить и непреднамеренно, когда не знающие о слежке цели продают телефоны или дают их друзьям либо родственникам. В результате система с огромной технической точностью имеет весьма неопределённый показатель фактического успеха, измеряемый как числом уничтоженных опасных лиц, так и числом невинных некомбатантов, убитых по ошибке. Даже когда довольно точного отслеживания местоположения и анализа социального графа нельзя избежать, обфускация посредством соединения и перемешивания подлинных сигналов вместо создания ложных способна обеспечить некоторую меру защиты и контроля.

1.11. Ретрансляторы Tor: запросы от имени других, скрывающие личный трафик

Tor - система, предназначенная для обеспечения анонимного использования Интернета посредством сочетания шифрования и передачи сообщения через множество различных независимых «узлов». В гибридной стратегии обфускации Tor можно применять совместно с другими, более мощными механизмами сокрытия данных. Такая стратегия частично достигает обфускации посредством смешивания и чередования подлинной (зашифрованной) деятельности. Представьте, что сообщение тайно передают вам через огромную толпу. В сообщении содержится вопрос без каких-либо идентифицирующих сведений; насколько вам известно, его написал последний державший его человек, который и передал его вам. Написанный и отправленный вами обратно ответ исчезает в толпе, следуя непредсказуемым маршрутом. Где-то в этой толпе автор получает свой ответ. Ни вы, ни кто-либо другой точно не знаете, кто был автором.

Если вы запросите веб-страницу, работая через Tor, запрос поступит не с вашего IP-адреса; он придёт с «выходного узла» (подобного последнему человеку, передающему сообщение адресату) системы Tor вместе с запросами многих других пользователей Tor. Данные входят в систему Tor и проходят в лабиринт ретрансляторов, то есть компьютеров сети Tor (подобных людям в толпе), которые предоставляют часть своей пропускной способности для обработки чужого трафика Tor и соглашаются передавать сообщения вслепую. Чем больше ретрансляторов, тем быстрее система в целом. Если вы уже используете Tor для защиты своего интернет-трафика, то ради общего коллективного блага можете превратить свой компьютер в ретранслятор. По мере того как сетью пользуется больше людей, улучшаются и сама сеть Tor, и обфускация отдельных пользователей в ней.

Как указывают создатели Tor, обфускация усиливает его и без того значительную защитную способность. Запуская ретранслятор Tor, «вы действительно получаете лучшую анонимность против некоторых атак. Простейший пример - злоумышленник, владеющий небольшим числом

ретрансляторов Tor. Он увидит соединение от вас, но не сможет узнать, возникло ли это соединение на вашем компьютере или было ретранслировано от кого-то другого».[36] Если у кого-то есть агенты в толпе, то есть если кто-то запускает ретрансляторы Tor ради наблюдения, агенты не могут прочитать передаваемое ими сообщение, но могут заметить, кто им его передал. Если вы используете Tor, но не запускаете ретранслятор, они знают, что переданное им сообщение написали вы. Но если вы позволяете своему компьютеру работать ретранслятором, сообщение может принадлежать вам, а может быть лишь одним из множества сообщений, которые вы передаёте за других людей. Началось ли это сообщение у вас или нет? Теперь информация неоднозначна, а написанные вами сообщения находятся в безопасности внутри стаи других сообщений, которые вы передаёте дальше. Короче говоря, это значительно более сложный и эффективный способ сделать конкретные операции с данными неоднозначными и сорвать анализ трафика посредством использования его объёма. Он не просто смешивает подлинные сигналы (как перемешивание SIM-карт в сумке со всеми вытекающими проблемами координации), но доставляет каждое сообщение по назначению. При этом каждое сообщение может создавать неопределённость относительно источников других сообщений.

1.12. Записи речевого шума: сокрытие речи внутри речи

Старое клише о гангстерах под угрозой со стороны ФБР предполагало множество разговоров в ванных комнатах: по этой версии, плеск и шипение воды и гул вентилятора затрудняли прослушивание разговоров, если в доме были установлены жучки или кто-то в комнате носил скрытый микрофон. Теперь существуют усовершенствованные (и гораздо более эффективные) приёмы противодействия аудионаблюдению, которые более непосредственно опираются на обфускацию. Один из них - применение так называемых записей речевого шума.[37] Как ни парадоксально, ими чаще пользовались не гангстеры, а адвокаты, обеспокоенные тем, что прослушивание может нарушить адвокатскую тайну.

Запись речевого шума - цифровой файл, предназначенный для фонового воспроизведения во время разговоров. У файла сложное устройство. Одновременно звучат сорок голосовых дорожек (тридцать две на английском, восемь на других языках), и каждую дорожку сжимают по частоте и времени, создавая дополнительные «голоса», которые заполняют весь частотный спектр. Присутствуют также разнообразные нечеловеческие механические шумы и периодический ультразвуковой импульс (неслышимый взрослыми), специально спроектированный для помех системе автоматической регулировки усиления, с помощью которой прослушивающее устройство настраивается для наилучшего приёма звукового сигнала. Что особенно важно для нашей темы, среди голосов на используемой адвокатом записи речевого шума присутствуют голоса самого клиента и адвоката. Плотная смесь голосов затрудняет различение любого отдельно взятого голоса.

1.13. Операция «Вула»: обфускация в борьбе против апартеида

Мы завершаем эту главу подробным повествовательным примером обфускации, применённой в сложном контексте группой, которая стремилась добиться освобождения Нельсона Манделы из тюрьмы в Южной Африке во время борьбы против апартеида. Операцию назвали «Вула» (сокращённо от Vul'indlela, что означает «Открывая дорогу»); её разработали руководители Африканского национального конгресса внутри Южной Африки, поддерживавшие связь с Манделой и координировавшие свои усилия с действиями агентов, сторонников и командиров АНК по всему миру.

Последний проект такого масштаба, проведённый АНК, привёл к катастрофе начала 1960-х годов, когда Мандела и практически все высшие руководители АНК были арестованы, а документы с фермы Лилислиф захвачены и использованы против них в суде. Это означало, что операция «Вула» должна была проводиться с абсолютно безупречными мерами безопасности и приватности. И действительно, когда в 1990-х годах раскрылся полный масштаб операции, это стало неожиданностью не только для правительства Южной Африки и международных разведывательных служб, но и для многих видных руководителей внутри АНК. Люди, которые якобы проходили пересадку почки или восстанавливались после аварии на мотоцикле, в действительности глубоко уходили в подполье с новыми личностями, а затем возвращались в Южную Африку, «открывая дорогу» для освобождения Манделы. Учитывая наблюдение внутри и за пределами Южной Африки, возможную компрометацию существовавших каналов связи АНК и интерес шпионов и правоохранительных органов по всему миру, операции «Вула» требовались безопасные способы обмена информацией и координации.

Необыкновенную историю операции «Вула» рассказал на страницах журнала АНК Mayibuye один из её главных создателей Тим Дженкин.[38] Она представляет собой превосходный пример операционной безопасности, методов агентурной работы и управления защищённой сетью.

Чтобы понять, когда и как в операции «Вула» начали применять обфускацию, необходимо разобраться в некоторых трудностях, с которыми столкнулись её создатели. Пользоваться стационарными телефонными линиями внутри Южной Африки, каждая из которых была связана с адресом и именем, было нельзя. Малейшая компрометация могла привести к прослушиванию линий и к тому, что теперь мы назвали бы анализом метаданных, а значит, картину сети активистов можно было бы составить по внутренним и международным журналам телефонных соединений. У агентов «Вулы» имелись различные системы кодирования, но каждой мешали трудность и утомительность ручного кодирования. Всегда возникал соблазн вернуться к «разговорам шёпотом по телефону», особенно когда случались кризисы и события начинали развиваться быстро. Операцию требовалось без помех координировать между Южной Африкой (прежде всего Дурбаном и Йоханнесбургом), Лусакой, Лондоном, Амстердамом и другими местами по всему миру, между которыми перемещались агенты. Почта работала медленно и была уязвима, шифрование отнимало огромное количество времени и часто выполнялось небрежно, пользоваться домашними телефонами запрещалось, а координация между несколькими часовыми поясами по всему миру казалась невозможной.

Дженкин знал о возможности применять персональные компьютеры для ускорения и повышения эффективности шифрования. Обосновавшись в Лондоне после побега из Центральной тюрьмы Претории, он в середине 1980-х годов работал над системой связи, необходимой для операции «Вула» и в конечном счёте превратившейся в замечательную сеть. Шифрование выполнялось на персональном компьютере, после чего зашифрованное сообщение представлялось в виде быстрой последовательности тональных сигналов, записанной на переносной кассетный магнитофон. Агент приходил к общественному телефону-автомату и набирал лондонский номер, на котором отвечал модифицированный Дженкином автоответчик, способный вести запись до пяти минут. Агент воспроизводил кассету в микрофон телефонной трубки. Тональные сигналы, записанные на другой стороне кассеты, можно было через акустический модем передать в компьютер, а затем расшифровать. (Существовал и автоответчик для «исходящей» связи. Удалённые агенты могли позвонить с телефона-автомата, записать тональные сигналы своих сообщений и расшифровать их в любом месте, где имели доступ к компьютеру, способному запускать разработанные Дженкином системы шифрования.)

Это уже была чрезвычайно впечатляющая сеть, не в последнюю очередь потому, что значительные части её цифровой стороны (включая способ применения кодов исправления ошибок для борьбы с шумом при воспроизведении сообщений по международным телефонным линиям из шумных будок) пришлось изобретать с нуля. Однако по мере роста операции «Вула» и расширения сети

оперативников один только объём трафика грозил перегрузить сеть. Оперативники готовили Южную Африку к действиям, и эта работа оставляла мало времени на поиски телефонов-автоматов, принимавших кредитные карты (звук падающих монет мог помешать сигналу), и стояние рядом с магнитофонами. Дженкин и его сотрудники засиживались допоздна, меняя кассеты в аппаратах по мере поступления потока сообщений. Пришло время перейти на зашифрованную электронную почту, однако вся система была разработана так, чтобы не пользоваться известными телефонными линиями с установленными владельцами внутри Южной Африки.

Операции «Вула» требовалась возможность отправлять зашифрованные сообщения на компьютеры и с компьютеров в Южной Африке, Лукасе и Лондоне, не вызывая подозрений. Пока в 1980-х годах описанная нами сеть обретала форму, более широкая среда международного бизнеса создавала именно тот фон, на котором могла скрыться эта уловка. Как сформулировал Дженкин, вопрос звучал так: «Имел ли противник возможность определить, какое из тысяч сообщений, ежедневно покидавших страну, было "подозрительным"?» Активистам требовался типичный пользователь зашифрованной электронной почты, не имевший явной политической принадлежности, чтобы выяснить, смогут ли их зашифрованные сообщения остаться незамеченными в общем потоке почты. Позднее Дженкин вспоминал, что им требовалось «найти человека, который обычно пользовался бы компьютером для связи с заграницей, и поручить этому человеку обрабатывать сообщения».

У них был агент, на котором можно было испытать эту систему до перевода связи на новый подход: уроженец Южной Африки, собиравшийся вернуться на родину после многолетней работы за границей программистом в британских телекоммуникационных компаниях. Их агент должен был вести себя точно как обычный гражданин, ежедневно отправляющий множество электронных писем: пользоваться коммерческой почтовой службой, а не собственным сервером, и опираться на тот факт, что многие компании применяли шифрование в своих сообщениях. «Для человека в его положении это было совершенно обычным делом», - вспоминал Дженкин. Система сработала: сообщения агента сливались с обычным трафиком, создавая платформу для открыто тайной связи, которую можно было быстро расширить.

Выдавая себя за компьютерных консультантов, Тим Дженкин и Ронни Пресс (ещё один важный член Технического комитета АНК) могли следить за появлением новых устройств и технологий хранения данных, а также организовывать их покупку и доставку туда, где они требовались. Сочетая коммерческих поставщиков электронной почты и службы электронных досок объявлений, работавшие на персональных и карманных компьютерах, они смогли распространять сообщения внутри Южной Африки и по всему миру, а также готовить полностью оформленные материалы АНК к распространению. (Система передавала даже сообщения от Манделы, которые его адвокат выносил в тайных отделениях книг, а затем вводил в систему.) Обычная деятельность обычных пользователей с непримечательными деловыми адресами превратилась в исключительно ценный информационный канал, по которому огромные объёмы зашифрованных данных шли из Лондона в Лукасу, затем в Южную Африку и между ячейками «Вулы» внутри страны. Успех этой системы отчасти объяснялся историческими обстоятельствами: персональные компьютеры и электронная почта (включая зашифрованную) стали достаточно обычными, чтобы не вызывать подозрений, но ещё не настолько распространёнными, чтобы побудить к созданию новых, более всеобъемлющих систем цифрового наблюдения, которыми сегодня располагают правительства.

Сеть «Вулы» на заключительном этапе не питала наивных представлений о безопасности цифровых сообщений: она защищала всё сложной системой шифрования с множеством изобретательных деталей и побуждала пользователей менять ключи шифрования и соблюдать надлежащую операционную безопасность. Но в этом контексте она даёт превосходный пример той роли, которую обфускация может играть в построении безопасной и тайной системы связи. Она показывает преимущества поиска подходящей существующей среды и слияния с ней, когда

информация теряется в гуле обычной коммерции и скрывается толпой.

Глава 2. Другие примеры

2.1. Пауки-кругопряды: обфускация у животных

Некоторые животные (а также некоторые растения) умеют скрываться или прибегать к визуальным уловкам. Насекомые подражают внешнему виду листьев или веточек, кролики имеют противотеневую окраску (белый живот), устраняющую признаки формы, по которым ястреб может легко их увидеть и атаковать, а пятна на крыльях бабочек имитируют глаза хищных животных.

Образцовый обфускатор в животном мире - паук-кругопряд Cyclosa mulmeinensis.[1] Этот паук сталкивается с особой проблемой, для которой обфускация служит разумным решением: чтобы ловить добычу, паутина должна быть несколько открытой, но из-за этого паук становится гораздо уязвимее для нападения ос. Решение паука состоит в том, чтобы создавать собственные подобия из остатков добычи, листового опада и паучьего шёлка; с точки зрения осы они имеют те же размер, цвет и отражательную способность, что и сам паук. Эти ложные цели паук размещает по всей паутине. В результате снижается вероятность того, что оса нанесёт точный удар, а Cyclosa mulmeinensis получает время, чтобы поспешно уйти от опасности.

2.2. Ложные заказы: применение обфускации для нападения на конкурирующие компании

Цель обфускации, состоящую в повышении уровня шума в канале, можно использовать не только для сокрытия значимого трафика, но и для увеличения затрат на организацию работы через этот канал, а значит, и стоимости ведения бизнеса. Практический пример такого подхода даёт компания Uber, предлагающая замену такси.

Рынок компаний, предлагающих нечто подобное такси и автомобильным перевозкам, быстро растёт, и за клиентов и водителей идёт ожесточённая конкуренция. Uber предлагала премии водителям, переходившим из конкурирующих служб, и вознаграждение просто за посещение штаб-квартиры компании. В Нью-Йорке Uber проводила особенно агрессивную стратегию против конкурента Gett, используя обфускацию для переманивания водителей Gett.[2] В течение нескольких дней сотрудники Uber заказывали поездки через Gett, а затем отменяли заказы незадолго до прибытия водителей Gett. Поток бесплодных заказов заставлял водителей Gett постоянно перемещаться, не получая платы и не имея возможности выполнить множество настоящих заявок. Вскоре после получения одного или нескольких бесплодных заказов водитель Gett получал текстовое сообщение от Uber с предложением денег за смену работы. Настоящие заявки на поездки фактически подвергались обфускации поддельными заявками Uber, снижая ценность работы в Gett. (Компания совместных поездок Lyft утверждала, что Uber проводила сходные обфускационные атаки на её водителей.)

2.3. Французские ложные радарные позиции: как победить детекторы радаров

Обфускация играет определённую роль в стратегии французского правительства против детекторов радаров.[3] Эти довольно распространённые устройства предупреждают водителей, когда полиция поблизости использует радар для измерения скорости. Некоторые детекторы способны указывать положение радара относительно автомобиля пользователя и потому ещё эффективнее помогают водителям избегать штрафов за превышение скорости.

В теории штрафы удерживают от чрезмерно быстрой и опасной езды; на практике они служат источником дохода для местных полицейских управлений и органов власти. По обеим причинам полиция весьма заинтересована в противодействии детекторам радаров.

Возможность регулировать или даже запретить детекторы радаров нереалистична, поскольку, по оценкам, ими владеют 6 миллионов французских водителей. Превращать столь многих обычных граждан в преступников кажется политически неразумным. Не имея полномочий прекратить наблюдение за радарами, французское правительство обратилось к обфускации, чтобы сделать такое наблюдение менее полезным в зонах интенсивного движения: оно размещает группы устройств, которые вызывают предупреждающие сигналы детекторов, но фактически не измеряют скорость. Эти устройства воспроизводят стратегию дипольных отражателей: предупреждающие звуки множатся снова и снова. Один из них действительно может указывать на настоящий радар измерения скорости, но какой именно? Значимый сигнал тонет в массе других правдоподобных сигналов. Водители либо рискуют получить штраф за превышение скорости, либо замедляются в ответ на поток радарных сигналов. И общественная цель достигнута. Как бы человек ни относился к дорожной полиции или превышающим скорость водителям, этот случай интересен как способ, которым обфускация помогает достичь цели не посредством прямого уничтожения устройств противника, а делая их функционально бесполезными.

2.4. AdNauseam: нажатие на все рекламные объявления

Применяя стратегию, напоминающую французские ложные радарные позиции, плагин браузера AdNauseam противодействует сетевому наблюдению ради поведенческой рекламы, нажимая на все баннерные объявления на всех веб-страницах, которые посещают его пользователи. Работая совместно с Ad Block Plus, AdNauseam действует в фоновом режиме и незаметно нажимает на все заблокированные объявления, одновременно записывая для пользователя сведения о показанной и заблокированной рекламе.

Идея AdNauseam родилась из ощущения беспомощности: невозможно остановить повсеместное отслеживание рекламными сетями или постичь запутанные организационные и технические сложности, составляющие его социотехническую внутреннюю инфраструктуру. К ним относятся файлы cookie и веб-маяки, формирование цифрового отпечатка браузера (когда сочетания и конфигурации технологий посетителя используют для идентификации его действий), рекламные сети и аналитические компании. Попытки найти компромисс с помощью технического стандарта Do Not Track были сорваны влиятельными участниками политической экономии таргетированной рекламы. В этой атмосфере отсутствия компромисса родился AdNauseam. Его замысел вдохновило небольшое прозрение относительно господствующей бизнес-модели, которая взимает с потенциальных рекламодателей повышенную плату за предоставление зрителей с подтверждённым интересом к их товарам. Какое свидетельство интереса красноречивее, чем нажатия на определённые объявления? Кроме того, нажатия иногда служат основанием оплаты рекламной сети и размещающему рекламу сайту. Нажатия на рекламу в сочетании с другими потоками данных постепенно формируют профили отслеживаемых пользователей. Подобно французским системам ложных радаров, AdNauseam не стремится уничтожить способность отслеживать нажатия; вместо этого он снижает ценность этих нажатий, обфусцируя настоящие нажатия создаваемыми автоматически.

2.5. Засорение котировками: введение в заблуждение алгоритмических торговых стратегий

Термин «засорение котировками» применяют к всплескам аномальной активности на фондовых биржах, которые выглядят как вводящие в заблуждение торговые данные, создаваемые ради получения преимущества над конкурентами на бирже. В узкоспециализированной области высокочастотной торговли (high-frequency trading, HFT) алгоритмы совершают большие объёмы сделок намного быстрее людей, используя крошечные промежутки времени и разницу цен, которые не привлекли бы внимания трейдеров-людей. Время всегда имело критическое значение для торговли, но в HFT прибыль от убытка отделяют тысячные доли секунды, и возникли сложные стратегии ускорения собственных сделок и замедления сделок конкурентов. Летом 2010 года аналитики рыночного поведения начали замечать необычные закономерности активности HFT: всплески запросов котировок конкретной акции, иногда по несколько тысяч в секунду. У такой активности, казалось, не было экономического обоснования, но одна из самых интересных и правдоподобных теорий состоит в том, что эти всплески представляют собой тактику обфускации. Один наблюдатель объясняет явление так: «Если бы вы могли создать большое число котировок, которые конкуренты должны обработать, а вы, как их создатель, можете игнорировать, то получили бы драгоценное время обработки».[4]

Несущественная информация в форме котировок используется для заполнения пространства значимой деятельности, чтобы создатели несущественной информации могли точно оценивать происходящее, одновременно усложняя эту задачу конкурентам и заставляя их тратить больше времени. Они создают облако, сквозь которое способны видеть только сами. При более длительном наблюдении ни одна закономерность в этой информации не обманула бы аналитика и даже не отвлекла бы его: было бы очевидно, что она искусственна и несущественна. Но в мире HFT с промежутками короче долей секунды решающее значение имеет одно только время, необходимое для наблюдения и обработки деятельности.

Если применение «засорения котировками» распространится, оно способно угрожать самой целостности фондового рынка как работающей системы, перегружая физическую инфраструктуру фондовых бирж сотнями тысяч бесполезных котировок, потребляющих пропускную способность. «Это чрезвычайно тревожное явление, - добавляет процитированный выше наблюдатель, - потому что по мере того, как всё больше систем HFT начнут так поступать, засорение котировками лишь вопрос времени остановит весь рынок из-за перегрузки».[5]

2.6. Обмен картами лояльности для противодействия анализу покупательских привычек

Продовольственные магазины давно находятся на переднем крае технологий, когда дело касается работы с данными. Относительно безобидные ранние программы карт лояльности применяли для привлечения постоянных покупателей, получения дополнительной прибыли от людей, не пользовавшихся картой, и поддержки примитивных проектов обработки данных, таких как организация прямых почтовых рассылок по почтовому индексу. Подавляющее большинство продавцов продуктов и торговых сетей передавали анализ данных на сторону компаниям ACNielsen, Catalina Marketing и ещё нескольким фирмам.[6] Хотя поначалу эти практики воспринимались как изолированные и безобидные, несколько происшествий изменили восприятие их назначения с безвредного и полезного на несколько зловещее.

В 1999 году падение из-за скользкого пола в супермаркете Лос-Анджелеса привело к судебному иску, и адвокаты сети супермаркетов пригрозили раскрыть суду историю покупок алкоголя пострадавшим.[7] Череда сходных дел на протяжении многих лет питала растущее в массовом воображении подозрение, что так называемые карты лояльности служат целям, выходящим за рамки предоставления скидок. Вскоре после их широкого появления возникли сети обмена картами. Люди делились картами, чтобы обфусцировать данные о своих покупательских привычках: поначалу на импровизированных личных встречах, а затем, с помощью списков рассылки и сетевых социальных сетей, во всё более крупных группах населения и на обширных географических территориях. Например, проект Rob's Giant Bonus Card Swap Meet начался с идеи о том, что система обмена штрихкодами позволит покупателям сети супермаркетов Giant в районе округа Колумбия распечатывать штрихкоды других клиентов, а затем наклеивать их на свои карты.[8] Подобным образом проект Ultimate Shopper изготовлял и распространял наклейки со штрихкодом карты лояльности Safeway, создавая тем самым «армию клонов», чьи покупательские данные будут накапливаться вместе.[9] Сайт Cardexchange.org, посвящённый обмену картами лояльности по почте, представляет себя прямым аналогом личных встреч, проводимых с той же целью. Обмен картами лояльности представляет собой обфускацию как групповую деятельность: чем больше людей готовы делиться своими картами и чем дальше путешествуют карты, тем менее надёжными становятся данные.

На сайтах обмена картами также проходят обсуждения и публикуются новостные статьи и очерки о разных подходах к обфускации карт лояльности и о некоторых возникающих при этом этических вопросах. Отрицательное воздействие на продуктовые магазины вызывает беспокойство, поскольку обмен картами ухудшает качество доступных им и, возможно, другим получателям данных. Стоит отметить, что такое воздействие зависит как от карточных программ, так и от подходов к обмену картами. Например, совместное использование карты лояльности внутри домохозяйства или среди друзей, возможно, лишает магазин данных об отдельных людях, но всё же может предоставить полезную информацию об отдельных эпизодах покупок или предпочтениях товаров в определённых географических районах. Ценность данных в масштабе почтового индекса, микрорайона или района далеко не ничтожна. А из подлинной информации, присутствующей в смешанных и соединённых данных, могут быть выведены более крупные закономерности.

2.7. BitTorrent Hydra: применение поддельных запросов для предотвращения сбора адресов

Ныне прекративший существование, но интересный и показательный проект BitTorrent Hydra боролся с наблюдением со стороны противников обмена файлами, смешивая подлинные запросы фрагментов файла с фиктивными запросами.[10] Протокол BitTorrent разбивал файл на множество мелких частей и позволял пользователям обмениваться файлами, одновременно отправляя и получая эти части.[11] Вместо загрузки целого файла у другого пользователя человек собирал его из частей, полученных от любых располагавших ими участников, а любой нуждавшийся в имеющейся у вас части мог получить её от вас. Этот подход «много частей от многих людей» ускорил обмен файлами всех видов и быстро стал предпочтительным методом передачи больших файлов, например содержащих фильмы и музыку.[12] Чтобы помочь пользователям BitTorrent собрать нужные файлы, «торрент-трекеры» записывали IP-адреса, отправлявшие и получавшие файлы. Например, если вы искали определённые части файла, торрент-трекеры указывали адреса пользователей, располагавших нужными частями. Представители индустрии контента, разыскивая нарушения своих прав интеллектуальной собственности, начали запускать собственные трекеры, чтобы собирать адреса крупных несанкционированных отправителей и получателей, остановить их

или даже привлечь к ответственности. Hydra противодействовала такому отслеживанию, добавляя к найденной торрент-трекером совокупности адресов случайные IP-адреса из числа ранее использовавшихся для BitTorrent. Если вы запрашивали части файла, вас время от времени направляли к пользователю, у которого не было искомого. Создавая небольшую неэффективность для системы BitTorrent в целом, это существенно снижало полезность адресов, собранных теми, кто обеспечивал соблюдение авторских прав: адреса могли принадлежать настоящим участникам, а могли быть фиктивными адресами, вставленными Hydra. В систему вернулись сомнение и неопределённость, снизив вероятность того, что иск можно будет подать с уверенностью. Вместо попыток уничтожить журналы противника или скрыть трафик BitTorrent Hydra обеспечивала защиту «Я Спартак». Hydra не предотвращала сбор данных, но, снижая его надёжность, ставила под сомнение любые конкретные выводы.

2.8. Намеренно расплывчатый язык: сокрытие субъекта действия

По словам Жаклин Беркелл и Александра Фортье, политики приватности сайтов медицинской информации используют особенно непонятные языковые конструкции при описании применения отслеживания, наблюдения и сбора данных.[13] Среди выявленных Беркелл и Фортье конструкций - условные глаголы (например, «может»), страдательный залог, номинализация, наречия времени (например, «периодически» и «время от времени») и качественные прилагательные (как в выражении «небольшой фрагмент данных»). Какой бы тонкой ни казалась эта форма обфускации, по принципу действия она явно сходна с другими уже описанными формами: вместо конкретного, ложного отрицания (например, «мы не собираем сведения о пользователях») или точного признания расплывчатый язык создаёт множество запутанных намёков на возможную деятельность и ответственность. Например, предложение «Определённая информация может пассивно собираться для связи использования этого сайта со сведениями об использовании других сайтов, предоставленными третьими сторонами» помещает конкретные сведения о том, что сайт делает с определённой информацией, внутрь облака возможных толкований.

Подобные письменные практики отклоняются от обфускации как таковой в более общую область трудного для понимания языка и «слов-лазеек».[14] Однако для демонстрации диапазона обфускационных подходов стиль обфусцированного языка полезен: документ должен существовать, прямое отрицание невозможно, и потому стратегия состоит в том, чтобы сделать загадочным и неясным, кто и что делает.

2.9. Обфускация анонимного текста: противодействие стилометрическому анализу

Какая часть текста указывает, что его создал один автор, а не другой? Стилометрия устанавливает авторство анонимных текстов, используя лишь элементы языкового стиля. Ей не требуется учитывать вероятность того, что только определённый человек мог знать о каком-либо предмете, сообщения на сетевом форуме, другие внешние признаки (например, IP-адреса) или время. Она рассматривает длину предложений, выбор слов и синтаксис, особенности форматирования и словоупотребления, регионализмы и повторяющиеся опечатки. Именно стилометрический анализ помог разрешить спор о скрывавшихся за псевдонимами авторах «Записок федералиста» (например, употребление while в противоположность whilst помогло различить стили Александра Гамильтона и Джеймса Мэдисона), а полезность стилометрии в правовом контексте теперь прочно установлена.[15]

Имея небольшой объём текста, стилометрия способна установить автора. И под небольшим мы действительно понимаем небольшой: по словам Джосьюлы Рао и Панкаджа Ратанги, образца примерно из 6500 слов достаточно (при использовании корпуса атрибутированных текстов, например электронных писем, публикаций в социальной сети или сообщений в блоге), чтобы обеспечить 80-процентную вероятность успешной идентификации.[16] При повседневном использовании компьютеров многие люди создают 6500 слов за несколько дней.

Даже если цель состоит не в установлении конкретного автора из группы известных лиц, стилометрия может предоставить сведения, полезные для наблюдения. Технологический активист Даниэль Домшайт-Берг вспоминает момент, когда понял: если пресс-релизы WikiLeaks, краткие изложения утечек и другие открытые тексты подвергнут стилометрическому анализу, он покажет, что за всеми этими текстами стояли лишь два человека (Домшайт-Берг и Джулиан Ассанж), а не большая и разнообразная группа добровольцев, впечатление о которой старались создать Ассанж и Домшайт-Берг.[17] Стилометрический анализ даёт противнику более точное представление об «анонимном» или скрытном движении и его уязвимостях, чем можно получить иными способами. Сузив авторство до небольшой горстки людей, противник получает лучшие возможности нацелиться на известный набор вероятных подозреваемых.

Обфускация даёт практическую возможность размыть сигнал открытого корпуса текстов и помешать связыванию этого корпуса с названным автором. Стилометрическая обфускация отличается ещё и тем, что её успех легче проверить, чем успех многих других форм обфускации, точное воздействие которых может быть крайне неопределённым и/или известным лишь не склонному к сотрудничеству противнику.

Три подхода к преодолению стилометрии позволяют сделать полезные выводы об обфускации. Первые два, интуитивно понятные и прямолинейные, предполагают принятие стиля письма, отличного от обычного стиля автора; их слабости подчёркивают ценность применения обфускации.

Атаки с помощью перевода используют слабости машинного перевода: текст переводят на несколько языков, а затем обратно на исходный язык. Это игра в испорченный телефон, способная исказить стиль автора настолько, чтобы помешать атрибуции.[18] Разумеется, текст при этом становится менее связным и содержательным, а по мере совершенствования средств перевода они могут уже недостаточно хорошо справляться с обезличиванием.

При атаках с помощью имитации первоначальный автор намеренно пишет документ в стиле другого автора. Исследование изящно выявило одну уязвимость такого подхода.[19] С помощью систем, применяемых для установления принадлежности текстов одному автору, можно определить самый сильный признак авторства, различающий два текста, затем исключить этот признак из анализа и найти следующий по силе, после чего продолжать повторять тот же процесс исключения. Если тексты действительно написаны разными людьми, точность их различения будет снижаться медленно, поскольку за крупными очевидными различиями между авторами скрывается множество более мелких и менее надёжных различий. Но если оба текста написаны одним человеком, причём один имитирует другого автора, точность различения будет падать быстро, потому что под заметными особенностями останутся глубинные сходства, от которых трудно избавиться.

Обфускационные атаки на стилометрический анализ предполагают такой способ письма, при котором отличительный стиль отсутствует. Исследователи различают «поверхностную» и «глубокую» обфускацию текстов. «Поверхностная» обфускация меняет лишь небольшое число самых очевидных признаков, например предпочтение while или whilst. «Глубокая» обфускация запускает ту же систему классификаторов, которая применяется для преодоления имитации, но делает это на пользу автору. Такой метод мог бы в реальном времени предоставлять обратную связь автору, редактирующему документ, выявлять признаки с наивысшим рейтингом и предлагать изменения, снижающие точность стилометрического анализа, например сложное

перефразирование. Он мог бы превратить банальности «общепринятого словоупотребления» в ресурс, позволяя автору раствориться в огромной толпе похожих авторов.

Anonymouth - средство, которое на момент написания книги находилось в разработке, - представляет собой шаг к реализации этого подхода: оно создаёт статистически непримечательную прозу, которую можно обфусцировать внутри корпуса похожих текстов.[20] Вспомните автомобиль, предоставленный водителю для отхода в фильме «Драйв» 2011 года: серебристый Chevrolet Impala недавнего года выпуска, самый популярный автомобиль в Калифорнии, о котором механик обещает: «На тебя никто не посмотрит».[21] Каким бы изобретательным это ни было, нас тревожит будущее, где политические манифесты и критические документы стремятся к полной риторической и стилистической банальности, а мы теряем эквивалент слов следующего Томаса Пейна: «Настали времена, испытывающие человеческие души».

2.10. Обфускация кода: поставить в тупик людей, но не машины

В области программирования термин «обфусцированный код» имеет два связанных, но разных значения. Первое - «обфускация как средство защиты», то есть усложнение кода для понимания людьми (или различными видами «алгоритмов дизассемблирования», которые помогают объяснить код, скомпилированный для использования) ради предотвращения копирования, изменения или компрометации. (Классический пример такой обратной разработки выглядит следующим образом: Microsoft рассылает исправление, обновляющее компьютеры с Windows в целях безопасности; злоумышленники получают исправление и изучают код, чтобы выяснить, какую уязвимость оно должно устранить; затем они разрабатывают атаку, использующую обнаруженную уязвимость.) Второе значение «обфусцированного кода» относится к форме искусства: написанию кода, который дьявольски трудно распутать человеку, но который в конечном счёте выполняет обыденную вычислительную задачу, легко обрабатываемую компьютером.

Проще говоря, обфусцированная программа обладает той же функциональностью, что и прежде, но человеку труднее её анализировать. Такая программа демонстрирует две характеристики обфускации как категории и понятия. Во-первых, она действует в условиях ограничения: вы применяете обфускацию, потому что люди смогут увидеть ваш код, а цели обфускации как защиты состоят в снижении эффективности анализа («как минимум удваивая необходимое время», согласно экспериментальным исследованиям), сокращении разрыва между начинающими и опытными аналитиками и придании системам, на которые (по любой причине) легче нападать, профилей угроз, более близких к профилям систем, на которые нападать труднее.[22] Во-вторых, код обфусцированной программы использует стратегии, знакомые по другим формам обфускации: добавление бессмыслицы, которая кажется значимой; дополнительные переменные, которые необходимо учитывать; произвольные или намеренно запутывающие имена сущностей внутри кода; намеренно запутывающие указания внутри кода (по существу, «перейди к строке x и сделай y»), ведущие в тупики или заставляющие гоняться за призраками; и различные формы перемешивания. В защитном режиме обфускация кода представляет собой подход к срыву анализа посредством выигрыша времени, своего рода «лежачего полицейского». (В последнее время появились достижения, значительно повышающие трудность деобфускации и требуемое для неё время; мы обсудим их ниже.)

В своей художественной, эстетической форме обфускация кода находится на переднем крае противоречащих интуиции, загадочных методов достижения целей. Ник Монтфорт весьма подробно описал эти практики.[23] Например, благодаря тому, как язык программирования C интерпретирует имена переменных, программист может запутать человеческий анализ, не мешая машинному выполнению, если напишет код с буквами o и O в контекстах, где они обманывают глаз

сходством с нулями. Некоторые из этих форм обфускации немного выходят за рамки нашего рабочего определения «обфускации», но полезны для демонстрации подхода к её основной проблеме: как превратить открытое для изучения нечто в неоднозначный объект, полный ложных следов, ошибочных идентичностей и несбывшихся ожиданий.

Обфускацию кода, как и стилометрию, можно точно анализировать, проверять и оптимизировать. Её функциональность расширяется от ограниченной задачи выигрыша времени и усложнения распутывания кода к чему-то более близкому к достижению полной непрозрачности. Недавняя публикация Санджама Гарга и его коллег превратила обфускацию кода из «лежачего полицейского» в «железную стену». «Многолинейная головоломка» (Multilinear Jigsaw Puzzle) может разбить код так, чтобы он «собирался» подобно частям головоломки. Хотя возможны многие варианты расположения, правилен лишь один, и именно он представляет фактическую работу кода.[24] Программист может создать чистую, понятную человеку программу, а затем пропустить её через обфускатор и получить нечто непостижимое, способное выдерживать изучение гораздо дольше, чем прежде.

Обфускация кода - живая, богатая область для исследования обфускации в целом - по-видимому, движется к системам, которыми относительно легко пользоваться и которые чрезвычайно трудно преодолеть. Это применимо даже к аппаратному обеспечению: Джейявиджаян Раджендран и его коллеги используют компоненты внутри схем для создания «логической обфускации», чтобы предотвратить обратную разработку функций микросхемы.[25]

2.11. Личная дезинформация: стратегии исчезновения отдельного человека

Специалисты по исчезновению способны многому научить будущих обфускаторов. Многие из этих специалистов - частные детективы или профессионалы по розыску скрывающихся лиц, занимающиеся поиском беглецов и должников, - выполняют обратную разработку собственного процесса, чтобы помочь клиентам оставаться потерянными. Очевидно, многие применяемые ими приёмы и методы не имеют отношения к обфускации, а служат лишь уклонению или сокрытию: например, создаётся корпорация, которая может арендовать вашу новую квартиру и оплачивать счета, чтобы ваше имя не связывалось с этими обычными и доступными для открытого поиска действиями. Однако в ответ на распространение социальных сетей и сетевого присутствия специалисты по исчезновению рекомендуют стратегию дезинформации - разновидность обфускации. По словам консультанта по исчезновению Фрэнка Ахерна, можно создать столько подробно проработанных «фиктивных лиц», что они «похоронят» существовавшие ранее личные сведения, которые могли бы появиться в списке результатов веб-поиска.[26] Для этого создаётся несколько десятков вымышленных людей с тем же именем и теми же основными характеристиками; у некоторых есть личные сайты, у некоторых - учётные записи в социальных сетях, и все время от времени проявляют активность. Клиентам, спасающимся от преследователей или жестоких супругов, Ахерн рекомендует одновременно создавать многочисленные ложные следы, по которым, вероятно, пойдёт расследователь: например, запрос проверки кредитоспособности для аренды квартиры в одном городе (хотя договор аренды в действительности так и не подписан) и заявки на коммунальные услуги; адреса работы и телефонные номера, разбросанные по стране или миру; а также расчётный счёт с фиксированной суммой и дебетовой картой, переданной путешественнику для оплаты расходов в отдалённых местах. Предлагаемые специалистами по исчезновению стратегии основаны на известных подробностях о противнике: цель не в том, чтобы заставить человека «исчезнуть полностью», а в том, чтобы для практических целей убрать его достаточно далеко из поля зрения и тем самым исчерпать бюджет и ресурсы разыскивающего.

2.12. Патент Apple на «службу клонирования»: загрязнение электронного профилирования

В 2012 году в рамках приобретения у Novell более широкого патентного портфеля компания Apple получила патент США 8,205,265 «Методы загрязнения электронного профилирования».[27] Этот подход к управлению наблюдением за данными без отказа от услуг подобен нескольким уже описанным системам технологической обфускации. Такая «служба клонирования» автоматизировала бы и расширила процесс создания вводящих в заблуждение личных сведений, нацеливаясь не на частных детективов, а на сетевых сборщиков данных.

«Служба клонирования» наблюдает за действиями человека и составляет правдоподобную картину его ритмов и интересов. По запросу пользователя она порождает клонированную идентичность, способную применять предоставленные идентификаторы, чтобы подтвердить (для социальных сетей, если не для более требовательных наблюдателей), что она представляет настоящего человека. В число таких идентификаторов может входить небольшой объём подлинных конфиденциальных данных (несколько подробностей жизни, например цвет волос или семейное положение), смешанных со значительным объёмом намеренно неточных сведений. Отталкиваясь от исходного набора данных, клонированная идентичность получает адрес электронной почты, с которого будет отправлять и принимать сообщения, телефонный номер (многие сетевые службы звонков предоставляют номера за небольшую плату) и службу голосовой почты. У неё может быть независимый источник средств (возможно, подарочная или дебетовая карта, связанная со счётом с фиксированной суммой, который время от времени пополняется), позволяющий совершать небольшие операции. У неё может быть даже почтовый адрес или ячейка Amazon Locker - ещё два сигнала, указывающих на существование личности. К этим сигналам можно добавить некоторые формально заданные пользователем интересы и наполнить их существующими данными, ставшими доступными посредством сбора с сайтов социальных сетей и сходными способами. Если настраивающий клона пользователь выберет в раскрывающихся меню, что клон - американец и интересуется фотографией и туризмом, система установит, что клону следует интересоваться творчеством Анселя Адамса. Он может выполнять поиск (подобно TrackMeNot), переходить по ссылкам, просматривать страницы и даже совершать покупки и создавать учётные записи в службах (например, подписаться на рассылку предложений о путешествиях в дикую природу или следовать за учётной записью National Geographic в Twitter). Эти интересы могут опираться на настоящие интересы пользователя, выведенные из истории просмотра и других подобных источников, но способны постепенно, маленькими шагами отклоняться от них. (Можно также дополнить профиль клона демографически подходящими действиями, выбранными автоматически, и на основе настоящих исходных данных человека подобрать настолько типичные интересы и поведение, что они сгладят красноречивые особенности личности.)

Проведя несложный анализ, клон может также перенять ритмы и привычки человека. Если вы обычно не бываете в сети по выходным, вечерам и праздникам, ваш клон будет поступать так же. Он не будет работать непрерывно, а вы сможете отозвать его, если собираетесь сесть в самолёт, чтобы противнику было нелегко определить, какие действия принадлежат не вам. Клоны возобновят работу одновременно с вами. (Объяснение того, почему теперь мы говорим о нескольких клонах, см. ниже.) Разумеется, можно также выбрать классы действий, которыми ваши клоны заниматься не будут, чтобы выдающие себя за вас действующие лица не пиратствовали с медиаконтентом, не начали искать инструкции по изготовлению бомб и не смотрели порнографию, если только им не потребуется сделать это ради сохранения правдоподобия: если все ваши клоны будут вести безупречный образ жизни и окажутся серьёзными пользователями сети, интересующимися только историей, благотворительностью и рецептами, это может вызвать

подозрения. (Мы перешли от единственного клона к множеству, потому что после запуска одного появится много других. Представьте даже борхесовскую шутку, где достаточно развитые клоны, обучившись на вашей истории, демографических характеристиках и привычках, создают собственных клонов - копии копий.) В ваших интересах расширять эту популяцию возможных «я», день за днём проживающих жизни, которые могли бы быть вашими. Тем самым достигается основная цель патента: клоны не уклоняются от сбора данных и не отказываются от него, но, подчиняясь, загрязняют собранные данные и снижают ценность созданных на их основе профилей.

2.13. Vortex: обфускация файлов cookie как игра и рынок

Vortex - игра (своего рода) для проверки концепции, разработанная художником, дизайнером и программистом Рэйчел Лоу[28], - одновременно выполняет две функции: рассказывает игрокам, как сетевые системы фильтрации влияют на их восприятие Интернета, и запутывает и направляет по ложному пути таргетированную рекламу, основанную на файлах cookie браузера и других системах идентификации. Она работает как игра, занимая и радуя человека, - превосходная площадка для вовлечения пользователей в тему, которая кажется столь сухой и отвлечённой, как таргетированная реклама на основе cookie. Иными словами, это массовая многопользовательская игра по управлению личными данными и обмену ими. Основные действия - «добыча» cookie на сайтах и обмен ими с другими игроками. В одном состоянии игра выглядит как несколько кнопок с цветовой кодировкой на панели закладок браузера, позволяющих накапливать cookie и переключаться между ними (фактически принимая разные идентичности); в другом она выглядит как ландшафт, где сайт представлен подобием планеты, на которой можно добывать cookie. (Представление в виде ландшафта отчасти вдохновлено популярной игрой об исследовании и строительстве Minecraft.)

Vortex изобретательно предлагает увлекательный и дружелюбный способ отображать файлы cookie, управлять ими и делиться ими. Создавая и собирая cookie и обмениваясь ими с другими игроками, вы можете одним щелчком переключаться между cookie, фактически маскируя себя и воспринимая другую Всемирную паутину, другой набор фильтров, другое сетевое «я». Это превращает таргетированную рекламу в своего рода выбор: можно переключиться на cookie, представляющие вас человеком другого пола, этнической принадлежности, профессии и с другим набором интересов; можно превратить рекламу и «персонализированные» подробности в простой фоновый шум, а не в отвлекающие и манипулятивные компоненты, которые подгоняют вас под модель вашей идентичности, созданную каким-либо маркетологом. Можно воспринимать Всемирную паутину как множество разных людей, а любую запись о себе превращать в портрет, от которого можно убедительно отречься и который имеет мало общего именно с вами. В доверенном кругу друзей можно делиться файлами cookie учётных записей, позволяющими приобретать недоступные в вашем местоположении вещи, например видеопотоки, доступные только зрителям из определённой страны.

Перескакивая от одного «я» к другому и тем самым разрушая процесс составления демографических досье, игроки Vortex превратили бы сетевую идентичность в поле возможностей, подобное экранам инвентаря сетевой ролевой игры. Вместо того чтобы скрываться или отказываться от преимуществ, которые могут дать cookie и персонализация, Vortex позволяет пользователям задействовать толпу идентичностей, одновременно предлагая собственную идентичность множеству других людей.

2.14. «Байесовское наводнение» и «обесценивание» сетевой идентичности

В 2012 году разработчик и предприниматель Кевин Ладлоу обратился к знакомой проблеме обфускации: как лучше всего скрыть данные от Facebook?[29] Короткий ответ: хорошего способа удалить данные нет, а полный уход из социальных сетей для многих пользователей нереалистичен. Ответ Ладлоу теперь уже знаком.

«Вместо попыток скрыть информацию от Facebook, - писал Ладлоу, - возможно, его следует просто завалить чрезмерным объёмом информации». Эксперимент Ладлоу (который он назвал «байесовским наводнением» по форме статистического анализа) состоял во внесении на протяжении нескольких месяцев сотен жизненных событий в его Хронику Facebook - событий, в совокупности составлявших жизнь, достойную трёхтомного романа. Он женился и разводился, боролся с раком (дважды), ломал многочисленные кости, становился отцом детей, жил по всему миру, исследовал десяток религий и сражался в целом ряде иностранных вооружённых сил. Ладлоу не ожидал, что кто-нибудь поверит этим историям; он стремился создать менее таргетированный личный опыт использования Facebook посредством неточных догадок, на которые теперь реагирует реклама, и выразить протест против манипуляций и «принудительных психологических уловок», встроенных как в саму рекламу, так и в механизмы сайта, побуждающие или склоняющие пользователей вводить больше сведений, чем они намеревались. На самом деле полная неправдоподобность жизни Ладлоу в Хронике - жизни путешествующего по всему миру распутного мистика-наёмника с невероятным невезением - действует как своего рода фильтр: ни один читатель-человек и уж точно ни один друг или знакомый Ладлоу не решил бы, что всё это правда, но лежащий в основе рекламы анализ не способен проводить такие различия.

Ладлоу предполагает, что при более широком принятии его подхода выявлять резкие географические, профессиональные или демографические выбросы - людей, Хроники которых слишком переполнены происшествиями, - и затем вымывать их результаты из более широкого анализа было бы нетрудно. Особое понимание победы, которое представляет Ладлоу и которое мы обсуждаем в типологии целей во второй части этой книги, ограниченно. Его байесовское наводнение предназначено не для противодействия огромному масштабу сбора и анализа данных и не для его искажения, а для того, чтобы оставить данные о себе внутри системы, одновременно сделав их недоступными. Макс Чо описывает менее крайнюю версию: «Хитрость в том, чтобы наполнить свой Facebook ровно таким количеством лжи, которое уничтожит ценность и подорвёт способность Facebook продавать вас»[30], то есть затруднить превращение вашей сетевой деятельности в товар в качестве акта убеждения и протеста.

2.15. FaceCloak: сокрытие самой работы по сокрытию

FaceCloak предлагает иной подход к ограничению доступа Facebook к личным сведениям. Когда вы создаёте профиль Facebook и заполняете личную информацию, в том числе где живёте, где учились, что вам нравится и не нравится и так далее, FaceCloak позволяет выбрать, отображать ли эти сведения открыто или сохранить их в тайне.[31] Если вы решите показывать информацию открыто, она передаётся на серверы Facebook. Если вы решите сохранить её в тайне, FaceCloak отправляет её в зашифрованное хранилище на отдельном сервере, где она может быть расшифрована и показана только разрешённым вами друзьям, когда они просматривают вашу страницу Facebook с помощью плагина FaceCloak. Facebook никогда не получает к ней доступа.

Для наших целей существенно то, что FaceCloak обфусцирует свой метод: создаёт поддельные сведения для обязательных полей профиля Facebook, скрывая от Facebook и неавторизованных

зрителей сам факт хранения настоящих данных в другом месте. Передавая настоящие данные на частный сервер, FaceCloak создаёт для Facebook правдоподобную несуществующую личность определённого пола, с именем и возрастом, никак не связанными с настоящими фактами о вас. Под прикрытием правдоподобной несуществующей личности вы можете устанавливать настоящие связи с друзьями, одновременно предъявляя остальным обфусцированные данные.

2.16. Обфусцированная накрутка отметок «Нравится»: сокрытие признаков манипуляции

Накрутка отметок «Нравится» теперь хорошо известна как стратегия создания иллюзии популярности в Facebook: работники, обычно в развивающихся странах, за плату ставят отметку «Нравится» определённой марке или товару (текущая цена - несколько долларов США за тысячу отметок).[32] Объекты с большим числом отметок получают ряд преимуществ: помимо прочего, алгоритмы Facebook распространяют страницы с признаками популярности, придавая им дополнительный импульс.

Накрутку легко обнаружить, особенно столь сложным системам, как системы Facebook. Она выполняется узконаправленными всплесками активности, посвящёнными отметкам одного объекта или одного семейства объектов, из учётных записей, почти не занимающихся ничем другим. Чтобы выглядеть естественнее, они применяют обфускационную стратегию, ставя отметки множеству страниц - обычно недавно добавленных в ленту Page Suggestions, которую Facebook продвигает в соответствии со своей моделью интересов пользователя.[33] Оплачиваемую работу по систематическому проставлению отметок одной странице можно скрыть среди разрозненных отметок, которые выглядят исходящими от человека со странно узкими, но безликими интересами. Накрутка демонстрирует разнообразие мотивов обфускации: в данном случае не сопротивление политическому господству, а простое оказание услуги за плату.

2.17. URME Surveillance: «протезы идентичности» как выражение протеста

Художник Лео Сельваджо хотел поработать с видеонаблюдением в общественном пространстве и последствиями применения программ распознавания лиц.[34] Рассмотрев обычный набор ответов (ношение маски, уничтожение камер, ироничное привлечение внимания в духе Surveillance Camera Players), Сельваджо нашёл особенно обфускационный ответ с протестной остротой: изготовил и распространил маски своего лица, достаточно точные для того, чтобы программа распознавания лиц Facebook помечала носивших их людей как его.

Описание проекта Сельваджо даёт краткое резюме обфускации: «Вместо попытки скрыть или заслонить своё лицо от камеры эти устройства позволяют предъявить камере другую, альтернативную идентичность - мою собственную».

2.18. Создание противоречащих друг другу доказательств: как сбить расследование с толку

«Искусство политического убийства: кто убил епископа?» - рассказ Франсиско Голдмана о расследовании смерти епископа Хуана Хосе Херарди Конедеры - показывает применение

обфускации для замутнения вод сбора доказательств.[35] Епископ Херарди, сыгравший чрезвычайно важную роль в защите прав человека во время гражданской войны в Гватемале 1960-1996 годов, был убит в 1998 году.

Документируя долгий и опасный процесс привлечения к ответственности за это убийство хотя бы нескольких виновных из гватемальских вооружённых сил, Голдман заметил, что люди, которым угрожало расследование, не просто подбрасывали доказательства, скрывая свою роль. Подставить кого-то другого было бы очевидной тактикой, и подброшенные доказательства сочли бы ложными. Вместо этого они создавали слишком много противоречивых доказательств, слишком много свидетелей и показаний, слишком много возможных историй. Цель состояла не в построении безупречной лжи, а в столь обильном умножении возможных гипотез, чтобы наблюдатели отчаялись когда-либо добраться до истины. Обстоятельства убийства епископа создали то, что Голдман называет «бесконечно пригодной для эксплуатации ситуацией», полной ведущих в никуда следов и гор изъятых доказательств, где каждый фактический элемент ставил под сомнение остальные. «Так много можно было связать и так много заставили бы казаться связанным», - пишет Голдман, курсивом подчёркивая силу неоднозначности.[36]

У головорезов из гватемальских вооружённых сил и разведывательных служб было множество способов управлять ситуацией: доступ к внутренней политической власти, деньгам и, разумеется, насилию и угрозе насилия. Учитывая, насколько неясной остаётся ситуация, мы не хотим строить предположения о конкретных решениях, но основная цель кажется достаточно ясной. На самых непосредственно значимых противников - следователей, судей, журналистов - можно было воздействовать убийством, угрозами, подкупом или иными средствами. Обфусцирующие доказательства и другие материалы предназначались более широкому сообществу наблюдателей: распространение ложных следов набрасывало на каждую сторону расследования достаточно отнимающего время сомнения, чтобы поставить под вопрос продолжающуюся работу и любые выводы.

Глава 3. Почему обфускация необходима?

Часть II. Понимание обфускации

> Где мудрец прячет лист? В лесу. Но что он делает, если леса нет? … Он выращивает лес, чтобы спрятать лист в нём.
>
> Г. К. Честертон, «Знак сломанного меча»

3.1. Кратко об обфускации

Приватность - сложное и даже противоречивое понятие, слово с настолько широкими значениями, что в некоторых случаях оно способно вводить в заблуждение или почти утрачивать смысл. Оно выражается в праве и политике, технологиях, философии и повседневном разговоре. Оно охватывает пространство от панели управления на сайте - ваших настроек приватности, которыми управляют с помощью раскрывающихся меню и переключателей, - до всеобъемлющего спора о развитии человеческого общества. Одни говорят, что приватность - устаревшая идея, двухвековая аномалия западной индустриализации, междуцарствие между деревенской жизнью и социальными сетями; что приватность позволяет нам развиваться как свободомыслящим, независимым личностям; что приватность - выражение буржуазного лицемерия и недобросовестности; что приватность - защита социального разнообразия…[1] Это показывает не просто способы употребления слова. Стоит немного подумать, и становится ясно, что за этими употреблениями стоят расходящиеся понятия. В доме приватности много комнат. Одни связаны с неприкосновенностью семейной жизни, другие - с государственным угнетением (нынешним или будущим), третьи - с полезностью и ценностью данных, четвёртые - с подлинным внутренним «я», способным проявиться только в анонимности; при этом многие комнаты пересекаются и соединяются дверями.[2] Это концептуальное разнообразие переносится на стратегии, практики, технологии и тактики, применяемые для создания, осуществления и защиты приватности.[3] В других работах мы показали, как многие из этих концепций можно объединить под знаменем контекстуальной целостности, однако здесь нас интересуют связи между этими проблемами в их конкретных формулировках и то, как нам следует защищаться.[4]

Цель этой главы - описать, что такое обфускация и как она вписывается в разнообразный ландшафт интересов приватности, угроз этим интересам и методов противодействия угрозам. Приватность - многогранное понятие, и для её создания и защиты доступен широкий спектр структур, механизмов, правил и практик. Если открывать ящик с инструментами приватности, один метафорический выдвижной ящик за другим, мы найдём политику и право местного, национального и мирового уровней; технологии с доказуемой безопасностью, такие как криптография; действия и практики отдельных лиц по раскрытию сведений; социальные системы конфиденциальности (например, у журналистов, священников, врачей и адвокатов); стеганографические системы; коллективное утаивание и омерту со стороны сообщества; и многое другое. Мы найдём BlackNet Тимоти Мэя, приложение криптографических технологий для описания полностью анонимного рынка информации с неотслеживаемыми, не облагаемыми налогами сделками, который способствует корпоративному шпионажу и распространению военных тайн, запрещённых и засекреченных материалов и в долгосрочной перспективе ставит целью «крах правительств».[5] Мы найдём правовую работу на основе Четвёртой поправки к Конституции США по созданию защиты

сетей связи и социальных сайтов, стремящуюся установить равновесие между правами отдельных граждан и полномочиями правоохранительных органов. К этому разнообразному набору мы добавим обфускацию - и как самостоятельный метод, и как подход, который в зависимости от цели можно применять внутри и наряду с другими методами. Мы стремимся убедить читателей, что для одних проблем приватности обфускация служит правдоподобным решением, а для некоторых - наилучшим.

В самом отвлечённом виде обфускация - это создание шума, смоделированного по существующему сигналу, чтобы сделать совокупность данных более неоднозначной, запутанной, менее пригодной для эксплуатации, более трудной для практического применения и потому менее ценной. Для этой деятельности выбрано слово «обфускация», поскольку оно подразумевает неясность, непонятность и замешательство и помогает отличить этот подход от методов, основанных на исчезновении или стирании. Обфускация предполагает, что сигнал каким-либо образом можно заметить, и добавляет множество связанных, похожих и уместных сигналов - толпу, с которой человек может смешаться, слиться и хотя бы ненадолго спрятаться.

Вспомним генерала сэра Артура Сент-Клэра, вымышленного военного мученика из рассказа Г. К. Честертона «Знак сломанного меча». Солдаты генерала Сент-Клэра были перебиты в непродуманной атаке на вражеский лагерь. Почему блестящий стратег предпринял заведомо неудачное наступление на превосходящую позицию противника? Церковный сыщик Честертона, отец Браун, отвечает вопросом: «Где мудрец прячет камешек?» - «На пляже», - отвечает его друг.[6] И лист он прячет в лесу, продолжает Браун, а если ему нужно спрятать тело, он должен создать множество мёртвых тел, среди которых оно затеряется. Чтобы защитить свою тайну, генерал Сент-Клэр убивает одного человека, а затем скрывает его в хаосе других мертвецов, который создаёт, приказав внезапно атаковать артиллерию, занимавшую господствующую высоту.

Риторический вопрос отца Брауна повторил достопочтенный лорд-судья Джейкоб в патентном деле 2007 года:

> Можно предположить, что выполнить такое массовое раскрытие дешевле, чем внимательно рассмотреть документы и решить, следует ли их раскрывать. И на этом этапе это действительно может оказаться дешевле: просто пропустить всё через копировальный аппарат или устройство записи компакт-дисков, особенно поскольку это допустимые расходы. Но дело не в этом. Ведь последующие затраты, вызванные чрезмерным раскрытием, столь часто бывают огромными и совершенно бессмысленными. Можно даже сказать, что в случаях массового чрезмерного раскрытия существует реальный риск упустить действительно важные документы: где мудрец прячет лист?[7]

От мёртвых солдат до раскрытых документов мы видим, что сущность обфускации состоит в том, чтобы заставить вещи остаться незамеченными и увеличить стоимость, хлопоты и трудность поиска.

Обфускацию полезно сравнить с камуфляжем. Камуфляж часто считают средством полного исчезновения: вспомните сцену из «Симпсонов», где Милхаус воображает, как надевает камуфляжный костюм и растворяется в зелени, оставляя видимыми лишь очки и улыбку.[8] На практике и естественный, и созданный человеком камуфляж использует разнообразные приёмы и цели, лишь некоторые из которых направлены на попытку полностью исчезнуть из поля зрения; другие применяют «разрушающие рисунки», скрывающие края, контур, ориентацию и движение формы с помощью фрагментов и намёков на другие возможные формы. Разрушение контуров не заставляет форму исчезнуть полностью, как бывает, когда камбала зарывается в песок или осьминог с помощью мантии выдаёт себя за камень. Напротив, в ситуациях, когда избежать наблюдения невозможно - когда мы движемся, меняем положение или иным образом оказываемся открыты, - разрушающие рисунки и разрушающая окраска мешают оценивать расстояние, размер, скорость, количество и тому подобное. Они затрудняют идентификацию отдельного объекта и

наведение на него, а также подсчёт членов группы. Многие ранние военные применения камуфляжа были посвящены тому, чтобы затруднить точную оценку с воздуха крупных, плохо скрываемых объектов, например артиллерийских позиций. В ситуациях, где исчезнуть нельзя, создание многочисленных возможных целей или векторов движения способно посеять замешательство и выиграть драгоценное время. Если у обфускации есть символическое животное, то это семейство пауков-кругопрядов Cyclosa mulmeinensis (упомянутых в главе 2), которые заполняют паутину собственными подобиями. Эти ложные цели далеко не совершенны, но при атаке осы действуют достаточно хорошо, чтобы дать кругопряду секунду или две для бегства в безопасное место.

В своей истории камуфляжа «Прятки: камуфляж, фотография и средства разведки» Ханна Роуз Шелл развивает тему «камуфляжного сознания» - способа существования и действия, основанного на внутренней модели технологии наблюдения, которой человеку приходится противостоять.[9] Шелл утверждает, что создающий рисунки специалист по маскировке, обучающий солдат специалист и сами солдаты на поле боя пытались определить свою видимость для биноклей и оптических прицелов винтовок, фото- и кинокамер, самолётов, наблюдателей и спутников и действовать так, чтобы уменьшить эту видимость. Для этого приходилось сочетать исследования, оценки, моделирование и догадки, используя недостатки и ограничения технологии наблюдения. Камуфляж, стремившийся либо к полной невидимости мимикрии, либо к временному решению в виде сокрытия формы в беспорядке других неоднозначных обфусцирующих возможных форм, всегда отражал возможности технологии, против которой его разрабатывали.

Нас здесь интересуют формы обфускации данных или информации - их техническая полезность для проектировщиков, разработчиков и активистов. Чтобы понять нравственную и этическую роль таких форм обфускации, необходимо понять технологии получения и анализа данных, которым они могут бросить вызов и помешать. Необходимо понять модели угроз, цели и ограничения. Обфускация - одно из средств построения и защиты приватности наряду с другими, и, как всякое средство, она оттачивается в соответствии с целями, которым может служить, и проблемами, которые может решить. Чтобы изложить природу этих проблем, мы вводим понятие информационной асимметрии.

3.2. Понимание информационной асимметрии: знание и власть

Вспомним теперь знаменитое запутанное объяснение Дональдом Рамсфелдом расчёта риска накануне вторжения в Ирак: «Есть известные известные, о которых мы знаем, что знаем; известные неизвестные, о которых мы знаем, что не знаем; и неизвестные неизвестные, о которых мы не знаем, что не знаем».[10] Как бы это ни напоминало намеренную логическую головоломку, объяснение различает три совершенно разные категории опасности. Мы можем увидеть камеру наблюдения, установленную на уличном фонаре или скрытую в куполе зеркального стекла на потолке коридора, и знать, что нас записывают. Мы знаем, что не знаем, передаётся ли запись лишь в пределах объекта или транслируется через Интернет в какое-то удалённое место. Мы знаем, что не знаем, как долго будет храниться запись и кому разрешено её просматривать: только ли охраннику в прямом эфире, страховому инспектору при наступлении страхового случая или полиции?

У такой, казалось бы, простой вещи, как запись системы видеонаблюдения, имеется гораздо более широкая категория неизвестных неизвестных. Мы не знаем, можно ли, например, обработать запись программой распознавания лиц или походки, можно ли сопоставить временной код с покупкой по кредитной карте или с номерным знаком машины, из которой мы вышли, чтобы связать наше изображение с нашей личностью; более того, если мы лично не занимаемся активизмом в области приватности или инженерией безопасности, то даже не знаем, что не знаем этого. Как бы

запутанно это ни звучало, тройное отрицание в предыдущем предложении не только точно, но и указывает на слои неопределённости: мы не осознаём, что не можем быть уверены в том, что видеофайл не проанализируют прогнозные демографические средства для выявления вероятных преступников или террористов и их допроса. Даже этим неизвестные не исчерпываются, и все они потенциально формируют важные решения, возникающие в плотном облаке нашего незнания. И это лишь одна камера видеонаблюдения, чей кабель или беспроводная передача заканчивается где-то на каком-то жёстком диске, резервная копия которого может находиться где-то ещё: в каких юрисдикциях, на каких условиях, при каких деловых договорённостях? Умножьте это на покупку по кредитной карте, подписку на рассылку, загрузку приложения для смартфона («Этому приложению требуется доступ к вашим контактам»? «Конечно!»), сообщение почтового индекса, даты рождения или идентификационного номера в ответ на разумный и законный запрос - и так далее в течение всего дня и по всему миру.

Очевидно, что сбор информации происходит в асимметричных властных отношениях: у нас редко есть выбор, наблюдают ли за нами, что делают с собранной информацией или что делают с нами на основе выведенных из неё заключений. Если вы хотите поехать на поезде, позвонить, воспользоваться гаражом или купить продукты, вы подвергнетесь сбору информации и откажетесь от части или всего контроля над отдельными её элементами. Речь редко идёт о явном соглашении в пространстве полной информации и осознанного выбора. Чтобы получить критически важные ресурсы или участвовать в гражданской жизни, вам придётся заполнять определённые формы, а чтобы пользоваться программой, которая может требоваться на работе, придётся согласиться с обременительными условиями обслуживания. Более того, инфраструктура по умолчанию собирает данные о вас. Обфускация связана с этой проблемой асимметрии власти: как подсказывает сравнение с камуфляжем, это подход, подходящий ситуациям, где мы не можем легко уйти от наблюдения, но должны двигаться и действовать. Однако данная проблема - лишь поверхностная сторона сбора информации, то, что мы знаем, что знаем. Вторая сторона, информационная или эпистемическая асимметрия, представляет собой более глубокую и пагубную проблему и сильнее влияет на формирование обфускации для защиты приватности.

Брэд Темплтон, председатель Electronic Frontier Foundation, рассказал об опасности «путешествующих во времени роботов из будущего»[11], которые с более мощным оборудованием и совершенными программами, чем есть у нас сегодня, возвращаются во времени и подвергают нас полному наблюдению; они соединяют разрозненные (и, как мы считали, незаметные) точки нашей жизни, превращая поток нашего личного опыта в слишком ясные, слишком человеческие закономерности, и направляют мощный свет анализа в тёмные углы прошлого. Эти роботы из будущего - наёмники, работающие на любого, кто достаточно богат, чтобы их нанять: рекламодателей, отрасли, правительства, заинтересованные стороны. Мы бессильны помешать им сопоставлять и собирать наши истории, потому что, в отличие от них, не можем путешествовать во времени и менять прошлые действия.

Однако история Темплтона - не научная фантастика. Каждый день мы создаём огромные объёмы данных. Эти данные сохраняются на неопределённый срок, а технологии, способные сопоставлять и анализировать их, продолжают совершенствоваться. То, что мы когда-то считали приватным, если вообще об этом задумывались, становится открытым, видимым и осмысленным для новых технологий. Это одна из сторон информационной асимметрии, формирующей наши практики приватности и автономии: мы не знаем, что алгоритмы, методы, оборудование и базы данных ближайшего будущего смогут делать с нашими данными. Постоянно наступает фронт перехода от бессмысленного к осмысленному: от мелких жизненных событий к вещам, которые могут изменить наши налоги, страховые тарифы, доступ к капиталу, свободу передвижения или решить, попадём ли мы в список.

Таково неизвестное будущее, но информационные асимметрии должны беспокоить нас и в настоящем. Сведения о нас ценны, и они перемещаются. Собравшая информацию о нас компания

может связать её с другими разрозненными массивами записей (журналами телефонных звонков, сведениями о покупках, персональными идентификационными данными, демографическими списками, действиями в социальных сетях, геолокационными данными), а затем упаковать эти сведения и продать другим компаниям или передать в ответ на государственный запрос либо судебную повестку. Даже если управляющие компанией люди обещают хранить информацию у себя, при банкротстве она может войти в перечень имущества, а затем быть приобретена или распродана. Вся работа по сопоставлению и анализу выполняется средствами и людьми с подготовкой, лежащими за пределами чего-либо большего, чем поверхностное понимание большинства тех, на кого она влияет. Население в целом не имеет доступа к другим базам данных, методам, математической и компьютерной подготовке, программному и аппаратному обеспечению, необходимым, чтобы понять, что можно сделать с кажущимися незначительными подробностями их жизни и деятельности и как такие подробности потенциально способны дать более мощный, более полный и более разоблачающий анализ, чем могли предвидеть обычные пользователи, - и даже более разоблачающий, чем могли предвидеть сами инженеры и аналитики.

Тал Зарски, один из ведущих теоретиков интеллектуального анализа данных, описал тонкую ловушку прогнозного программного обеспечения - ещё один, дальнейший шаг асимметрии. Прогнозные системы используют огромные существующие наборы данных для создания предсказаний человеческой деятельности: они делают точные или неточные прогнозы, которые применяют для принятия решений и получения принудительных результатов, а людей наказывают или вознаграждают за то, чего они ещё не сделали. Возможности дискриминации и манипуляции очевидны. Однако, как объясняет Зарски, у этих опасений есть ещё один слой: «Неинтерпретируемый процесс может возникнуть в результате анализа данных, который невозможно объяснить человеческим языком. Здесь программа принимает решения об отборе на основе множества переменных (даже тысяч). … Правительству было бы трудно дать подробный ответ на вопрос, почему автоматизированная рекомендательная система выделила конкретного человека для отличающегося обращения. Самое большее, что могло бы сказать правительство: именно это алгоритм обнаружил на основе предыдущих случаев».[12]

Развивая эти идеи, Солон Барокас показывает, насколько мы уязвимы перед агрегированием данных, аналитикой и прогнозным моделированием, которые теперь принято называть «большими данными». Методы больших данных берут информацию, которой мы добровольно поделились или которую нас заставили предоставить, и посредством выводов создают знания, которых мало кто, и менее всего мы, отдельные субъекты данных, мог предвидеть.[13] Дело не только в том, что решение принимается и принудительно исполняется. Мы даже не можем быть полностью уверены, что знаем, почему решение принято и исполнено, потому что в предельном непознаваемом неизвестном сбора данных сами принимающие решение не знают, почему оно принято и исполнено. Нам остаётся гадать о внутренней работе непрозрачной операции. Мы не понимаем оснований суждения. Мы находимся в состоянии информационной асимметрии.

Поскольку это рассуждение частично построено на том, чего мы не знаем и в действительности не можем знать, оно рискует оказаться несколько отвлечённым. Но мы можем сделать его совершенно конкретным и обсудить другую грань проблемы информационной асимметрии, ненадолго обратившись к теме риска. Подумайте о «риске» в выражении «кредитный риск». Как показало исследование Джоша Лауэра, управление кредитом имело решающее значение в истории сбора данных, составления досье и интеллектуального анализа данных.[14] Преобразования торгового и общественного строя Соединённых Штатов в XIX веке заставили компании выдавать кредиты клиентам, не располагая «личным знакомством и мнением сообщества», которые прежде учитывались при оценке доверия и риска. Вместо «личного знакомства и мнения сообщества» они полагались на кредитные бюро, собиравшие данные для принятия обоснованных решений о том, получат ли люди ссуды, страхование, аренду и другие связанные с риском вещи. К концу 1920-х годов отчёты и анализ кредитных бюро составляли частную систему наблюдения, по масштабу

намного превосходившую любой внутренний проект правительства США. Это привело к нескольким крупным последствиям, среди которых принудительная оценка характера, встроенная в «финансовую идентичность» человека, и возникновение таргетированного маркетинга по мере изобретения новых способов использования накопленных данных. Одно последствие особенно важно для нашего рассуждения. Оно в полной мере проявляется с появлением цифровых баз данных и средств и состоит в том, что кредитная отчётность действительно снижает риск, но при некоторых обстоятельствах также экспортирует риск. (Эти последствия относятся к области «произведённых рисков» Энтони Гидденса: опасностей, которые создаёт, а не смягчает процесс модернизации и для которых, в свою очередь, требуются новые системы смягчения.[15])

В процессе снижения риска для кредитора, страховой компании или предприятия, открывающего клиенту кредитную линию, риски для самого человека возрастают. Один риск - кража личности: вам приходится доверять субподрядчику универмага, кем бы он ни был, и рассчитывать, что тот соблюдает безупречные правила безопасности. Другой - риск нарушения контекста, например магазин может продать данные сомнительным брокерам данных, поделиться ими с партнёрами, допустить их приобретение вместе с остальной компанией или их неизбирательный сбор государством в ходе какого-либо более широкого проекта сбора данных. Возможно, это справедливый обмен, но важно помнить, что риск не исчезает благодаря сбору данных: держатели данных создают и выносят наружу новые формы риска. Эти риски будете нести вы и другие люди, для более качественного анализа и понимания которых могут использоваться ваши данные. В более широком масштабе проекты наблюдения и сбора данных, запускаемые нашими правительствами во имя безопасности, всегда направлены на защиту от одного класса рисков, от которых должно защищать государство, но создают другой класс рисков, опасность которых принимают на себя граждане: риск подавления инакомыслия, риск разгрома законной оппозиции или просто риск несчастных случаев, при которых невинных людей задержат, будут отслеживать, раскроют и накажут. Это случаи, когда увеличение объёма и подробности собранной информации снижает риск для одних и одновременно повышает его для других; с таким проявлением информационной асимметрии мы сталкиваемся ежедневно и считаем, что определённые формы обфускации способны помочь его исправить.

«Они» (или целый ряд разных «их») знают о нас многое, а мы мало знаем о них или о том, что они могут сделать. В ситуациях со столь асимметричными знанием, властью и риском трудно спланировать эффективные ответы, не говоря уже об их осуществлении. Это не асимметрии священника или любопытного человека в маленьком городе, где люди знают дела друг друга, а некоторые знают больше остальных. Описанное нами отличается из-за схождения асимметрий: знающие о нас имеют над нами власть. Они могут отказать нам в работе, лишить кредита, ограничить передвижение, отказать в жилье, членстве или образовании и ограничить наш доступ к хорошей жизни.

3.3. Иллюзия отказа от участия

Разумеется, мы всё-таки сами выбираем участие в этих асимметричных отношениях, не так ли? При большинстве форм сбора данных часть вины должна лежать на людях, которые пользуются службами или взаимодействуют с учреждениями, предлагающими невыгодные условия обслуживания и известными плохим поведением. Разве несправедливо целиком винить государственные учреждения и частные службы, когда они стараются поддерживать безопасность и получить часть ценных данных, создаваемых их пользователями? Разве это не подвергает пользователей классическому моральному риску, заставляя поставщиков услуг принимать на себя бремя риска и ответственности за выбор, сделанный пользователями? Разве мы, пользователи, не можем просто выйти из систем, с которыми не согласны?

Чтобы увидеть, насколько простой отказ от участия становится всё менее разумным, рассмотрим один день из жизни вполне обычной женщины в большом городе стабильной страны с демократическим правлением. Она не находится в тюрьме или закрытом учреждении, не является диссиденткой или врагом государства, но живёт в условиях постоянного и полного наблюдения, не имеющего прецедентов по точности и близости. Как только она выходит из квартиры, она попадает на камеру: в коридоре и лифте своего дома, при использовании банкомата у банка (который создаёт крупный план с временной меткой, связанной с записью о снятии денег), проходя мимо магазинов и ожидая на пешеходных переходах, на станции метро и в поезде, в вестибюле, лифте и своей кабинке на рабочем месте - и всё это до обеда. Можно было бы смонтировать запись почти каждого движения её городской жизни вне квартиры и учесть каждый шаг, особенно если она решит надеть устройство отслеживания физической активности. Но такой монтаж едва ли понадобился бы: мобильный телефон в ходе обычной работы, разыскивая базовые станции и антенны для сохранения связи во время ходьбы, постоянно записывает её положение и перемещения. Можно учесть даже время, проведённое в «мёртвых зонах» без телефонной связи: проездной регистрирует её вход в метро, а радиочастотный идентификационный пропуск создаёт запись о входе в здание, где она работает. (Если она водит автомобиль, сходной цели служит электронный транспондер оплаты проезда, как и автоматическое фотографирование номерных знаков.) Если её квартира входит в программу интеллектуальной электросети, всплески потребления электричества могут точно показать, когда она встаёт и начинает двигаться, включая свет, вентиляторы, микроволновую печь и кофеварку.

Прежде чем вернуться к вопросу отказа от участия, рассмотрим, насколько глубоко упомянутые в предыдущем абзаце системы встроены в повседневную жизнь нашей гипотетической обычной женщины и насколько сильнее простых журналов её ежедневных приходов и уходов они вторгаются в эту жизнь. Наблюдатель мог бы с криминалистической подробностью восстановить её социальные и семейные связи, трудности и интересы, убеждения и обязательства. Покупки на Amazon и выделенные места в Kindle, записи о покупках, связанные с картами лояльности в аптеке и супермаркете, метаданные Gmail и журналы чатов, история поиска и записи о выдаче книг из публичной библиотеки, фильмы, транслировавшиеся через Netflix, действия в Facebook и Twitter, на сайтах знакомств и в других социальных сетях складываются в совершенно определённое личное повествование. Мобильное устройство в кармане, устройство отслеживания физической активности на запястье и регистратор данных о событиях в автомобиле следуют за ней в пути. Когда хотя бы часть данных объединяют и сопоставляют с данными, созданными другими похожими на неё людьми, можно делать убедительные демографические выводы и прогнозы. Мы знаем нашу героиню с такой полнотой, которой позавидовал бы любой агент тайной полиции несколько десятилетий назад, и затрачиваем сравнительно мало усилий, поскольку наша героиня шпионит для нас сама за собой.

Если бы описанный здесь аппарат полного наблюдения был намеренным, централизованным и явным, машиной Большого Брата, переключающейся между камерами, он потребовал бы восстания, а мы могли бы представить жизнь вне тоталитарного микроскопа. Но если за нами наблюдают и документируют нас почти так же тщательно, как любого человека в истории, наше положение представляет собой тюрьму, из которой трудно сбежать, хотя у неё нет стен, решёток или надзирателей.

Это возвращает нас к проблеме «отказа от участия». При всём драматизме слов о тюрьмах и паноптикумах описанные здесь виды сбора данных, на которые отвечает обфускация, в демократических странах теоретически по-прежнему добровольны. Но цена отказа высока и продолжает расти: жизнь в усиливающейся социальной изоляции; использование любых доступных телефонов-автоматов (сейчас в Нью-Йорке их вдвое меньше, чем всего пять лет назад) или мобильных «одноразовых телефонов»; возможность принимать лишь совершенно определённые виды работы; жизнь вдали от центров бизнеса и торговли; отсутствие доступа ко многим формам

кредита, страхования и другим значимым финансовым инструментам; не говоря уже о мелких неудобствах и недостатках - долгом ожидании в полосах оплаты проезда наличными, более высоких ценах в продуктовых магазинах, худших местах на авиарейсах, - неуказанной платой за устранение которых служит раскрытие сведений.[16] Не каждый может жить в соответствии с принципами; на практике многим из нас приходится идти на компромиссы в асимметричных отношениях без желаемых контроля или согласия. В подобных ситуациях, то есть в повседневной жизни XXI века, всё же существуют способы выкроить пространство сопротивления, возражения и автономии. Это оружие слабых.

3.4. Оружие слабых: что может обфускация

Политолог Джеймс К. Скотт отправился в «Седаку», деревню в Малайзии, название которой заменено псевдонимом, чтобы ответить на вопрос, занимавший историков, антропологов и активистов всех направлений: как люди, лишённые общепризнанных средств политической защиты - голосов, денег, насилия, - участвуют в сопротивлении?[17] У крестьян, издольщиков и подневольных работников забирают труд и извлекают из него прибавочный продукт в виде зерна, денег, различных форм долга или времени на неоплачиваемых работах. Лишь изредка крестьяне могут рискнуть вступить в противоборство с эксплуатирующими их силами. У них меньше ресурсов, чем у квалифицированных промышленных рабочих в городских центрах, на которые можно опереться, чтобы занять драматическую и исторически памятную позицию против несправедливости. Скотта интересовал эмпирический вопрос: что делают крестьяне перед лицом явно несправедливых действий? Ответом стал перечень обычных, повседневных, в высшей степени практичных способов действовать и возражать, которые Скотт объединил под заголовком «оружие слабых». Они дополняют богатые и разнообразные описания сопротивления и сохранения некоторой автономии в равновесии между согласием и прямым отказом, прежде всего, применительно к наблюдению, в работах Гэри Маркса.[18]

Очевидно, но всё же заслуживает упоминания, что мы не намерены проводить прямое сопоставление между описанными Скоттом людьми и пользователями обфускации в целом. Мы также не считаем, что обфускация имеет точно такой же набор ограничений и свойств, как понятие Скотта. Для целей этой книги нас вдохновляют основополагающие темы идеи Скотта: действия по обфускации можно лучше понять в контексте неизбежных отношений между людьми и учреждениями с большой информационной и властной асимметрией. Прежде всего, мы отмечаем неизбежно малый и суммирующийся характер многих из этих видов «оружия» - обфускации и тех, которые наблюдает Скотт, - отражающий их роль в продолжающемся и неограниченном во времени наборе общественных и политических порядков, а не в ниспровергающей мир революции. Вместо массового вторжения на несправедливо распределённую землю этот подход состоит в самовольном заселении или браконьерстве. Мелкие кражи и мошенничество с «пальцем на весах» (явление, которое крупные розничные торговцы эвфемистически называют «товарными потерями») представляют собой дробные версии проекта перераспределения необходимых вещей. Ответом на приказы служит не кинематографический отказ, а волокита, замедление работы, притворное неведение, намеренная глупость и видимость подчинения. Наконец, что важнее всего для наших целей, вместо открытых дерзких ответов или героических речей в духе «на том стоим» возникает уклончивое бормотание, сплетни и клевета того, что Скотт называет скрытым транскриптом.[19]

Вероятно, каждый читатель этой книги отворачивался от вышестоящего (по службе, семье, закону, религии или иным отношениям) и едва слышно бормотал несогласие. Возможно, несогласие целиком происходит в уме; возможно, человек отваживается на почти неслышный шёпот, предназначенный лишь для себя; возможно, им делятся в приватной обстановке внутри подчинённой группы. (Как указывает Скотт, у могущественных групп тоже есть скрытые

транскрипты - способы накопления и поддержания власти, которые нельзя открыто обсуждать или раскрывать.) Несогласие на рабочем месте может принимать форму сплетен, шуток, анекдотов или историй, позволяющих критиковать порядок власти, не высказываясь прямо. Несогласие создаёт пространство, где могут существовать достоинство и относительная автономия говорящего, одновременно достигая и других результатов. Пусть и скрытно, но человек утверждает, что он не таков, каким может казаться на публике.

Проведя этот общий контур, изложим несколько кратких различий. Нельзя провести разумную аналогию между одним из изученных Скоттом крестьян и обфускатором, устанавливающим расширение браузера или запускающим ретранслятор Tor: широта доступных им ресурсов, структур и инфраструктур, а также механизмы принуждения и контроля, с которыми они сталкиваются, не допускают простых сравнений. Однако, как подсказывает наше изложение, один из результатов работы Скотта состоит в расширении учитываемого нами спектра ответов на угнетение и принуждение. Выбор не сводится к вооружённому восстанию или полному бездействию, и никто не бывает просто пассивен. Доступ к власти, богатству, статусу и другим составляющим автономии и восстановления справедливости имеет очень разные степени, но мы сопротивляемся там и тогда, где и когда можем. Продолжая эту нить, мы можем обратиться к одному из вечных вопросов о цифровой приватности: почему люди не пользуются мощными, доказуемо надёжными, открыто проверяемыми, устойчивыми системами защиты, например сквозным шифрованием сообщений с открытым ключом, то есть «сильной» криптографией? Почему не использовать оптимальную систему?

Мы не хотим утверждать, что её не следует использовать. Совсем наоборот! Однако существуют времена, обстоятельства, группы населения и события, где сильная система, оптимальная система невозможна, недоступна, нежелательна или сочетает эти три свойства. Возникают ситуации, в которых мы обязаны быть видимыми, должны быть видимыми или хотим быть видимыми (для друзей либо соратников или в качестве акта публичного протеста либо присутствия), но всё же хотим как можно лучше замутить свои следы. Иногда у нас нет выбора, будут ли собирать наши данные, и потому мы с тем же успехом можем (если нас это сильно волнует) насыпать немного песка в шестерёнки. Работая на государство или разрабатывая программы, мы можем быть вынуждены собирать данные ради предоставления услуги, но при этом стремиться поступать справедливо по отношению к пользователям и защищать их интересы от будущих групп, которые не разделяют наших благих намерений. В такие моменты, при таких ограничениях мы часто остаёмся со слабыми системами или сильными системами с несколькими слабыми компонентами и сами оказываемся «слабыми».

Мы хотим последовать за Скоттом, но направить его работу несколько иначе, расширяя спектр ответов на ситуации, связанные с наблюдением за данными и обфускацией. Обфускационный подход приносит реальную пользу независимо от того, состоит ли она в укреплении существующей сильной системы приватности, сокрытии конкретного действия, небольшом усложнении задачи противника или даже «простом жесте» регистрации нашего недовольства и отказа. Обфускационный подход предлагает выразительные и функциональные, хотя иногда хрупкие, методы протеста и уклонения, доступные широкому кругу действующих лиц, но особенно важные для тех, кому недоступны другие методы или кто хочет их дополнить. Поэтому мы применяем понятие «оружие слабых».

Прежде чем в следующем разделе перейти к видам ситуаций, где обфускация может быть полезна, необходимо ещё одно пояснение во избежание путаницы: «сильные» силы способны применять и применяют приёмы обфускации. Вспомним некоторые уже приведённые в книге примеры: корпоративное чрезмерное раскрытие документов в судебных делах, антиконкурентные уловки компаний, изготовление доказательств и некоторые военные технологии камуфляжа. Слабым нужно быть невидимыми, чтобы избегать внимания, но невидимость может быть выгодна и сильным. Наше рассуждение касается относительной полезности. Скажем прямо: если вам

доступны богатство, закон, общественная санкция и сила, если вы располагаете всем словарём сильных систем, находитесь на выгодной стороне асимметрии власти, способны нанять лучших адвокатов и толковых программистов, зачем утруждать себя обфускацией? Если у вас есть дипломатическая почта и защищённые АНБ телефонные линии, не нужно тратить время на перемешивание SIM-карт и выдумывание идентичностей. Иногда обфускация действительно оказывается полезной могущественным участникам, у которых уже действуют сильные системы приватности, и мы соответствующим образом обсуждаем эту сторону, но это средство охотнее принимают те, кому приходится довольствоваться слабой системой.

3.5. Отличие обфускации от систем строгой защиты приватности

До сих пор мы утверждали, что бывают случаи, когда оптимальные, «сильные» практики безопасности и приватности непрактичны или недоступны отдельным людям и группам. Это не довод против других систем и практик, а простое признание существования обстоятельств, в которых обфускация может предоставить подходящую альтернативу или быть добавлена к существующей технологии

До сих пор мы утверждали, что бывают случаи, когда оптимальные, «сильные» практики безопасности и приватности непрактичны или недоступны отдельным людям и группам. Это не довод против других систем и практик, а простое признание существования обстоятельств, в которых обфускация может предоставить подходящую альтернативу или быть добавлена к существующей технологии или подходу. Обфускация способна выполнять функцию, подобную скрытому транскрипту: скрывать несогласие и тайную речь и давать возможность утверждать собственное чувство автономии - акт отказа, скрытый внутри жеста согласия; она также может предоставлять более прямолинейные средства протеста или сокрытия. Бывают ситуации, где многие люди время от времени вынуждены чем-то жертвовать с неопределёнными последствиями и без ясного механизма восстановления контроля; в такие моменты обфускация способна сыграть роль, предлагая не всеобъемлющее решение военного уровня для контроля данных (хотя её можно с пользой сочетать с таким решением), а интуитивно понятный подход к созданию небольшой дымовой завесы.

Чтобы объяснить, что такое обфускация, необходимо прояснить, чем она не является и какие пустые пространства заполняет (подобно тому как «оружие слабых» Скотта заполняет пространство между согласием и восстанием). Необходимо обсудить, чего достигает обфускация и чего не достигают другие службы и системы, а также чего она стоит с точки зрения трудностей, потраченных впустую данных и времени. Что делает обфускацию необходимой в контексте защиты данных посредством оптимальной технологии, лучших методов ведения бизнеса или законодательства и государственного вмешательства? Учитывая затраты, которые может налагать обфускация, зачем к ней обращаться? Описание этих затрат и изложение нашего рассуждения с их учётом прояснят обфускацию в целом, прежде чем мы поместим её в рамки этических и политических вопросов (в главе 4), а затем проектирования ради конкретных целей и результатов (в главе 5).

Мы уже рассмотрели одну из альтернатив, от которой следует отличать обфускацию: отказ людей от любой платформы, службы или взаимодействия, которые будут неправомерно использовать их данные. Такое решение кажется свободным от нравственного компромисса: люди не согласны и потому отказываются, никому не мешая. Хотя подобный отказ может быть возможен для очень узкого круга потенциальных пользователей и применений, он не служит практичным или разумным выбором для всех. Мученичество редко бывает продуктивным выбором в политическом расчёте; каким бы прямолинейным ни казался бинарный выбор рационального деятеля между участием и отказом, выбор между согласием и падением с края (сетевого) мира в действительности вовсе не

является выбором. Мы часто оказываемся в компромиссных ситуациях, пытаясь принять лучшее решение из узкого меню вариантов, проблематичных в разной степени и разными способами. Пользователь, неизменно принимающий безупречные решения о безопасности и приватности данных, подобно совершенно рациональному экономическому субъекту, скорее встречается в теории, чем на практике, а на практике такой человек представлял бы собой странное равновесие между чрезвычайно искушённым технологом и луддитом-отказником.

А как насчёт того, чтобы положиться на применение компаниями лучших методов в интересах клиентов?

Разумеется, пользователи - не единственная сторона уравнения получения данных. Участвующие компании могли бы разрешить многие опасения пользователей и сделать обфускацию ненужной. Хорошо спроектированная политика отказа могла бы предоставить точное управление процессами агрегирования и анализа, позволяя выбирать между крайностями отказа и подчинения. Она позволяла бы получать определённые преимущества в обмен на некоторую степень использования и указывала бы, что данные можно собирать или применять лишь в определённых контекстах, лишь в определённых целях и лишь в течение установленного срока. Это могло бы предоставить пользователям настоящие варианты для оценки. Однако усилиям частного сектора такого рода мешает то, что компании по веским и дурным причинам являются основными стратегическими выгодоприобретателями интеллектуального анализа данных. Современная потребительская экономика работает на данных: опросах, анализе конверсии, анализе удержания клиентов, демографии, таргетированной рекламе и данных, собранных в точке продажи и проходящих обратно через всю цепочку поставок, от производства точно в срок до системы выявления тенденций.[20] Независимо от того, занимается ли конкретная компания сбором, упаковкой и продажей индивидуальных данных (как DoubleClick и Acxiom), использует ли созданные и предоставленные клиентами данные для совершенствования своей работы (как Amazon и Wal-Mart), основана ли на рекламных доходах, зависящих от пользовательских данных (как Google), или передаёт анализ потребительских данных субподрядчикам ради выявления кредитных, страховых или арендных рисков, поддерживать общие ограничения доступа к этой информации не в интересах компании.[21]

Из-за связанного с общими ограничениями доступа к информации конкурентного недостатка любая отдельная компания рискует потерять отдачу от данных о покупателях, клиентах, потребителях и даже пациентах. Сетевые издатели, особенно обязанные отвечать перед акционерами, боятся оставить неиспользованной ценность, которую можно извлечь из личной информации. Кроме того, ликвидность и переносимость данных делает любую частичную стратегию отказа от них крайне проблематичной, поскольку материал, не имеющий большого значения в руках одной компании, может привести к серьёзному нарушению приватности в руках другой компании, располагающей более богатой или лучше управляемой базой данных. Для компаний отрасли информационных услуг или компаний, использующих данные ради усиления конкурентного преимущества, огорчение потребителей, периодические штрафы и выговоры представляют собой достаточно малую стоимость ведения бизнеса, и такие компании яростно борются за сохранение доступа к «наличному запасу» личных данных.[22]

А как насчёт того, чтобы положиться на принятие и исполнение государством лучших законов?

Разве государство не должно быть площадкой, где уравновешивают интересы и защищают ценности и политические принципы? Это ставит ещё один вопрос, перед которым обфускация

должна оправдать себя: почему компаниям приходится самостоятельно изобретать практики сбора данных и управления ими? Конечно, такие практики должны определять и обеспечивать государства.

И действительно, регулирование и право исторически служили центральными бастионами личной приватности: от Четвёртой поправки к Конституции США до требований и директив Европейского союза о защите данных. Вероятно, в конечном счёте именно в законах состоится разговор, в котором мы как общество ответим на трудные вопросы о сборе и накоплении личной информации. Но законы действуют медленно, и любой импульс, направляющий представителей государства и права к защите приватности в общественных интересах, в полной мере уравновешивается противодействующими силами корпораций и других институциональных участников, включая само государство.

В мире после Сноудена стало ясно, что для многих организаций национальной безопасности, шпионажа и правоохранительной деятельности весьма выгодно иметь население, уже склонное раскрывать компаниям огромные объёмы сведений о себе, которые можно получить по повестке или скрытно использовать.[23] Плохо спроектированные и управляемые социальные платформы создают эффективно шпионящее само за собой население, которое бесплатно прослушивает себя посредством фотографий, загруженных с сохранёнными метаданными EXIF, и подробной социальной болтовни, ожидающей обработки алгоритмами интеллектуального анализа данных.

Особенно в Соединённых Штатах людям придётся задавать тщательные и требовательные вопросы о любом государственном проекте реформирования правил и практик сбора данных. Огромные объёмы личных данных уже находятся в обращении. Всё больше свободно предоставляемых личных данных упаковывают и продают, пока терпеливая и неопределённая работа законодательства и судебных решений движется медленно, делая шаги то вперёд, то назад. Скорость прогресса не внушает большого оптимизма. Это возвращает нас

к вопросу, с которого мы начали: раз технологии создали контекст и параметры многих из этих проблем, почему более совершенные технологии не могут их решить?

А как насчёт того, чтобы положиться на более совершенные технологические решения?

Для сохранения и усиления приватности были созданы мощные, продуманные, хорошо спроектированные системы, будь то интеллектуальный анализ данных, просмотр или поиск во Всемирной паутине либо передача конфиденциальной информации. И всё же положение остаётся несовершенным. Создание средств выявления происхождения данных, надлежащего обезличивания наборов данных, формирования осведомлённости о контексте и обеспечения безопасной конфиденциальной связи ставит серьёзные технические задачи. Потенциальные системы такого рода также сталкиваются с сопротивлением богатых деловых интересов и государственных организаций, которые предпочли бы, чтобы мы пользовались худшими, плохо реализованными и слабо принятыми (и приспособленными) системами.[24] Более того, какими бы убедительными ни были технические разработки и стандарты, принятие их общественными участниками, чьи организации и учреждения опосредуют многие потоки данных, сопряжено с политикой. Трудности сохраняются даже на уровне отдельного человека, как отмечает Арвинд Нараянан в исследовании применения «прагматической криптографии» (в отличие от «криптографии шифропанков», технодетерминистского проекта полного переустройства общества посредством шифрования): для разработчиков принятие сопряжено со сложными инженерными проблемами и вопросами удобства использования.[25] Ни одна из этих проблем не умаляет достижений или полезности технологий приватности: от Tor и обмена сообщениями Off-the-Record (OTR) до наборов средств шифрования электронной почты, таких как Gnu Privacy Guard (GPG).

Однако сочетание технических достижений, права и регулирования, лучших отраслевых практик и пользовательского выбора оставляет большие, пренебрегаемые, незащищённые пустые пространства, подобные отрицательной диаграмме Венна, где обфускация вступает в свои права.

Как мы позднее обсудим подробнее с практической стороны, обфускация отчасти представляет собой стратегию создания неприятностей. Хотя приватности служат ограничения права и регулирования, ограничения раскрытия, налагаемые лучшими организационными практиками, защитные технологические возможности, предоставленные добросовестными разработчиками, и воздержание или отказ от участия, области уязвимости остаются огромными. Обфускация обещает дополнительный слой прикрытия для этих областей. Обфускация скрывает, создавая шум и замутняя воду; её можно применять для неповиновения в отношении данных в трудных обстоятельствах и как цифровое оружие информационно слабых.

Глава 4. Оправдана ли обфускация?

> Огнём будь для огня; грози тому, кто угрожает, и взглядом взгляд смути.
>
> Шекспир, «Король Иоанн», 1595 год

После лекции о TrackMeNot[1] одна слушательница встала и сказала, что её глубоко тревожит возвеличивание обмана и нечестности. Ей казалось неправильным отправлять поисковые запросы, которые не представляют настоящего интереса. Обман был не единственным основанием для возражений против обфускации; среди других оснований - расточительство, безбилетничество, загрязнение баз данных и нарушение условий обслуживания.

Такие возражения, как высказанное слушательницей лекции, беспокоили нас: предполагалось, что нравственное превосходство находится на нашей стороне, а TrackMeNot защищает людей от неправомерных и эксплуататорских практик обращения с информацией. Но подобные возражения нельзя было просто отмести. Поскольку обфускационные тактики часто носят принципиально состязательный характер, предполагают притворство и направление по ложному пути, присвоение ресурсов для непредусмотренных или нежелательных целей необходимо объяснить и оправдать. В статье «Кнопка в ботинке» Гэри Маркс пишет: «Необходимы критерии, позволяющие говорить о "хороших" и "плохих", уместных и неуместных попытках нейтрализовать сбор личных данных».[2] Недостаточно применять обфускацию потому, что она работает, и даже потому, что это единственный работающий подход. Если обфускация используется, её необходимо защищать на этических основаниях, и она должна быть совместима с политическими ценностями общества, в котором живёт человек.

TrackMeNot выявил многие этические вопросы, с которыми могут столкнуться не только разработчики обфускационных систем, но и пользователи, а следовательно, показал необходимость отличать нравственно оправданные способы применения от неоправданных. Интуиция относит грабителя с Craigslist и его невольных одинаково одетых сообщников ко второй категории, а дипольные отражатели союзников - к первой, но почему? Чем они отличаются? И как приспособить ответ к более неоднозначным случаям? Простого одобрения или неодобрения недостаточно, если мы хотим защитить правомерность конкретной системы; вместо этого мы должны привести систематические причины, по которым система избегает нравственных и политических опасностей.

Эта глава готовит проектировщиков и пользователей обфускации к целому ряду возражений, с которыми они, вероятно, столкнутся. Некоторые возражения этические: они утверждают, что обфускация причиняет вред или нарушает этические права помимо вреда общего характера. Другие возражения политические: они предполагают, что обфускация ущемляет политические права и ценности, несправедлива или неправосудна, неправомерно перераспределяет власть либо в целом противоречит политическим ценностям окружающих обществ или сообществ.

4.1. Этика обфускации

Нечестность

Почти невозможно избежать обвинений в нечестности, когда цель обфускации состоит во введении в заблуждение и направлении по ложному пути. Связывая обфускацию с этикой лжи, мы попадаем в обширный ландшафт философской мысли, который выходит за рамки нашей книги, но даёт

важные идеи для нашей более узкой цели.

Классическая кантовская позиция о лжи, согласно которой ложь абсолютно неправильна и которая, как известно, предписывает говорить правду даже убийце, разыскивающему невинную жертву, осудила бы любое применение обфускации. Другие оправдания лжи основывались на более разнообразных и зависящих от обстоятельств этических позициях. В целом литература о лжи имеет два направления: одно занимается определением лжи, другое - её этикой, то есть тем, всегда ли она неправильна, бывает ли когда-либо правильна и может ли быть когда-либо простительна, даже оставаясь неправильной. На практике эти два направления взаимозависимы, потому что жёсткая позиция о неправильности лжи смягчается узким определением. Например, Фома Аквинский допускал, что благоразумное притворство проходит этическую проверку не потому, что ложь иногда нравственно приемлема, а потому, что притворство иногда не подпадает под определение.[3] Мы полагаем, что немногие столь же непреклонно преданы правдивости, как Кант и Фома Аквинский, и что большинство одобрило бы ложь при надлежащем оправдании, например для предотвращения вопиющего вреда, действия под принуждением, выполнения обещания или достижения других важных целей.[4]

Во многих рассмотренных в этой книге случаях обфускация предоставляет средство сопротивления принуждению, эксплуатации или угрозе - целям, которые в целом способны узаконить нечестные действия. Поэтому можно сказать, что нравственная оправданность обфускации, как и лжи, зависит от правомерности её целей: дипольные отражатели, защищающие бомбардировщики союзников, проходят проверку, а распространение вредоносных программ, ограбление банка или подтасовка выборов - нет, хотя мы можем восхищаться изобретательностью совершающих такие действия или посмеиваться над ней. Мы не хотим преувеличивать вывод и утверждать, что одни только правомерные цели оправдывают обфускацию в той мере, в какой она является формой нечестности; мы хотим сказать лишь, что правомерные цели - необходимое условие этичной обфускации.

Даже если человек выбирает обфускацию для достижения достойных целей, ему потребуется защищать этот выбор от дальнейших возражений. Рассмотрев некоторые другие этические обвинения против обфускации, мы вернёмся к вопросу достаточности, чтобы объяснить, чего помимо похвальных или хотя бы просто приемлемых целей всё ещё недостаёт этической оценке.

Расточительство

Критики могут назвать обфускационную систему расточительной, если она использует какие-либо важные ресурсы для создания шума. Например, TrackMeNot упрекали в расточительном использовании серверов поисковых систем, нагрузке на пропускную способность сети и даже ненужном потреблении электричества. Аналогично CacheCloak[5] можно обвинить в растрачивании ресурсов сети и мобильных приложений, многие создающие шум средства социальных сетей - в чрезмерном использовании служб Facebook, а Uber - в напрасной трате усилий водителей, отвечающих на ложные вызовы. Защищая предпочитаемую систему обфускации, следует сразу признать скрытую программу любых подобных обвинений, поскольку понятие расточительства насквозь нормативно. Оно предполагает стандарты приемлемого, желательного или правомерного использования, потребления, эксплуатации или применения рассматриваемых ресурсов. Лишь прочное общественное согласие относительно этих стандартов поднимает такие обвинения выше простого личного мнения, и лишь твёрдая основа фактического знания придаёт убедительность утверждению, что конкретная система обфускации расходует ресурсы впустую.

Но когда стандарты не установлены, граница между использованием и расточительством становится более неопределённой. Все мы можем согласиться, что небрежно оставленный открытым кран напрасно расходует воду, но жители Лос-Анджелеса не согласятся с жителями

Сиэтла в том, расточителен ли ежедневный полив ради сохранения зелёных газонов в пустынном климате. Защищая TrackMeNot от обвинений в расточительстве, можно указать, что использование им сети минимально по сравнению с трафиком файлов изображений, аудио и видео, богатыми информационными потоками социальных сетей и службами связи через Интернет. Однако замечание об огромной разнице масштабов между трафиком, создаваемым поисковыми терминами TrackMeNot, и трафиком, необходимым для работы, например, Bitcoin или World of Warcraft, не даёт полного ответа на жалобу. В конце концов, общий объём воды из капающего крана может быть намного меньше требуемого для ежедневного душа, но первый всё равно могут признать расточительным, поскольку он не нужен.

Считает ли человек шум, создаваемый системами вроде CacheCloak и TrackMeNot, расточительным, зависит не только от объёма шума, но и от его ценностей. Защитник укажет, что защита приватности посредством предотвращения профилирования на основе поисковых запросов стоит потраченной пропускной способности и наверняка более достойна, чем множество видеороликов, забивающих полосу на пути от серверов к домохозяйствам. Некоторые критики всё же сомневаются, хотя их сомнения относятся не столько к расточительному использованию общих ресурсов, сколько к растрате частных, например серверного пространства, принадлежащего поставщикам поисковых систем и мобильных приложений. Здесь также имеют значение и количество, и правомерность. Когда шум перегружает систему противника или, в более крайних случаях, даже поглощает все доступные ресурсы, он становится атакой типа «отказ в обслуживании», и планка оправдания оказывается очень высокой. Если вы не можете убедительно показать, что ваша цель применяет угнетающие, властные или явно несправедливые практики, обфускационную атаку, выводящую систему из строя, трудно оправдать.

Когда обфускационная система лишь использует частный ресурс, но не выводит его из строя, не всегда очевидно, что считать правомерным. Возьмём веб-поиск. Запросы, отправленные вручную, какими бы несерьёзными ни были их цели, по-видимому, не вызывают жалоб на расточительство. Никто не утверждает, что запрос «черепашка-ниндзя» или «фэнтези-футбол» больше растрачивает ресурсы серверов Google, чем, скажем, «симптомы Эболы», хотя некоторые критики называли расточительными автоматические поисковые запросы TrackMeNot. Мы не видим иной причины такой критики, кроме того, что запросы TrackMeNot противоречат интересам, желаниям или предпочтениям Google, а те, по мнению критиков, превосходят интересы, желания или предпочтения пользователей в обфускации ради приватности. Такова риторическая борьба между защищающими обфускацию как средство защиты пользователей от неправомерного захвата информации и целями обфускации, которые называют такие действия расточительными. Победитель этого спора занимает нравственную высоту и превращает частный спор о конфликтующих корыстных интересах в вопрос общественной морали. Но в данном случае важно видеть, что, очерняя обфускацию как «расточительство», защитники поисковых ресурсов исходят из недоказанного предположения по тому самому вопросу, который мы все вместе ещё не рассмотрели должным образом. Во имя защиты приватности обфускация запросов использует частные ресурсы без разрешения владельцев, но сочтём ли мы это расточительным или правомерным, запретным или допустимым - политический вопрос об осуществлении власти и привилегий, к которому мы вернёмся далее в этой главе.

Безбилетничество

В зависимости от устройства предпочитаемой системы обфускации вас могут обвинить в безбилетничестве, то есть использовании готовности других людей подчиниться сбору, агрегированию и анализу данных или использовании услуг сборщиков данных с одновременным лишением их прибыли от вашей личной информации. В первом случае противник преследует менее затратную цель - людей, которые не применяют обфускацию, - подобно тому как, согласно

поговорке, хищники преследуют более медленную добычу. Во втором случае, если вы пользуетесь службами таких целей, как Facebook и Foursquare, способами, отклоняющимися от условий обслуживания, вы нарушаете подразумеваемый договор и едете без билета не только за счёт людей, чьё поведение соответствует условиям обслуживания, но и за счёт инвестиций поставщиков услуг. Например, это относится к пользователям блокирующих рекламу плагинов браузера, которые могут наслаждаться более спокойной и быстро загружающейся Всемирной паутиной без рекламы, получая при этом доступ к контенту, оплачиваемому пользователями, которые не установили блокировщики. Во всяком случае, так утверждают критики. Представленные безбилетниками обфускаторы выглядят скорее пронырами, чем бунтарями; в конце концов, стремясь к нравственной высоте, хотите ли вы вместо этого оказаться человеком, который обыгрывает систему, используя неведение и глупость других? К этим обвинениям необходимо относиться серьёзно, но, на наш взгляд, их убедительность зависит от ответов на два вопроса: доступна ли ваша система обфускации (созданная или используемая вами) другим людям свободно? И не оказывается ли положение людей, не применяющих обфускацию, хуже вследствие использования этой системы вами? Если ответы на оба вопроса положительны, как в случае многих рассмотренных систем, мы не видим ни эксплуатации, ни нравственной неправоты. Если ответ хотя бы на один вопрос отрицателен, ситуация сложна и требует дальнейшего изучения. Тайная обфускация может быть простительна, если не ухудшает положение тех, кто её не применяет; обфускация, ставящая не применяющих её людей в невыгодное положение, может быть оправдана, если широко и свободно доступна всем. Хотя в обоих сценариях требуется дальнейшее оправдание, самые трудные вопросы ставит закрытая, тайная обфускация, которая создаёт невыгодное положение для не применяющих её людей.

Эти трудные вопросы погружают нас в философские споры о нравственной ответственности. Даже в худшем случае можно перенаправить вину на цели вашей обфускационной системы - сборщиков данных. Можно спросить: «Кто кем пользуется?» Возвращаясь к метафоре хищника и добычи, можно возразить: «Не вините меня за быстроту ног; в конце концов, именно хищник ответственен за гибель своих жертв». Хотя вы увеличиваете вероятность поимки более медленных товарищей, основная вина наверняка лежит на хищнике. В итоге возникает пат взаимных обвинений: сборщик данных обвиняет обфускатора в безбилетном использовании услуг, а обфускатор обвиняет сборщика данных в безбилетном использовании личной информации.

В господствующей экономике Интернета отдельные пользователи пользуются бесплатными службами, которые поддерживаются ценностью, извлекаемой рекламными сетями и другими сторонними агрегаторами данных из сведений об этих пользователях. В отличие от традиционного коммерческого рыночного обмена, где за товары или услуги явно уплачивается цена, сложившаяся в Интернете экономика основана на захвате информации косвенными, тонкими и часто хорошо скрытыми средствами. По словам специалистов, чьи комментарии вдохновили наши собственные размышления, такая информационная цена, фактически незаполненный чек, совершенно не бесплатна.[6] Когда отказ от личной информации без разумного объяснения её использования служит необходимым условием получения услуги, когда он несоразмерен потребности (как при чрезмерном сборе) и неуместен (как при нарушении контекстуальных ожиданий), такая цена носит эксплуататорский характер, а практика является угнетающей. Кроме того, когда традиционные институциональные средства защиты не способны эффективно противостоять подобным практикам, обвинённый в безбилетничестве обфускатор вправе оспаривать предполагаемые права укоренившейся системы, где наивные пользователи поддаются риторическим уловкам и вступают в обмен на условиях, в установлении которых почти не участвовали.[7] Каждая сторона заинтересована устанавливать условия обмена ценными ресурсами, но вопрос о том, чьим интересам отдавать предпочтение, должен быть справедливо разрешён; иначе, говорит обфускатор, это притязание, не заслуживающее уважения.

Это рассуждение не делает любую обфускацию информации правомерной и защищённой от обвинения в безбилетничестве; оно делает это лишь при соблюдении других нравственных требований и когда вопрос о безбилетничестве зависит от того, кто вправе получить прибавочную ценность, созданную взаимодействием отдельных пользователей с поставщиками услуг, собирающими сведения о них. Иными словами, после того как вы убедились, что ваша система соответствует другим этическим критериям, например достойным целям, оставшиеся вопросы о конфликтующих интересах и желаниях либо справедливом распределении выгод и прав переходят в области экономического и политического анализа, рассматриваемые ниже.

Загрязнение, подрыв и повреждение системы

Обвинение в загрязнении данных столь же сложно, сколь неизбежно. Обфускация, определяемая как внесение шума, вызывает параллель с загрязнением - превращением чего-либо в нечистое или грязное. Человека, загрязняющего воду, почву или воздух токсичными химикатами, частицами или отходами, можно решительно критиковать, поскольку целостность окружающей среды высоко ценится не только как идеал, но и как практическая цель. Однако критики, опирающиеся на нормативный вес загрязнения окружающей среды, не бесстрастно замечают, что обфускация захламляет хранилище данных; они утверждают, что она загрязняет среду данных, целостность которой ценна. Но есть различие. В большинстве современных обществ ценность природной среды предполагается, а доказанно загрязняющее её действие считается предосудительным. Но если нельзя явно показать, что набор данных достоин защиты, притязание на его целостность основано на недоказанном предположении.

Даже целостность окружающей среды не имеет абсолютной ценности и обменивается на другие ценности, такие как безопасность, торговля и права собственности. Аналогично, чтобы обвинение в загрязнении данных было убедительным, необходимо показать, что набор данных имеет большую ценность, чем то, что стремится защитить обфускатор. Простое выявление отрицательных последствий для базы данных опять-таки исходит из недоказанного этического предположения. Всё сводится к следующему: загрязнение данных неэтично лишь тогда, когда целостность рассматриваемого потока или набора данных этически необходима. Кроме того, необходимо явно решить, превосходит ли целостность данных другие поставленные на карту ценности и интересы. Когда вопрос состоит в том, наносит ли обфускация ущерб интересам сборщика данных, этические вопросы можно решить лишь путём установления того, что эти интересы обладают общей ценностью и превосходят интересы обфускатора. Если нет ясных нравственных оснований предпочесть соответствующие конфликтующие интересы (или предпочтения) сборщика данных и обфускатора, лучшее, на что можно надеяться, - политическое или, возможно, рыночное решение.

Если в целостности конкретных потоков или наборов данных действительно присутствует общественный интерес, а обфускация отрицательно влияет на систему в целом, бремя оправдания действий переходит к обфускатору. Например, можно справедливо оспаривать действия обфускатора, снижающего целостность базы данных о здоровье населения, если это уменьшает потенциальную общественную пользу, которую она способна принести. Но даже в таком случае следует оценить, справедлива ли цена, которую человек платит ради блага других или в общественных интересах. Если людей принуждают вносить вклад, им необходимо хотя бы гарантировать, что способы использования информации, места её перемещения и защита будут соответствовать известным принципам добросовестной информационной практики. Иными словами, этическое рассуждение зависит от двух соображений: представляют ли рассматриваемые данные настоящий общественный и общий интерес и насколько большой жертвы требуют от людей ради таких интересов. Удержание обоих соображений в поле зрения признаёт, что целостность набора данных, даже признанного ценным, не абсолютна, а контролёры данных несут бремя защиты общественной важности набора (и связанных практик), а также правомерности любых

тягот, которые он может возлагать на отдельных субъектов данных.

До сих пор в обсуждении мы не проводили различий между тремя терминами: «загрязнение», «подрыв» и «повреждение системы». Стремясь обеспечить этически оправданную систему, полезно подумать, какой из трёх относится к ней. Обфускационные системы, загрязняющие или подрывающие только след данных самих обфускаторов, ставят меньше этических вопросов, чем системы, затрагивающие также других субъектов данных, и ещё меньше, чем системы, мешающие общей работе системы, как при отказе в обслуживании. Тщательная оценка предполагала бы вопросы, сходные с рассмотренными выше, о соответствующем вреде, правах, общественном благосостоянии и соразмерности как сбора, так и обфускации данных по отношению к правомерным целям.

4.2. От этики к политике

Цели и средства

Поскольку обфускация почти всегда включает притворство, несанкционированное использование системных ресурсов или ухудшение функциональности, понимание намеченных конечных результатов, замыслов, назначений или целей обфускации имеет решающее значение для оценки её нравственного положения. Хотя одни цели могут казаться безоговорочно хорошими, а другие безоговорочно плохими, между ними существует обширная средняя область, охватывающая просто непроблематичные цели (например, срыв наблюдения супермаркета) и несколько спорные цели (например, обеспечение однорангового обмена файлами). В этих зонах этической неоднозначности или гибкости в дело вступают политика и государственная политика.

Однако цели - лишь часть картины, необходимое, но не достаточное условие. Этическая теория и здравый смысл требуют оправданности и средств, а поговорка предупреждает, что цель может оправдывать не все средства. Приемлемость средств может основываться на многочисленных этических факторах, но, как часто бывает, способна зависеть от взаимодействия целей с различными зависящими от обстоятельств и контекста факторами, рассмотрение которых находится в политической области.

Признание того, что некоторые споры об этических вопросах лучше всего разрешаются политически, не обязательно полностью исключает их из этического рассмотрения, если придерживаться такого взгляда, как взгляд Исайи Берлина на политическую философию как нравственное исследование, «применённое к группам и нациям и, в сущности, ко всему человечеству».[8] В некоторых случаях разногласия об этике обфускации, сводящиеся к разногласиям о сталкивающихся целях и ценностях, всё же могут допускать чисто этическое разрешение, подобное тому, которое, по-видимому, нашёл Кант, поставив истину выше предотвращения убийства. Но разногласия о целях не всегда доступны чисто этическому рассуждению. В таких случаях решение становится вопросом социальной политики, поскольку способ урегулирования разногласий влияет на устройство или форму общества, в которое они встроены. Этические вопросы, требующие общественного решения, на протяжении веков вдохновляли политических философов - от Платона до Гоббса и Руссо и до наших дней, - стремившихся сравнивать и оценивать политические системы, выявлять политические свойства и способы принятия решений, характерные для хороших обществ, и формулировать политические принципы правосудия, справедливости и порядочности. Делая вывод, что на этические вопросы необходимо отвечать политически, поскольку они касаются распределения власти, полномочий и благ в обществе, мы по-прежнему думаем об этике. Мы имеем в виду не любое общество; мы

говорим об обществах, которые противостоят тирании и стремятся быть хорошими, справедливыми и порядочными так, как великие философы, критические мыслители и политические лидеры воплощали в идеалах словами и действиями. Помня об этом, вернёмся к вопросам нечестности (притворства), расточительства, безбилетничества, загрязнения и повреждения системы, возникающим в контексте обфускации.

Разбирая вопрос расточительства, мы представляли столкновения противников, отражающих выпады друг друга: один обвиняет другого в расточительной деятельности, а другой настаивает, что эта деятельность представляет собой правомерное использование. Так происходило, когда критики обвиняли пользователей TrackMeNot в расходовании пропускной способности на поиски, не представлявшие настоящего интереса, а пользователи TrackMeNot отвечали, что не растрачивают пропускную способность, а применяют её для продвижения правомерных притязаний на приватность. Подобным образом обвинённый в загрязнении набора данных или снижении способности системы к интеллектуальному анализу данных возражает, что назначение набора или анализа не заслуживает общественной защиты или хотя бы не должно превосходить уклонение обфускатора от наблюдения.

В целом утверждения о том, что обфускация данных ухудшает и повреждает базу данных или компрометирует систему либо чрезмерно использует или растрачивает общий ресурс, не дают права называть обфускацию неэтичной, если нельзя ясно объяснить, как рассматриваемое хранилище данных или система продвигает общественные цели, более важные, чем противоположные цели, которые стремится продвинуть обфускатор. Эти конфликтующие цели редко рассматривают явно или систематически таким образом, чтобы требовать от сборщиков данных оправдать ценность их деятельности. Чтобы понять критерий целей, следует спросить о назначениях или ценностях, которым служит сбор данных - база данных или информационный поток, - и задать тот же вопрос об обфускационной деятельности. Далее следует спросить, какое место эти цели занимают в более широких политических обязательствах коллектива - общества, нации и так далее. Пока мы, по-видимому, предоставляем Управлению транспортной безопасности США большую свободу в поиске и сборе профилей личной информации постольку, поскольку оно ставит целью безопасность пассажиров. Поэтому мы можем быть менее терпимы к людям, применяющим обфускацию в таком контексте даже ради защиты приватности; суть в том, что цели должны влиять на наше отношение к этичности как сбора данных, так и обфускации.

Но средства тоже имеют значение. Даже хорошие цели могут оправдывать не все средства. В праве и политике нас часто просят учитывать соразмерность, например требуя, чтобы наказание соответствовало преступлению. Хотя обфускатор должен быть готов оправдать разрушительные и даже наносящие ущерб средства, безусловно справедливо предъявить требование и цели. Вы можете решить установить TrackMeNot не потому, что возражаете против базовой практики регистрации поисковых запросов, а потому, что возражаете против неприемлемых крайностей: хранения чрезмерно подробных данных слишком долго и без надлежащих ограничений использования. Хранение данных ради улучшения функций поиска и даже сопоставления контекстной рекламы с запросами может казаться приемлемым, но разве не совершенно несоразмерно основной функции поисковой системы хранить данные неограниченно долго ради совершенствования поведенческой рекламы и сопоставлять историю поиска с другой сетевой деятельностью, чтобы профилировать людей слишком лично, слишком точно, слишком интимно? Подобные вопросы относятся ко всем крайним формам информационного наблюдения, причём сетевое наблюдение представляет собой особый случай, где повсеместное отслеживание поведения в сети кажется совершенно несоразмерным средством, поскольку служит лишь узким целям коммерческой рекламы, даже если это отслеживание немного повышает эффективность объявлений. Но обфускатор тоже должен отвечать на требования соразмерности, причём в совершенно конкретных выражениях. Так, мы можем согласиться, что цели TrackMeNot правомерны, но всё же захотеть регулировать объём шума, например срывать профилирование, но

не полностью выводить поисковую систему из строя атаками типа «отказ в обслуживании». Провести точную границу между соразмерным и несоразмерным всегда трудно, но интуитивное убеждение в существовании такой границы, даже если её приходится проводить отдельно в каждом случае, прочно и глубоко.

Соразмерность предлагает нормативные стандарты для конкретных пар средств и целей, действий и реакций, но средства можно измерять и сравнительными стандартами, например тем, ниже ли их стоимость, чем стоимость альтернатив. Показателен утилитарный образ мысли: он требует не только, чтобы счастье от рассматриваемых действий или общественной политики превосходило несчастье либо выгоды превышали затраты, но и чтобы действия или политика давали оптимальное соотношение среди доступных альтернатив. Когда обфускация предполагает введение кого-либо в заблуждение, порчу набора данных или ухудшение работы системы, пусть даже ради достойных целей, этичный обфускатор всё равно должен выяснить, доступны ли столь же легко другие средства с меньшей нравственной ценой. Можно спросить, значительно ли различаются затраты, связанные с разными формами обфускации, но можно также спросить, способны ли другие средства достичь тех же целей без затрат, которые мы рассматривали до сих пор.

Стоит задаться вопросом, можно ли найти менее разрушительные, но столь же или более эффективные альтернативы обфускации, хотя в главе 3, где мы рассмотрели некоторые стандартные подходы к сопротивлению тревожным практикам наблюдения за данными, оснований для оптимизма обнаружилось немного. Отказ от участия, предлагаемый критиками, которые говорят: «Если вам не нравится эта практика, всегда можно отказаться от взаимодействия», может быть осуществим для занятных мобильных приложений, цифровых игр и различных форм социальных медиа, но неудобен и дорог в случае сетевых покупок, EZ Pass и программ для часто летающих пассажиров; а отказ от множества векторов наблюдения - мобильных телефонов, кредитных карт, страхования, автомобилей, общественного транспорта - теперь почти неосуществим для многих людей.

Другие альтернативы, включая лучшие корпоративные практики и правовое регулирование, хотя и многообещающи в теории, ограничены на практике. По структурным причинам, связанным с радикальным несовпадением интересов и известной глупостью поручать лисе охранять курятник, корпоративные участники едва ли установят значимые ограничения на практику обращения с данными. Более того, история неудачных попыток заставить различные отрасли регулировать собственные практики обращения с данными оставляет мало надежд на существенную реформу. Хотя государственное законодательство также имело переменный успех,[9] его влияние не охватило коммерческий сектор, особенно в части регулирования сетевого и мобильного отслеживания. Несмотря на упорные усилия и твёрдую приверженность Федеральной торговой комиссии, Национального управления телекоммуникаций и информации Министерства торговли и других государственных учреждений, общий прогресс минимален. Например, уведомление и согласие, выраженные в политиках приватности, остаются господствующими механизмами защиты приватности в сети, несмотря на убедительные доказательства того, что они непонятны субъектам данных, сформулированы неоднозначно, постоянно пересматриваются и на практике не ограничили степень и масштаб сбора и использования данных. Кроме того, согласно большинству оценок, согласованные усилия по установлению стандарта Do Not Track для просмотра Всемирной паутины саботировала рекламная отрасль,[10] а разоблачения Сноудена[11] показали, что правительство США и другие правительства давно ведут массовое наблюдение. У людей есть веские причины сомневаться, что их интересы приватности в надлежащем сборе и использовании информации в скором времени будут защищены обычными средствами.

Правосудие и справедливость

До сих пор мы показывали, что разногласия об этичности обфускации между обфускаторами и их критиками иногда сводятся к столкновению целей и ценностей. Критик обвиняет обфускатора в нарушении правомерных целей; обфускатор обвиняет цель ровно в том же. Подобным столкновениям помогли бы открытое изложение и обсуждение в политическом пространстве, которое мы решительно поддерживаем. Но в обсуждении этики обфускации мы выявили и столкновения, относившиеся скорее к конфликтующим интересам и предпочтениям, чем к конкурирующим целям и ценностям. Ясный пример возник в обсуждении безбилетничества. Обвинённые в неблаговидном поведении обфускаторы могут указать на односторонне установленные сборщиками данных условия взаимодействия, позволяющие этим сборщикам захватывать прибавочную ценность, созданную в ходе взаимодействия. Применительно к равным участникам жалобы на безбилетничество поставили сложные вопросы: кому уместнее приписать вину - обфускатору, который, возможно, подверг равных ещё более пристальному вниманию или поставил их в ещё более невыгодное положение, либо самим деятелям такого внимания или создания невыгодного положения.

Чисто этическое разрешение таких притязаний и встречных притязаний может оказаться невозможным, когда, взятые в отдельности, они сводятся к предпочтению интересов и предпочтений либо обфускатора, либо его цели. Однако в более широком общественном контексте споры о том, чьим предпочтениям и интересам придают наибольший вес, глубоко политичны. Они признают одни права над другими и тем самым часто приводят к систематическому распределению или переустройству власти, полномочий и благ, а также тягот и подчинения. Это входит в число вопросов правосудия и справедливости, веками беспокоивших политических философов при разрешении столкновений относительно того, какие ценности превосходят другие и чьи права значат больше прав других людей. Однако помимо прав и ценностей общества искали принципы, управляющие распределением широкого круга благ, чтобы смягчать глубоко несправедливые, неправосудные и непорядочные результаты, а не оставлять их грубой конкуренции между действующими лицами (людьми, учреждениями и организациями) или указу действующих обладателей положения, как предпочли бы сильные обладатели.

Чтобы направлять наше рассуждение о правосудном и справедливом распределении благ (власти, богатства, полномочий и так далее), мы обратились к недавним работам по политической философии. Просим читателей снисходительно отнестись к тому, что ради идей, которые помогут рассмотреть выявленное нами противостояние между целью и обфускатором во всех его подробностях, мы берём отдельные образцы из огромной дисциплинарной традиции. Может показаться ненужным углубляться до первичных принципов, когда технологически развитые, либеральные и прогрессивные демократии, вероятно, уже включили такие принципы в свои законы и нормативные акты. Это означало бы, что для ответов на политические вопросы о приватности и обфускации нам достаточно обратиться к существующему праву и регулированию. Однако именно потому, что существующие законы и политика не смогли или пока ещё не смогли должным образом устранить огромные пробелы в защите приватности, возникает потребность обратиться к основополагающим принципам за лучшими ответами.

Возвращаясь к ситуациям, где сопротивление обфускаторов мешает воле или интересам цели, спросим, как эти соображения правосудия могут направлять нашу оценку. Джон Ролз в «Теории справедливости»[12] в качестве основного требования настаивает, чтобы рассматриваемые практики обфускации не нарушали и не подрывали основные права и свободы. Это требование ставит под вопрос обфускационные системы, основанные на обмане, подрыве системы и эксплуатации, которые потенциально способны нарушать права собственности, безопасности и автономии. Данный принцип устанавливает презумпцию против таких систем, если нельзя ясно показать сильные встречные притязания равного или большего веса, включая автономию, справедливое обращение, свободу слова и свободу политического объединения, то есть в целом свободы, связанные с правом на приватность. Первый принцип быстро разбирается с

обфускацией, которую преступники применяют для маскировки нападений и запутывания следов.

Для тонких случаев, где ни один противник не имеет явного этического преимущества в конкурирующих притязаниях, важен второй принцип Ролза, принцип максимина. Он требует, чтобы справедливое общество предпочитало «альтернативу, худший результат которой превосходит худшие результаты других».[13] На практике это означает, что при взвешивании вариантов политики справедливое общество не обязательно должно стремиться уравнять положение разных людей или групп, но, когда это невозможно или бессмысленно, должно сосредоточиться на положении находящихся в нижней части социально-экономического спектра и обеспечить выбор такой политики, которая максимизирует результаты для этих заинтересованных сторон. Иными словами, политика справедливого общества должна максимизировать минимум.

Возвращаясь к предыдущим случаям, рассмотрим теперь спор о напрасно расходуемых ресурсах - не общих ресурсах, которые мы уже обсуждали, а частных, например когда обфускация якобы растрачивает ресурсы Facebook вводящими в заблуждение профилями. Здесь поставщики услуг и владельцы ресурсов заявляют, что, поскольку права собственности позволяют им по своему усмотрению и в свою пользу устанавливать условия использования, несанкционированные действия по определению представляют собой неэтичное или расточительное использование их услуг или ресурсов. Обфускаторы, напротив, утверждают, что их ослабляют, эксплуатируют, делают уязвимыми и компрометируют, а они лишь действуют ради исправления дисбаланса контроля, власти и преимуществ и ради снижения риска и неоднозначности. Как отмечалось ранее, от нашей оценки конкурирующих притязаний зависит, признаем ли мы обфускационную деятельность, например создание поддельных запросов TrackMeNot, расточительной или правомерной, запретной или допустимой. Если на карту не поставлен очевидный этический вопрос, такой политический выбор относительно осуществления власти и привилегий подчиняется принципу справедливости максимина. Как именно он работает, зависит от подробностей конкретных случаев, например определённых различий в свойствах TrackMeNot, «Вулы» и российских ботов Twitter, а также контекстов их работы.

В отношении безбилетничества второй принцип Ролза заставляет спросить, имеют ли службы данных, чьи условия позволяют им захватывать прибавочную ценность личной информации, право на эту прибавочную ценность. Он позволяет увидеть, что права на прибыль и контроль, односторонне заявленные этими компаниями в условиях обслуживания, в действительности открыты для перераспределения посредством принятия иной общественной политики. Обфускаторы не являются безбилетниками, если невыгодность конкретного взаимодействия чрезмерна и несправедлива и если единственные притязания, которые они могут нарушать, заявлены поставщиками услуг при режиме, не вполне признающем последствия для потоков информации, недавно ставших возможными благодаря социотехническим системам. Сходное замечание относится к загрязнению. Хотя некоторые предполагают правоту сборщиков данных лишь на том основании, что те собрали и объединили данные и потому имеют право на их целостность, мы считаем, что никакое обвинение в загрязнении не будет убедительным без доказательства общественной ценности. Если это невозможно, требуется довод в пользу утверждения, что любая ценность должна доставаться только или главным образом сборщикам данных; предполагать это нельзя. Хотя люди, применяющие обфускацию для укрытия, действительно могут снижать чистоту массива данных, налагать затраты на сборщиков или лишать их выгод от прибавочной ценности, созданной сбором, агрегированием и анализом данных, полная картина учитывает ценность данных и правомерность притязаний сборщиков. При обвинениях в безбилетничестве или загрязнении частные притязания владельцев данных и встречные притязания обфускаторов рассматриваются как конфликты предпочтений или интересов. По нашему мнению, попытка найти решение, указав на права собственности, исходит из недоказанного предположения о пределах этих прав в текучей среде технологий и данных. Этот вопрос остаётся открытым для политических переговоров и корректировки. Следует учитывать

общее процветание и общественное благосостояние, в идеале с учётом второго принципа Ролза.

Распределение вины и нравственной ответственности также можно оценивать политически. Рассматривая ответственность за безбилетничество и загрязнение данных, мы утверждали, что, хотя в обоих случаях обфускатор служит причинным деятелем, нравственная ответственность всё же может разумно возлагаться на цель обфускации, если только деятельность и деловые практики либо практики обращения с данными этой цели не безупречны. Соображения правосудия в равной степени относятся к справедливому распределению затрат и выгод.[14]

В различных теориях справедливости, предложенных политическими философами, включая Ролза, присутствует довольно единообразное представление о находящихся в нижней части социально-экономического спектра людях, на которых направлено особое внимание. Подчёркивая различные способы, которыми принцип максимина важен для политического положения обфускации, мы предполагали, что традиционные или стандартные взгляды на то, что означает находиться в лучшем или худшем положении - быть сильным или слабым, богатым или бедным, хорошо или плохо образованным, здоровым или больным, - сохраняют значение. К этим измерениям неравенства наша тема информационной асимметрии власти и знания добавляет два измерения различий между имущими и неимущими, имеющих решающее значение для принципа максимина.[15]

Информационное правосудие и асимметрии власти и знания

Обстоятельства, окружающие обфускационные системы, представленные в части I этой книги, обычно характеризуются одновременно асимметрией власти и асимметрией знания. Разница во власти между людьми и корпоративными и государственными учреждениями и организациями, которые помещают их под наблюдение, захватывают сведения об их действиях, а затем объединяют и анализируют эти сведения, очевидна. Судящий, хищный взгляд неопределённых цифровых сообществ[16] также может направить на людей свой дисциплинирующий взор. Хотя, как мы показали в части I, обфускацию могут применять и применяли более могущественные против менее могущественных, у более могущественных обычно есть более прямые способы навязать свою волю. Обфускация в целом не так сильна или надёжна, как эти более прямые методы, и лишь изредка принимается могущественными участниками, обычно для ухода от внимания других могущественных участников.[17] Сильным участникам реже требуется прибегать к обфускации, поскольку, желая что-то скрыть, они располагают лучшими методами, среди которых грифы секретности, цензура, коммерческая тайна и угрозы государственного насилия. Поэтому рассмотрим менее могущественных членов общества, которые могут обратиться к обфускации, чтобы уравнять шансы.

Людям, которые небогаты, не имеют политического влияния и не могут отказаться от условий взаимодействия; людям, которым недостаёт технической искушённости или знаний для применения сильного шифрования; людям, желающим получать скидки в супермаркете, бесплатные учётные записи электронной почты и дешёвые мобильные телефоны, обфускация предлагает некоторую меру сопротивления, сокрытия и достоинства, пусть и не постоянное переустройство контроля или переворачивание укоренившейся иерархии. Как выразился Анатоль Франс, «закон в своём величественном равенстве запрещает и богатым, и бедным спать под мостами и красть хлеб».[18] Тем, кого обстоятельства и необходимость вынуждают отдавать данные о себе, то есть тем, кто больше всего нуждается в укрытии под мостом, каким бы импровизированным и неудовлетворительным оно ни было по сравнению с настоящим домом, обфускация предоставляет средство восстановления справедливости.

То, что мы назвали асимметриями власти, тесно соответствует традиционным векторам власти: богатству, общественному классу, образованию, расе и так далее. В современных обществах,

движимых данными, эпистемическая или информационная асимметрия имеет важные последствия. Обфускация может предоставить прикрытие от известных конкретных угроз, но способна также защитить от таящихся, плохо понятных угроз из неопределённых источников (государственных или корпоративных), присутствие которых мы ощущаем, но о которых мало знаем. Мы подозреваем, что эти «другие» могут захватывать информацию, которую мы создаём и излучаем, перемещаясь в сети, совершая операции в сети и вне её, работая, общаясь и участвуя в общественной жизни, но просто не знаем, какие именно сведения они захватывают, куда отправляют, как затем используют и по какой логике они влияют на нас. Такова природа эпистемической асимметрии в самой крайней форме. В этих обстоятельствах обфускация может казаться беспорядочным размахиванием руками в темноте, но даёт некоторую надежду против неизвестных знающих.

Обфускация против прямого осуществления власти и контроля представляет собой сопротивление знакомого рода, но щит, который она может обещать от таящихся неизвестных противников, заставляет вспомнить иную политическую угрозу. В книге «Республиканизм: теория свободы и государственного управления» Филип Петтит предпочитает определять свободу не как фактическое невмешательство, а как отсутствие господства, то есть защищённость от произвольного вмешательства: «Не просто то, что люди (или другие участники, например правительства или корпорации), обладающие властью произвольного вмешательства, вероятно, не станут её применять, а то, что рассматриваемые участники утрачивают эту власть: они лишаются возможности применять её или по крайней мере их возможность применения серьёзно сокращается».[19] Смотря со слабой стороны эпистемической асимметрии, мы можем осознавать, что сведения о нас и сведения, исходящие от наших действий в сети и вне её, доступны тем, кто находится выше на шкале, часто в форме рационализированных информационных наборов - профилей, которые можно применять для прямого или косвенного контроля над нами и для решения, что нам можно и нельзя иметь и куда можно и нельзя идти. По мере того как общества принимают обещания аналитики больших данных, а корреляция и кластеризация занимают господствующее место в принятии решений, люди могут всё чаще подвергаться решениям, которые «работают» статистически, но «не имеют смысла».[20] Наша свобода подрывается не только тогда, когда нам мешают иметь или делать желаемое, но и тогда, когда другие способны применять эту власть способами, которых мы не понимаем и воспринимаем как произвольные. По мнению Петтита, именно это и есть господство. Республиканизм не исключает непроизвольного подчинения подходящим формам права и государственного управления; он требует лишь, чтобы люди были защищены от произвольного вмешательства, «контролируемого arbitrium, волей или суждением вмешивающегося: в особенности в той мере, в какой оно не вынуждено следовать интересам и идеям тех, кто испытывает вмешательство».[21]

Находящиеся на проигрывающей стороне асимметрий власти и знания информационного общества, как мы утверждали, фактически составляют класс его менее обеспеченных членов: они являются субъектами наблюдения, не знают, как оно влияет на их судьбу, и не имеют власти устанавливать условия взаимодействия. Поэтому при разработке политики общества, признанного справедливым согласно двум принципам Ролза,[22] людям на проигрывающей стороне асимметрий следует позволить свободу утверждать свои ценности, интересы и предпочтения посредством обфускации (в соответствии с этическими требованиями), даже если это означает ущемление интересов и предпочтений находящихся на выигрышной стороне асимметрий знания и власти. Таким образом, выполнив этические требования первого принципа, согласно второму принципу максимина общественная политика, направленная на разрешение конфликтующих интересов и предпочтений, присущих рассмотренным случаям, должна учитывать важную работу, которую те потенциально выполняют для повышения положения находящихся на проигрывающей стороне укоренившихся асимметрий власти и знания.

Ради благосостояния других

Мы завершаем этот раздел, возможно, самым трудным вопросом, стоящим перед обфускацией данных: можно ли терпеть её, когда она направлена на системы, обещающие общественные выгоды, выходящие за рамки самих отдельных субъектов. По мере всё более глубокого вхождения в эпистемическую и принимающую решения парадигму больших данных и разжигания надежды на её способность служить общему благу возникают вопросы об обязанности людей участвовать.[23] Обфускаторов могут упрекнуть в нежелании платить за выгоды и в отказе внести вклад в общее благо. Но каковы точный объём и пределы этой обязанности? Обязаны ли люди платить любую требуемую цену, подчиняться любым условиям обслуживания и вносить вклад, даже если он связан с затратами? Обязаны ли, например, страдающие редким заболеванием участвовать в исследованиях и разрешать включать данные о них в статистический анализ, где размер N улучшает результаты? А если это связано с затратами?

Положение этичного обфускатора напоминает положение этичного гражданина, от которого ожидают вклада в общее благо, например уплаты налогов или службы в вооружённых силах. Некоторые могли бы аналогично сказать, что мы должны выполнить обязанность не только внесением данных в общий запас, но и честным, точным и добросовестным внесением. Даже если некоторое чувство обязанности существует, какие принципы определяют её форму, особенно если с ней связаны риск или затраты? Этика в целом не требует сверхдолжных поступков, а либеральные демократии не требуют и не оправдывают принесение невинных людей, пусть даже немногих, в жертву ради блага большинства. Где провести границу? Какие принципы справедливости дают указания по этим вопросам?

Джереми Уолдрон заметил, что после террористических атак 11 сентября 2001 года граждан попросили сместить равновесие безопасности и свободы в пользу безопасности.[24] Хотя общественная политика нередко требует компромиссов - обмена одной ценности или одного права на другое либо другие, - Уолдрон напоминает, что такие компромиссы необходимо принимать мудро, со скрупулёзным вниманием к последствиям. Одно особенно важное последствие - распределительное воздействие; потери и приобретения, затраты и выгоды должны справедливо распределяться между людьми и группами. Уолдрона тревожит, что, когда мы говорим, будто коллективно отказываемся от части свободы в обмен на коллективную безопасность, происходит важное опущение: некоторые люди или группы несут несоразмерную потерю свободы ради выгоды безопасности для всех или, как иногда бывает с компромиссами в целом, могут даже полностью исключаться из коллективных выгод. Обобщая это предупреждение на вопросы оплаты коллективного блага индивидуальными данными, мы должны учитывать не только общую сумму затрат по отношению к выгодам, но и то, кто оплачивает затраты и кто пользуется выгодами. Компании часто защищают жадность до данных, ссылаясь на улучшение услуг или безопасность, но расплывчато говорят о важнейших подробностях, например о том, поддерживают ли существующие клиенты и поставщики данных новых клиентов, не внёсших вклад, и какая доля извлечённой ценности достаётся «всем», а какая - компании. На эти вопросы необходимо ответить, чтобы рассмотреть природу и объём обязанностей субъектов данных вносить вклад в общий запас данных.

Риск и данные

Язык риска часто возникает в восхвалении обещаний больших данных на благо всех. Сторонники хотят убедить нас, что данные помогут снизить риски терроризма и преступности, неэффективного лечения, плохих кредитных решений, недостаточного образования, неэффективного использования энергии и так далее. Эти заявления должны убедить или даже заставить людей щедро делиться информацией, как мы любезно открываем содержимое чемоданов в аэропортах.

По логике таких утверждений обфускаторы поступают неэтично, уменьшая, обделяя или подрывая общий запас. Убедительно? Неопровержимо? Однако и здесь правосудие требует внимания к распределению и справедливости: кто рискует и кто получает выгоду? Мы не отвергаем эти утверждения категорически, но, пока на эти вопросы не даны ответы и не рассмотрены вопросы вреда и затрат, такой обязанности быть не может. Возьмём, например, банальную и повсеместную практику сетевого отслеживания ради поведенческой рекламы.[25] Рекламные сети утверждают, что сетевое отслеживание и поведенческая реклама снижают «риск» дорогостоящей рекламы, направленной на неподходящие цели, или направления привлекательных предложений неприбыльным клиентам. Возможно, риск и правда снижается, но информационные вклады всех улучшают положение лишь немногих, прежде всего рекламных сетей, предоставляющих услугу, возможно, рекламодателей и, быть может, привлекательных клиентов, которых они стремятся заманить. Выше мы высказали сходное замечание, обсуждая агрегирование данных ради снижения кредитного мошенничества: ссылка на снижение риска часто чрезмерно упрощает картину, где риск в целом может не снижаться, а даже если снижается, то не для всех. В действительности риск перемещается и перераспределяется. Мы высказываем сходные предостережения против неуместного раскрытия медицинской информации, которое может увеличивать риск для одних субъектов информации и снижать для других; или против сбора и анализа данных ради ценовой дискриминации, которые налагают риски на находящихся под наблюдением потребителей и одновременно снижают риски для торговцев, применяющих схемы профилирования данных.

Итоги

Обфускация данных ставит важные этические вопросы, которые следует учитывать каждому проектировщику или пользователю обфускационных систем. Мы тщательно рассмотрели эти вопросы и исследовали контексты и условия, важные для их разрешения в этических категориях. Но мы также обнаружили, что разрешение этических вопросов часто вызывает соображения политического и практического характера. Политика вступает в дело, когда споры зависят от разногласий об относительной важности общественных целей и относительном значении этических и общественных ценностей. Она также вступает в дело при рассмотрении достоинств конкурирующих ненравственных притязаний, распределения благ и рисков. При переходе в область политики обфускацию необходимо проверять по требованиям правосудия. Но если такой проверке подвергаются обфускаторы, ей следует подвергать и сборщиков данных, информационные службы, средства отслеживания и профилировщиков. Мы обнаружили, что захлёбывающаяся риторика вокруг обещаний и практики данных недостаточно говорит о правосудии и проблеме перемещения рисков. Обладатели положения встроили мало средств защиты и смягчения в возводимые ими здания данных. На этом фоне обфускация предлагает средство стремления к равновесию, оправданное, когда оно противостоит господству сильных над слабыми. Справедливое общество оставляет этот путь к отступлению открытым.

Глава 5. Будет ли обфускация работать?

Как обфускация может добиться успеха? Как усилия нескольких людей, создающих посторонние данные, могут сработать против хорошо финансируемых, решительных учреждений, не говоря уже о таких гигантах данных, как Google, Facebook, Axciom и Агентство национальной безопасности? Снова и снова сталкиваясь с этими сомнениями, мы пришли к пониманию, что, когда люди спрашивают о конкретных воплощениях обфускации или об обфускации в целом: «Но работает ли она?», разумный ответ звучит так: «Да, но это зависит от обстоятельств». Зависит от целей, обфускатора, противника, доступных ресурсов и многого другого. А они, в свою очередь, подсказывают средства, методы и принципы проектирования и осуществления.

Ранее мы представляли типичный сценарий с людьми, действующими внутри информационных экосистем, которые часто созданы и выбраны не ими. По отношению к проектировщикам, операторам, управляющим и владельцам этих экосистем отдельные субъекты данных находятся в асимметричном отношении знания, власти или того и другого. Хотя люди осознают, что сведения о них или созданные ими необходимы для этих отношений, они многого не знают. Сколько забирают? Что с этим делают? Как это на них повлияет? Они могут достаточно понимать экосистемы, в которые сознательно или неосознанно включены, от веб-поиска до распознавания лиц, чтобы полагать или осознавать неуместность применяемых практик, но одновременно понимать, что не способны разумно действовать вне экосистемы или разумным образом добиться изменений внутри неё.

Работает ли обфускация, то есть выполняет ли конкретный проект обфускации одностороннее изменение условий взаимодействия с личной информацией, может казаться простым вопросом об определённом методе решения проблемы, но при ближайшем рассмотрении это в действительности несколько вопросов. Работа обфускации зависит от характеристик существующих обстоятельств, желаемого изменения условий, того, что считается осуществлением этих желаний, а также архитектуры и свойств рассматриваемого конкретного проекта. Именно поэтому ответ «Это зависит от обстоятельств» на вопрос «Работает ли она?» не является шутливым; напротив, это приглашение систематически рассмотреть, какие характеристики информационной экосистемы позволяют обфускации работать. Помимо этих соображений мы стремимся сопоставить проектные возможности проектов обфускации с набором разнообразных целей, которые могут иметь инициаторы и пользователи таких проектов.

Поэтому в этой главе нам предстоит ответить на два вопроса. Вопрос «Будет ли обфускация работать?» можно понимать как «Как обфускация может сработать для меня в моей конкретной ситуации?» или как «Работает ли обфускация вообще?». Мы ответим на оба. Общий ответ прямолинеен: да, обфускация может работать, но сработает ли она и насколько, зависит от того, как она реализована для ответа на угрозу, достижения цели и соответствия другим конкретным параметрам. В этой главе представлен набор вопросов, на которые, по нашему мнению, следует ответить для правильного применения обфускации.

5.1. В обфускации важны цели

В мире теории безопасности и приватности теперь прочно установлено, что ответ на каждый вопрос «Работает ли это?» звучит: «Это зависит от обстоятельств». Защита чего-либо, придание ему приватности, безопасности или секретности предполагает компромиссы, многие из которых мы уже обсуждали. Защита требует времени, денег, усилий и внимания, добавляет организационное и личное трение, одновременно уменьшая удобство и доступ ко многим средствам и службам. В конце концов, почти полная свобода отдельного человека от цифрового наблюдения проста:

достаточно вести жизнь незарегистрированного мигранта-подёнщика 1920-х годов, без Интернета, телефонов, страхования и имущества, ездить на товарных поездах и неофициально получать плату за незаконный ручной труд. Просто, но чрезвычайно дорого, поскольку модель угрозы «всё» смехотворно широка. Размышляя о компромиссах организационной безопасности, можно вспомнить «Конус тишины» из пародирующего шпионские фильмы телесериала Get Smart.[1] Конус используется для проведения совершенно секретных совещаний и работает настолько хорошо, что находящиеся внутри люди не слышат друг друга: он совершенно приватен и до смешного бесполезен.[2]

Модели угроз снижают стоимость безопасности и приватности, помогая понять, что ищут противники и что способны найти, чтобы мы могли защищаться именно от этих опасностей.[3] Если вы знаете, что ваша организация сталкивается с опасностью, включающей сложные атаки на информационную безопасность, следует залить резиновым клеем все USB-порты на компьютерах организации и хранить конфиденциальные сведения на изолированных машинах, которые никогда не подключаются к сети. Но если вы не считаете, что организация сталкивается с такой опасностью, зачем лишать людей пользы USB-накопителей? Обфускация в целом полезна в отношении конкретного типа угрозы, сформированного необходимой видимостью. Как мы неоднократно подчёркивали, обфускатор уже в некоторой степени открыт: видим радару, людям, внимательно изучающим открытые судебные документы, камерам безопасности, прослушиванию, поставщикам веб-поиска и вообще сбору данных, определённому условиями обслуживания. Более того, он открыт в преимущественно неизвестной степени, находясь на проигрывающей стороне информационной асимметрии, и эта неизвестная открытость ещё больше усугубляется временем, будущим обращением данных и систем анализа. Мы принимаем эту видимость за исходную точку для определения роли, которую способна сыграть обфускация.

Иными словами, у нас нет доступной модели угроз, основанной на лучших практиках; более того, у обфускатора может не быть достаточных ресурсов, исследований или подготовки для создания такой модели. Мы действуем из слабого положения, вынужденные принимать варианты, от которых, вероятно, следовало бы отказаться. Если это так, нам приходится обходиться имеющимся (подробнее об этом ниже), и мы должны ясно понимать желаемый результат. Рассмотрим исследование даны бойд об использовании социальных медиа американскими подростками. Подростки в Соединённых Штатах подвергаются огромному вниманию, почти целиком без их согласия или контроля (со стороны родителей, школы, других авторитетных фигур). Казалось бы, социальные медиа подвергают их ещё большему вниманию. По умолчанию они открыты для изучения; более того, с точки зрения приватности им выгодно казаться видимыми каждому. «Сталкиваясь с определёнными технологиями, подростки принимают решения на основе того, чего пытаются добиться», - пишет бойд,[4] а часто они пытаются делиться содержанием, не делясь смыслом. Они не обязательно могут создавать тайные социальные пространства для своего сообщества: родители способны требовать и требуют пароли от учётных записей в социальных сетях и доступ к телефонам. Вместо этого подростки применяют разнообразные практики, исходя из того, что каждый может видеть их действия, а затем ведут себя так, чтобы лишь немногие могли понять смысл этих действий. «Ограничение доступа к смыслу, - пишет бойд, - может быть гораздо более мощным средством достижения приватности, чем попытка ограничить доступ к самому содержанию».[5] Их методы не обязательно используют обфускацию (они в значительной мере опираются на тонкие социальные сигналы, отсылки и нюансы, создавая материал, который разные аудитории читают по-разному, - практику «социальной стеганографии»), но подчёркивают важность понимания целей. Цель не в том, чтобы исчезнуть или сохранять полный контроль над информацией (что может быть невозможно), а в ограничении и формировании сообщества, способного правильно истолковать действия, видимые каждому.

Почти то же относится к обфускации. Многие случаи и практики, которые мы объединили под этим заголовком, выражают конкретные цели, принимающие обнаружимость, видимость или уязвимость

за исходную точку. По всем уже рассмотренным причинам люди теперь не могут уйти от определённых видов сбора и анализа данных, и потому возникает вопрос: «Что обфускатор хочет сделать с помощью обфускации?» Ответ на него даёт набор параметров (вариантов, ограничений, механизмов), с помощью которых можно сформировать подход к обфускации.

5.2. Я хочу применить обфускацию…

Несокрушимого сейфа не существует. Сейфы оценивают в часах, то есть по тому, сколько времени потребуется злоумышленнику (с различными наборами инструментов), чтобы их открыть.[6] Сейф приобретают как источник безопасности в дополнение к другим элементам защиты, включая запертые двери, сигнализацию, охранников и сотрудников правоохранительных органов. Часового сейфа с сигнализацией, вероятно, достаточно в участке, где полиция надёжно прибывает за двадцать минут. Если немного абстрагироваться, этим можно охарактеризовать цели обфускации. Сила обфускационного подхода измеряется не единым объективным стандартом (как сейфы), а относительно цели и контекста: он должен быть достаточно сильным. Его можно применять отдельно или совместно с другими приёмами приватности. Успех обфускации всегда относителен к её назначениям и к учёту ограничений, препятствий и неровного игрового поля эпистемической и властной асимметрии.

Собирая разные примеры обфускации, мы наблюдали сближение вокруг общих замыслов и назначений, которые возникали многократно, хотя одна система могла быть связана с несколькими конечными результатами или назначениями, а промежуточные результаты иногда служили средствами достижения других. Существуют и более тонкие различия, но ради более простого применения к проектированию и практике мы упростили и объединили назначения и конечные результаты в цели. Они расположены примерно в порядке включения: от выигрыша времени до выражения протеста. Противодействие профилированию, пятая цель, может включать некоторые более ранние цели, например предоставление прикрытия, а само может содержаться внутри выражения протеста (шестой цели). (Поскольку практически вся обфускация затрудняет быстрый анализ и обработку данных в целях наблюдения, все цели высшего порядка включают первую цель: выигрыш времени.) Определяя цель, подходящую вашему проекту, вы поднимаетесь по лестнице сложности и разнообразия возможных типов обфускации.

Скептически настроенные читатели, а скептиками следует быть всем нам, заметят, что мы больше не опираемся в значительной мере на примеры обфускации, применяемой могущественными группами ради злонамеренных целей, такие как использование ботов Twitter для препятствования протестам против выборов, накрутка отметок «Нравится» в мошенничестве в социальных сетях или корпоративная война между компаниями. Мы хотим, чтобы этот раздел сосредоточился на применении обфускации в положительных целях.

Если вы можете дать удовлетворяющие вас ответы на вопросы предыдущей главы, эта глава предназначена для вас. Начнём с возможности, что вы хотите применить обфускацию, чтобы выиграть немного времени.

…чтобы выиграть время

«Сработали» ли дипольные отражатели? В конце концов, через несколько минут они опустились на землю и снова открыли небо для прохода радиолуча, но, разумеется, к тому времени самолёт уже вышел за пределы действия радара.

Эфемерные системы обфускации, предназначенные для выигрыша времени, в некотором смысле изящно просты, но требуют глубокого понимания запутанного физического, научного, технического, общественного и культурного окружения. Для успеха не требуется выиграть определённое или максимально возможное время; требуется выиграть ровно столько времени, сколько нужно. Использование одинаково выглядящих сообщников или даже простое замедление процесса просмотра документов, работы с бюрократией либо отделения истинной информации от ложной способно работать на эту цель. Большинство стратегий обфускации лучше всего действуют совместно с другими приёмами защиты приватности или протеста, но это особенно верно для подходов, направленных на выигрыш времени, которые опираются на уже действующие другие средства уклонения и сопротивления и очень ясное представление о противнике. (См. вопросы в разделе 5.3.)

…чтобы предоставить прикрытие

Этот и следующий подразделы связаны, но различны и значительно пересекаются. Они подходят к одной проблеме с разных сторон: не позволить противнику окончательно связать конкретные действия, результаты или предметы с действующим лицом. Обфускация для прикрытия предполагает сокрытие действия в пространстве других действий. Одни подходы можно реализовать так, чтобы они выдерживали тщательное изучение; другие полагаются на предоставленное контекстом прикрытие, позволяющее ускользнуть от наблюдения. Вспомните записи речевого шума, которые погребают сообщение в десятках голосовых каналов: мы знаем, что говорящий говорит, но не знаем, что именно. Или вспомните подход, на котором в конечном счёте остановилась операция «Вула»: не просто зашифрованная электронная почта, а зашифрованная почта, идеально соответствующая профилю банального международного бизнеса. Связь оперативников АНК могла получить прикрытие как дополнительный слой защиты (наряду с шифрованием и превосходной операционной безопасностью), используя трафик других похожих сообщений, чтобы избежать наблюдения. Один метод предполагает тщательное изучение, другой стремится остаться незамеченным; каждый подходит своей ситуации.

…для правдоподобного отрицания причастности

Если предоставление прикрытия скрывает действие в пространстве других действий, предоставление возможности отрицать причастность скрывает решение и затрудняет уверенное связывание действия и действующего лица. Одно из преимуществ запуска ретранслятора Tor - создаваемый им дополнительный слой неопределённости: начинается ли этот трафик у вас или вы лишь передаёте его за кого-то другого? (У TrackMeNot есть сходный механизм; мы подробнее обсудим его в подразделе о противодействии профилированию.) Подобным образом вспомним имитацию загрузок на сайты утечек, которая затрудняет окончательный вывод о том, что определённый файл был загружен во время сеанса с конкретного IP-адреса. Наконец, подумайте о столь простой вещи, как перемешивание SIM-карт: оно не скрывает деятельность по ношению телефонов и совершению звонков, но затрудняет уверенность в том, что в конкретный момент именно этот человек находится именно с этим телефоном. Хотя предоставление возможности отрицать причастность несколько размывается с предоставлением прикрытия и предотвращением наблюдения за отдельным человеком, оно особенно полезно, когда вы знаете, что противник хочет быть уверен в выборе правильного человека.

…чтобы не допустить раскрытия отдельного человека

Эта несколько необычная цель поначалу может звучать обобщённо (разве не все подходы к обфускации хотят предотвратить наблюдение за отдельным человеком?), но мы вкладываем в неё совершенно определённый смысл. Некоторые обфускационные подходы хорошо подходят для достижения положительного общественного результата: позволяют людям, компаниям, учреждениям и государствам использовать агрегированные данные, не давая возможности применять их для наблюдения за конкретным человеком. Совместное зондирование с сохранением приватности может собирать ценные агрегированные данные о транспортных потоках, не раскрывая ничего достоверного об отдельном транспортном средстве. CacheCloak сохраняет значительную общественную полезность мобильных служб на основе местоположения, одновременно не позволяя поставщикам этих служб отслеживать пользователей (и оставляя открытыми другие способы получения дохода).

Системы обмена картами лояльности дают продуктовым и розничным сетям большую часть ожидаемых выгод (карты приводят к ним покупателей и предоставляют полезные демографические данные, почтовые индексы или сведения о покупках), но не позволяют составлять досье на конкретных покупателей.

…чтобы помешать профилированию

На следующей ступени лестницы всеохватности обфускация против профилирования может мешать наблюдению за отдельными людьми или анализу группы, предоставлять прикрытие или возможность отрицать причастность либо повышать стоимость работы с данными во времени и деньгах. Она может оставлять полезные агрегированные данные нетронутыми или наполнять их неоднозначностью, правдоподобной ложью и бессмыслицей.

Vortex был системой обмена файлами cookie, позволявшей пользователям перескакивать между идентичностями и профилями. Если бы его широко реализовали за пределами стадии прототипа, он сделал бы бесполезным сетевое профилирование ради рекламы. Различные описанные нами службы «клонирования» и дезинформации предлагают сходные средства снижения надёжности профилирования. TrackMeNot позволяет отрицать причастность к поисковым запросам (например, исходил ли от вас запрос «вступить в Чайную партию» или «пушистые секс-игрушки»?) в рамках более общей цели снижения надёжности поисковых профилей. Каким запросам можно доверять? Какие запросы определяют кластер, к которому относится ищущий? В ответ на какие запросы следует показывать рекламу и какие действия и идентичности пользователя следует предоставить в ответ на судебную повестку?

…чтобы выразить протест

Разумеется, TrackMeNot представляет собой жест протеста, как и многие другие наши примеры, например активисты, обменивающиеся картами, и толпы в масках Гая Фокса. Многие стратегии обфускации способны достигать уже упомянутых целей или способствовать им и одновременно служить регистрации недовольства или отказа. Относительно своего обфускационного подхода следует задать важный вопрос: предназначен ли он для того, чтобы вы оставались незамеченным, казались безобидным или заявили о своём несогласии.

5.3. Мой проект обфускации…

Теперь, когда вы понимаете свои цели, можно обратиться к четырём оставшимся вопросам, которые основываются на целях и формируют компоненты проекта обфускации. Как и у шести целей, между этими вопросами есть некоторое пересечение. Они определяют работу обфускационной системы, но не совершенно обособлены и в некоторой степени влияют друг на друга. Мы разделили их по ролям в реализации обфускации.

…индивидуальный или коллективный?

Может ли один человек эффективно осуществить ваш проект обфускации или для него требуются коллективные действия? Одного человека в маске легче выявить и отследить, чем человека без маски, но сто человек в одинаковых масках превращаются в толпу с коллективной идентичностью, что затрудняет приписывание действий отдельным людям. Некоторые проекты обфускации может использовать отдельный человек или малая группа, но по мере присоединения людей они становятся эффективнее. Верным может быть и обратное (см. ниже «…известный или неизвестный?»): метод, который основан на слиянии с окружением и незаметности, то есть действует посредством ухода от тщательного изучения, при широком принятии станет гораздо уязвимее.

Из ответа на вопрос этого подраздела последуют два результата.

Во-первых, метод обфускации, основанный на коллективном действии, может подталкивать к принятию посредством «сетевого эффекта». Если метод становится надёжнее или устойчивее для всех существующих пользователей по мере присоединения новых, можно размышлять о проектировании с точки зрения пересечения порога, за которым становятся очевидны значительные выгоды присоединения и можно вызвать широкое применение. Требуется ли вашему методу определённое число пользователей, прежде чем он станет действительно эффективным? Если да, как вы доведёте его до этой точки? Это возможность подумать, способен ли метод «масштабироваться», то есть продолжать приносить пользу после быстрого принятия множеством людей. Это также относится к удобству использования: для успеха метода, требующего множества пользователей, необходимо тщательно продумать его непосредственную применимость, понятность и дружелюбность. Если для обфускации требуется множество пользователей, план должен включать способ их привлечения. Например, проект Tor признал необходимость большей доступности для пользователей-неспециалистов.

Во-вторых, метод, основанный на относительной неизвестности, то есть на отсутствии широкого принятия или на том, что противник его не ищет, выигрывает от исключительности.

…известный или неизвестный?

Одни методы обфускации используют способность сливаться с создаваемыми ими безобидными данными, чтобы избежать тщательного изучения; другие используют её, чтобы уйти от такого изучения. Может ли ваш метод ради достижения поставленных целей работать, если противник знает о его применении или подробно знаком с принципом работы?

Для многих методов, лишь выигрывающих время, ответ не имеет значения. Например, считает ли оператор радара противника множество точек настоящими самолётами, никак не влияет на способность противника организовать контратаку. Пока работа оператора радара замедлена на десять минут, предоставленная дипольными отражателями обфускация успешна. Более сложные методы способны достигать разных целей в зависимости от того, знает ли противник об их применении. Например, если деятельность AdNauseam неизвестна противнику, она срывает профилирование, наполняя запись рекламных нажатий неизбирательными, бессмысленными

действиями. Если она известна, то одновременно затрудняет профилирование человека и приобретает роль протеста, известного жеста насмешливого отказа. (Построили машину наблюдения, чтобы заставить меня нажать несколько объявлений? Я нажму на все!)

Однако в некоторых случаях различие важно и должно учитываться. Если ваша цель - надолго сделать базу данных менее эффективной или ценной, чтобы противник продолжал ею пользоваться и тем самым действовал на основе вводящей в заблуждение или ложной информации, источники правдоподобной обфускации должны оставаться неизвестными, чтобы их нельзя было выбрать и удалить или нейтрализовать. Формы обфускации, действующие прежде всего как акты публичного протеста, должны явно показывать свою обфускационную природу, чтобы выглядеть отказом, а не подчинением.

…избирательный или общий?

Это самый сложный вопрос с четырьмя различными следствиями, которые необходимо рассмотреть.

Каждая из обсуждавшихся выше целей в той или иной степени опирается на понимание противника, против которого направлена обфускация. Часто это понимание, будь оно формализовано как модель угроз или представляй оно собой обоснованную догадку, фрагментарно, лишено важных компонентов или иным образом нарушено. Впервые нас заинтересовало применение обфускации людьми, которым часто недоставало точного владения стоявшей перед ними проблемой приватности: она была собственностью частной стороны или засекречена, опиралась на непонятные им технологии и методы, среди «противников» были другие люди, добровольно отдававшие свои данные, или проблема существовала одновременно в настоящем и в возможных будущих уязвимостях. Помимо ясного понимания пределов обфускации, то есть знания противника, необходимо помнить о том, чего мы не знаем, и остерегаться полагаться на один-единственный метод защиты конфиденциальной информации. Отсюда возникает вопрос, насколько направленна конкретная стратегия обфускации. Это общая попытка замести следы или создаваемый вами обфускационный шум специально приспособлен к конкретной угрозе, о которой вам кое-что известно? Из ответа следуют ещё несколько вопросов.

Во-первых, направлен ли ваш обфускационный подход на конкретного противника или на любого, кто может собирать и использовать данные о вас? Существует ли конкретная точка анализа, которую вы задерживаете или предотвращаете, или вы просто пытаетесь поднять как можно больше пыли? Пример последнего даёт стратегия, изложенная в приобретённом Apple патенте на «клонирование»: создание множества вариантов пользователя, каждый из которых порождает правдоподобные данные для любого возможного сборщика. Если вы знаете противника, его методы и цели, то можете действовать в обфускации намного точнее.

Если вы знаете противника, возникает второй вопрос: нацелен ли этот противник на вас (или избранную группу) либо вы подвергаетесь более общему агрегированию и анализу данных? В первом случае необходимо найти способы избирательно искажать свои данные. Второй вариант ставит перед обфускатором иную задачу: создание вводящих в заблуждение данных может принимать значительно более широкую форму и напоминать данные, возможно, множества людей.

Это, в свою очередь, ставит третий вопрос: должен ли ваш метод приносить избирательную или общую пользу? Учитывая, что значительная часть работы по наблюдению за данными посвящена не изучению отдельных людей, а использованию выводов из более крупных групп, ваш метод может обфусцировать только ваши следы, а может снижать надёжность общих профилей и моделей. Каждый вариант ставит собственные, отличные от других трудности. Например, если TrackMeNot действует эффективно, он способен ставить под сомнение не только профиль обфускатора, но и профили других людей в наборе данных.

Размышления о выгодоприобретателях ставят четвёртый вопрос: хотите ли вы создать данные, которые в целом невозможно прочитать, чтобы никто не знал и не должен был знать, что настоящее, а что обфускация? Или создать обфусцированные данные, из которых противник не может извлечь никакой ценности (или может извлечь лишь уменьшенную), но которые говорят правду тем, кому необходимо знать, что реально? Вспомните FaceCloak, систему, которая не позволяет Facebook получить доступ к личным данным, предоставляя ему бессмысленный шум, но сохраняет доступность настоящих, значимых личных и социальных данных для друзей. Или рассмотрим систему, предназначенную для сохранения общественно ценных классов данных, например полученных при переписи населения ради эффективного распределения ресурсов или управления, и одновременно предотвращающую идентификацию отдельных субъектов данных внутри них. Создать избирательно читаемую систему гораздо труднее, чем просто создать в целом правдоподобную ложь, но избирательно читаемая система вместе с защитой приватности приносит более широкие выгоды, а трудности её создания представляют собой задачу, которую следует учитывать в самом начале проекта.

…краткосрочный или долгосрочный?

Наконец, на протяжении какого времени ваш проект должен оставаться эффективным? Цель выигрыша времени даёт отправную точку для ответа. Если вы хотите запутать ситуацию лишь на десять минут, это одно; если хотите навсегда сделать базу данных ненадёжной, не заслуживающей доверия и бесполезной для выводов или прогнозов, это гораздо труднее. Важная составляющая информационной асимметрии, которую помогает устранить обфускация, имеет временной характер: проблема «путешествующих во времени роботов из будущего», обсуждавшаяся в главе 3. Сейчас определённые данные могут быть безобидны, но изменение контекста, владельца, средств или законов способно сделать те же данные опасными. Должен ли ваш метод работать только сейчас и лишь для одного возмутительного случая, одной компании и одного способа сбора и анализа или ему необходимо испортить данные так, чтобы им нельзя было доверять в будущем или для других целей? Первое нелегко, но относительно прямолинейно. Второе включает гораздо более широкий набор задач. Этот вопрос стоит рассмотреть сейчас, на этапе разработки, чтобы не оказаться застигнутым врасплох после широкого принятия метода, когда вы поймёте, что он был временным или относился к конкретной компании, связанной определёнными национальными законами, которые больше не применяются.

Помня об этих шести целях и четырёх вопросах, можно оценить основы и некоторые подводные камни создания стратегии обфускации. Разумеется, на этом вопросы не заканчиваются. Обфускации как жизнеспособной практике, мощному и убедительному ответу угнетающим режимам данных помогут условия, позволяющие ей развиваться и процветать. К ним относятся следующие:

• **Прогресс в соответствующих естественных и инженерных науках.** Разработка в статистике, криптографии, системной инженерии, машинном обучении, системной безопасности, сетевых технологиях и моделировании угроз методов, отвечающих на вопросы: сколько шума, какой именно шум, как приспособить его к цели, как защититься от атаки и для каких конкретных проблем обфускация является правильным решением?
• **Прогресс в соответствующих общественных науках, теории и этике.** Ответы на вопросы о том, чего люди хотят и в чём нуждаются при использовании обфускационных систем, и проведение обоснованных нормативных оценок предлагаемых систем.
• **Прогресс в политике и регулировании технологий.** Защита открытых и публичных стандартов и протоколов, позволяющих разработчикам обфускационных систем получать доступ к критической инфраструктуре и взаимодействовать с ней; побуждение крупных публичных систем предлагать разработчикам обфускационных систем открытые API; отказ от принудительного исполнения

Условий обслуживания, запрещающих разумные обфускационные системы.

Обфускация в своём скромном, временном, лучшем, чем ничего, и зависящем от общества виде глубоко переплетена с контекстом применения. Создаёте ли вы личный акт отказа, предназначенный самостоятельно служить жестом протеста независимо от того, действительно ли он снижает полезность сбора данных? Используете ли обфускацию как один элемент более широкого набора средств защиты приватности, приспособленного к группе и противнику, причём эта обфускация должна доказуемо работать против конкретной стратегии анализа данных? Возможно, вы применяете обфускацию на уровне политики или к сбору данных, злоупотребление которыми требует больших усилий, чтобы увеличить стоимость неизбирательного наблюдения. Или, возможно, вы разрабатываете программу либо вносите в неё вклад, чтобы она могла предоставлять услугу со слоем обфускации, который затрудняет любые действия помимо предоставления услуги. У вас может быть доступ к значительным техническим, общественным, политическим и финансовым ресурсам, а может быть мало выбора при заполнении форм, взаимодействии с учреждениями или работе в сети. Но при всех этих разных возможностях вопросы, поставленные нашими целями и проблемами, являются общими для проектов обфускации в разных областях, а их проработка даёт отправную точку для выпуска вашей обфускационной работы в мир, где она сможет начать приносить пользу, создавая шум.

Эпилог

Не мы изобрели обфускацию. Вначале у нас был инструмент, специально предназначенный для того, чтобы мешать работе с журналами поисковых запросов, а затем мы поняли, что он делает нечто такое, что можно увидеть повсюду вокруг нас. Мы взялись дать этому явлению название и прояснить его важнейшие составляющие, чтобы его можно было обобщить и чтобы оно могло стать началом метода, способного сыграть свою роль в решении некоторых из самых трудноразрешимых проблем конфиденциальности, связанных с информационными технологиями, сетями связи, а также сбором и анализом данных. Начав присматриваться, мы поразились разнообразию обнаруженных применений. В части I этой книги мы предложили свод таких возможностей.

В части II мы изложили концепцию обфускации данных как стратегии защиты конфиденциальности, рассмотрели этические вопросы, которые поднимает обфускация, и сформулировали несколько важных вопросов, которые следует задать о любом обфускационном проекте. На протяжении всей книги мы старались подчёркивать, что обфускация - это дополнение к набору средств защиты конфиденциальности, а не замена одного или всех инструментов, на которые мы уже полагаемся. Ей предстоит играть свою роль в составе богатой сети инструментов, теорий, концептуальных схем, навыков и оборудования, позволяющих нам отвечать на современные угрозы конфиденциальности. Мы лишь начали эту работу, дав явлению имя, выявив и определив его. Эта книга представляет собой собрание отправных точек для понимания и применения обфускации. Нам ещё многое предстоит узнать из практики, из самого процесса работы.

Мы описали случаи, когда обфускация действует совместно с другими подходами к защите конфиденциальности, и показали, как её можно объединять с правом, социальными медиа, политикой и шифрованием, чтобы повышать действенность этих альтернатив. Учитывая разнообразие целей обфускации - от выигрыша времени и срыва профилирования до протеста, - можем ли мы разработать разные модели успеха с количественно измеримыми показателями? Разумеется, обфускацию формируют её отношения с противником, однако большинство ситуаций, в которых она применяется, связано с разными видами и степенями неопределённости: неопределённостью относительно того, что можно сделать с данными, того, как эти возможности расширяются при объединении наборов данных, и прочих загадок, присущих информационной асимметрии, которая характеризует повседневную жизнь. Можем ли мы разработать оптимальные методы обфускации при разных видах неопределённости для проектов, специально нацеленных на обеспечение возможности отрицать причастность или на предоставление прикрытия либо на противодействие профилированию, особенно в более долгосрочной перспективе? Можем ли мы взять сложные современные методы анализа данных, такие как передовые нейронные сети и глубокое обучение, и использовать их для разработки более эффективных стратегий обфускации? Мы выявили общие цели и обнаружили принципиально важные вопросы, но существуют ли передовые методы введения обфускации в действие, применимые к разным обфускационным проектам? Ответы на эти вопросы должны дать дальнейшие исследования и практическое применение. По мере того как полезность обфускации будет раскрывать её потенциал, за ними последуют другие вопросы - по крайней мере до тех пор, пока не будет должным образом удовлетворена потребность в более твёрдых и справедливых подходах к регулированию надлежащих методов работы с данными.

У проблемы конфиденциальности нет простого решения, поскольку сама конфиденциальность является решением общественных проблем, которые непрерывно меняются. Некоторые из них естественны и находятся вне нашего контроля; другие имеют технологическую природу и должны находиться под нашим контролем, однако их формирует целый сонм сложных социальных и материальных сил с неопределёнными последствиями. Конфиденциальность означает не прекращение потока данных, а его мудрое и справедливое направление на службу общественным

целям и ценностям, а также тем людям, к которым относятся эти данные, особенно уязвимым и обездоленным. Конфиденциальность должна поддерживать свободы и самостоятельные устремления, питающие конструктивное взаимодействие людей друг с другом и с коллективом. Для достижения понимаемой таким образом конфиденциальности возникло бесчисленное множество обычаев, понятий, инструментов, законов, механизмов и протоколов; к этому собранию мы и добавляем обфускацию, чтобы поддерживать конфиденциальность как деятельный диалог, борьбу и выбор.

Рассмотрев обфускацию посредством основных случаев, отдельных примеров, объяснений и этических вопросов, а также обдумав её эффективность и пригодность для различных целей, вы, возможно, захотите отложить книгу и подумать о внедрении обфускации - в программном обеспечении или политике - для проекта, которым вы руководите, или проекта, которому противостоите: создать толпу и раствориться в ней ради собственной пользы, пользы других и пользы познания через практику.

Примечания

Глава 1

1. Меир Финкель, *О гибкости: восстановление после технологической и доктринальной неожиданности на поле боя* (Stanford University Press, 2011), 125.

2. Фред Коэн, «Применение методов обмана: ханипоты и ложные цели», в *Справочнике по информационной безопасности*, том 3, под ред. Хоссейна Бидголи (Wiley, 2006), 646.

3. Кирилл Маслинский, Сергей Кольцов и Олеся Кольцова, «Изменения тематической структуры русскоязычного LiveJournal: влияние выборов 2011 года», исследовательская работа WP BPR 14/SOC/2013, Национальный исследовательский университет, Москва, 3. Свежие данные о доле пользователей LiveJournal по странам см. на alexa.com.

4. Приведённая здесь статистика LiveJournal взята с livejournal.com. (Этот сайт больше недоступен.)

5. Саймон Шустер, «Почему хакеры атаковали самый популярный в России сервис блогов?», time.com, 7 апреля 2011 года (content.time.com). (Указанное в статье число российских учётных записей, по-видимому, является общим числом учётных записей, а не числом активных учётных записей. Мы считаем активность более содержательной мерой.)

6. Екатерина Пархоменко и Арч Тейт, «Разговор о блогах», *Index on Censorship* 37 (февраль 2008): 174-178 (doi:10.1080/03064220701882822).

7. Сурен Газарян, «Россия: контроль сверху вниз», *Враги Интернета*, 11 марта 2014 года (12mars.rsf.org).

8. Брайан Кребс, «Твиттер-боты заглушают антикремлёвские твиты», *Krebs on Security*, 11 декабря 2008 года (krebsonsecurity.com).

9. Энн Фридман, «Журналистика хештегов», блог #realtalk издания *Columbia Journalism Review*, 29 мая 2014 года (cjr.org).

10. «Твиттер-боты», *Krebs on Security* (krebsonsecurity.com).

11. Мануэль Реда, «Мексика: твиттер-боты саботируют протест против PRI», *Fusion*, 21 мая 2012 года (thisisfusion.tumblr.com).

12. О более прямом применении спама в Twitter на мексиканских выборах, обходящем это правило, см.: Майк Оркатт, «Злоупотребления в Twitter преследуют выборы в Мексике», *MIT Technology Review*, 21 июня 2014 года (technologyreview.com).

13. Джозеф Мейеровиц и Ромит Р. Чоудхури, «Скрывая звёзды фейерверками: конфиденциальность местоположения посредством камуфляжа», в *Трудах 15-й ежегодной международной конференции по мобильным вычислениям и сетям* (ACM, 2009).

14. Там же, 1.

15. Дэниел Хоу и Хелен Ниссенбаум, «TrackMeNot: сопротивление наблюдению в веб-поиске», в *Уроках следа идентичности: анонимность, конфиденциальность и идентичность в сетевом обществе*, под ред. Иэна Керра, Кэрол Лакок и Валери Стивс (Oxford University Press, 2009), 417.

16. О случае с журналами поиска AOL см.: Майкл Барбаро и Том Зеллер-младший, «Раскрыто лицо пользователя поиска AOL № 4417749», *New York Times*, 9 августа 2006 года. О запросе Министерства юстиции к Google см. первоначальную повестку: *Gonzales v. Google, Inc.*, дело

(повестка) CV 06-8006MISC JW (N.D. Cal.), google.com, и последующее решение: *American Civil Liberties Union v. Gonzalez*, дело 98-5591 (E.D. Pa.) (google.com).

17. Обратите внимание, например, что сведения о запуске более персонализированных результатов поиска Google, использующих данные Google+, включают переключатель, позволяющий видеть результаты без влияния истории веб-поиска. Это не удаляет историю, однако представляет историю запросов как нечто, что по крайней мере должно быть необязательным, а не безусловным благом. См.: Амит Сингхал, «Поиск плюс ваш мир», официальный блог Google (googleblog.blogspot.com), 10 января 2012 года.

18. Венсан Тубиана и Хелен Ниссенбаум, «Анализ политики хранения журналов Google», *Journal of Privacy and Confidentiality* 3, № 1 (2011): 3-26 (repository.cmu.edu).

19. Энди Гринберг, *Эта машина убивает секреты: как разоблачители WikiLeaks, шифропанки и хактивисты стремятся освободить мировую информацию* (Dutton, 2012), 157.

20. Там же, 293.

21. Фил Хельмут, Марвин Карлинс и Джо Наварро, *Фил Хельмут представляет: читайте их и пожинайте плоды* (HarperCollins, 2006). (Интересно представить покерную стратегию, основанную на более широком применении обфускации: игрок непрерывно воспроизводит поток манер и типичных теллсов, чтобы любое непроизвольное проявление было трудно вычленить. Но это, вероятно, раздражало бы настолько, что игрока выгнали бы из-за стола.)

22. Уэсли Реммер, «Изучая тайный язык бейсбола», *Bremerton Patriot*, 23 июля 2010 года (bremertonpatriot.com).

23. *Спартак*, режиссёр Стэнли Кубрик (Universal Pictures, 1960).

24. Чарльз Диккенс, *Повесть о двух городах* (Penguin Classics, 2003); Алан Мур и Дэвид Ллойд, *V значит вендетта* (Vertigo/DC Comics, 1982).

25. Марко Дезериис, «Много денег, потому что меня много: проект Лютер Блиссетт и стратегия имени многократного использования», *Thamyris/Intersecting* 21 (2011): 65-93.

26. *Афера Томаса Крауна*, режиссёр Джон Мактирнан (Metro-Goldwyn-Mayer, 1999).

27. *Не пойман - не вор*, режиссёр Спайк Ли (Universal Pictures, 2006).

28. *К северу через северо-запад*, режиссёр Альфред Хичкок (Metro-Goldwyn-Mayer, 1959).

29. Томас Хабинек, *Мир римской песни: от ритуализированной речи к общественному порядку* (Johns Hopkins University Press, 2005), 10.

30. Артур Конан Дойл, «Шесть Наполеонов», в *Возвращении Шерлока Холмса* (Penguin Classics, 2008).

31. Сара Неттер, «Мужчина из штата Вашингтон совершил ограбление с помощью Craigslist и перцового аэрозоля», *ABC News*, 1 октября 2008 года (abcnews.go.com).

32. Йенс Лунд, с ответом Иштвана Деака, «Легенда о короле Кристиане: обмен мнениями», *New York Review of Books* 30, № 5 (1990) (nybooks.com). (То, что конкретный случай с жёлтой звездой вымышлен, ничуть не умаляет героическую историю помощи датчан евреям, которых они укрывали и спасали во время войны.)

33. Лео Голдбергер, ред., *Спасение датских евреев: нравственное мужество в условиях стресса* (New York University Press, 1987).

34. Бен Кафка, *Демон письма* (MIT Press, 2012), 67.

35. Джереми Скахилл и Гленн Гринвальд, «Тайная роль АНБ в американской программе убийств», *The Intercept*, 10 февраля 2014 года (firstlook.org).

36. Проект Tor, «Часто задаваемые вопросы» (torproject.org).

37. *Штат Калифорния против Нирулы*, дело INF 064492 (I.B. Cal.) (cryptome.org).

38. Тим Дженкин, «Разговор с Вулой», *Mayibuye*, май-октябрь 1995 года (anc.org.za).

Глава 2

1. Лин Цзэн и И-Мин Цо, «Рискованная защита паука с помощью заметных ложных целей, внешне похожих на него самого», *Animal Behavior* 78, № 2 (2009): 425-431 (doi:10.1016/j.anbehav.2009.05.017).

2. Рип Эмпсон, «Конкурент сервиса чёрных автомобилей обвиняет Uber в атаке типа DDoS; Uber признаёт тактику "слишком агрессивной"», *TechCrunch*, 24 января 2014 года (techcrunch.com).

3. «Правительство хочет сделать предупреждения о радарах неэффективными», *Le Monde*, 29 ноября 2011 года (lemonde.fr).

4. «Анализ "мгновенного обвала", часть 4: засорение котировками», *Nanex*, 18 июня 2010 года (nanex.net).

5. Там же.

6. Джоаб Джексон, «Карточные игры: следует ли покупателям опасаться того, как супермаркеты используют "карты лояльности" для сбора персональных данных?», *Baltimore City Paper*, 1 октября 2003 года (joabj.com).

7. Роберт Эллис Смит, *Privacy Journal*, март 1999 года, с. 5.

8. epistolary.org, дата обращения: 25 октября 2010 года.

9. «Идеальный покупатель», Cockeyed.com, последнее обновление 11 декабря 2002 года (cockeyed.com).

10. «Проект Hydra» (code.google.com).

11. Несколько технический, но доступный обзор BitTorrent с ясным объяснением трекеров см. в работе: Микель Исаль, Гийом Урвуа-Келлер, Эрнст В. Бирсак, Паскаль Фельбер, Анвар Аль Хамра и Луис Гарсес-Эрисе, «Анатомия BitTorrent: пять месяцев в жизни торрента», *Passive and Active Network Measurement* 3015 (2004): 1-11 (doi: 10.1007/978-3-540-24668-8_1).

12. Хендрик Шульце и Клаус Мохальски, «Исследование Интернета 2008/2009», Ipoque (christopher-parsons.com).

13. Жаклин Беркелл и Александр Фортье, «Раскрытие политики конфиденциальности при поведенческом отслеживании на потребительских сайтах о здоровье», *Труды Американского общества информационной науки и технологии* 50, № 1 (май 2014): 1-9 (doi: 10.1002/meet.14505001087_).

14. Виола Гантер и Михаэль Штрубе, «Поиск оговорок путём погони за словами-лазейками: обнаружение оговорок с использованием тегов Википедии и поверхностных лингвистических признаков», в *Кратких докладах конференции ACL-IJCNLP*, 2009 (dl.acm.org).

15. Дэвид И. Холмс и Ричард С. Форсайт, «Новый взгляд на "Федералиста": новые направления в установлении авторства», *Literary and Linguistic Computing* 10, № 2 (1995): 111-127 (doi: 10.1093/llc/10.2.111).

16. Джосюла Р. Рао и Панкадж Рохатги, «Может ли псевдонимность действительно гарантировать конфиденциальность?», в *Трудах 9-го симпозиума USENIX по безопасности*, 2000 (usenix.org).

17. Даниэль Домшайт-Берг, *Внутри WikiLeaks: моё время с Джулианом Ассанжем на самом опасном сайте мира* (Crown, 2011).

18. Рао и Рохатги, «Может ли псевдонимность действительно гарантировать конфиденциальность?»

19. Моше Коппель и Джонатан Шлер, «Проверка авторства как задача одноклассовой классификации», в *Трудах 21-й Международной конференции по машинному обучению*, 2004 (doi: 10.1145/1015330.1015448).

20. Об Anonymouth см. cs.drexel.edu и github.com.

21. *Драйв*, режиссёр Николас Виндинг Рефн (Film District, 2011).

22. Мариано Чеккато, Массимилиано Ди Пента, Джасвир Награ, Паоло Фалькарин, Филиппо Рикка, Марко Торкиано и Паоло Тонелла, «Эффективность обфускации исходного кода: экспериментальная оценка», в *Трудах 17-й Международной конференции по пониманию программ*, 2009 (doi: 10.1109/ICPC.2009.5090041).

23. См.: Майкл Матеас и Ник Монтфорт, «Тёмный ящик: обфускация, странные языки и эстетика кода», в *Трудах 6-й ежегодной конференции по цифровому искусству и культуре*, 2005 (elmcip.net).

24. Санджам Гарг, Крейг Джентри, Шай Халеви, Мариана Райкова, Амит Сахай и Брент Уотерс, «Кандидатная обфускация неразличимости и функциональное шифрование для всех схем», в *Трудах 54-го ежегодного симпозиума IEEE по основаниям информатики*, 2013 (doi: 10.1109/FOCS.2013.13).

25. Джейявиджаян Раджендран, Озгюр Синаноглу, Майкл Сэм и Рамеш Карри, «Анализ безопасности камуфлирования интегральных схем», представлено на Конференции ACM по компьютерной и коммуникационной безопасности, 2013 (doi: 10.1145/2508859.2516656).

26. Из интервью с Ахерном: Джоан Гудчайлд, «Как полностью исчезнуть», *CSO*, 3 мая 2011 года (csoonline.com).

27. Стивен Картер, «Патент США: 20070094738 A1 - методы загрязнения электронного профилирования», 26 апреля 2007 года (google.com).

28. Рейчел Лоу, «Vortex» (milkred.net). Значительная часть подробностей в этом разделе основана на беседе с Лоу и на её выступлении на инструментальных семинарах Симпозиума по обфускации, прошедшего в Нью-Йоркском университете в 2014 году.

29. Кевин Ладлоу, «Байесовское затопление и манипулирование Facebook», KevinLudlow.com, 23 мая 2012 года (kevinludlow.com).

30. Макс Чо, «Сделайте себя непродаваемым - модель протеста против Facebook», *Yale Law & Technology*, 10 мая 2011 года (yalelawtech.org).

31. Ваньин Ло, Ци Се и Урс Хенгартнер, «FaceCloak: архитектура конфиденциальности пользователей сайтов социальных сетей», в *Трудах Международной конференции IEEE 2009 года по конфиденциальности, безопасности, риску и доверию* (cs.uwaterloo.ca).

32. Чарльз Артур, «Как низкооплачиваемые работники "ферм кликов" создают видимость популярности в Интернете», theguardian.com, 2 августа 2013 года (theguardian.com).

33. Джарон Шнайдер, «Лайки или ложь? Как совершенно честный бизнес могут захватить спамеры Facebook», *TheNextWeb*, 23 января 2004 года (thenextweb.com).

34. Лео Сельваджо, «URME Surveillance», 2014 (urmesurveillance.com).

35. Франсиско Голдман, *Искусство политического убийства: кто убил епископа?* (Grove, 2008).

36. Там же, 109.

Глава 3

1. Краткий обзор истории современной теории конфиденциальности см. в следующих работах: Дэниел Дж. Солов, *Понимание конфиденциальности* (Harvard University Press, 2010); Рут Гэвисон, «Конфиденциальность и пределы права», в *Философских измерениях конфиденциальности: антология*, под ред. Фердинанда Дэвида Шумана (Cambridge University Press, 1984); Дэвид Брин, *Прозрачное общество* (Perseus Books, 1998); Присцилла М. Риган, *Законодательное обеспечение конфиденциальности: технологии, общественные ценности и государственная политика* (University of North Carolina Press, 1995); Джеффри Х. Райман, «По дороге в паноптикум: философское исследование рисков для конфиденциальности, создаваемых дорожными технологиями будущего», *Santa Clara High Technology Journal* 11, № 1 (1995): 27-44 (digitalcommons.law.scu.edu); Алан Ф. Уэстин, «Наука, конфиденциальность и свобода: проблемы и предложения для 1970-х годов. Часть I - современное влияние наблюдения на конфиденциальность», *Columbia Law Review* 66, № 6 (1966): 1003-1050 (jstor.org).

2. Различающиеся теории см. в следующих работах: Хелен Ниссенбаум, *Конфиденциальность в контексте: технологии, политика и целостность общественной жизни* (Stanford University Press, 2009); Джули Э. Коэн, «Жизни под наблюдением: информационная конфиденциальность и субъект как объект», *Stanford Law Review* 52 (май 2000): 1373-1437 (scholarship.law.georgetown.edu); Дэниел Дж. Солов, «Таксономия конфиденциальности», *University of Pennsylvania Law Review* 154, № 3 (2006): 477-560 (doi: 10.2307/40041279); Кристина Э. Нипперт-Энг, *Острова конфиденциальности* (University of Chicago Press, 2010); Михаэль Бирнхак и Йофи Тирош, «Обнажённый перед машиной: нарушает ли сканирование в аэропорту конфиденциальность?», *Ohio State Law Journal* 74, № 6 (2013): 1263-1306.

3. См.: Пол Дуриш, «Коллективная информационная практика: исследование конфиденциальности и безопасности как социальных и культурных явлений», *Human-Computer Interaction* 21, № 3 (2006): 319-342 (doi: 10.1207/s15327051hci2103_2); Пол Дуриш, Эмили Трошински и Шарлотта Ли, «Ответственность присутствия: новое осмысление систем, основанных на местоположении», в *Трудах конференции SIGCHI по человеческим факторам в вычислительных системах*, 2008 (doi: 10.1145/1357054.1357133).

4. Хелен Ниссенбаум, *Конфиденциальность в контексте: технологии, политика и целостность общественной жизни* (Stanford University Press, 2009).

5. Кевин Келли, *Вне контроля: новая биология машин, социальных систем и экономического мира* (Addison-Wesley, 1994), с. 176.

6. Гилберт Кит Честертон, «Знамение сломанного меча», в *Неведении отца Брауна* (Cassell, 1947), с. 143.

7. *Nichia Corp против Argos Ltd.*, дело A3/2007/0572, EWCA Civ 741 (19 июля 2007 года) (bailii.org).

8. *Симпсоны*, «Троянский лимон», 14 мая 1995 года.

9. Ханна Роуз Шелл, *Прятки: камуфляж, фотография и средства разведки* (Zone Books, 2012).

10. Дональд Х. Рамсфелд, 12 февраля 2002 года (11:30), «Брифинг новостей Министерства обороны - министр Рамсфелд и генерал Майерс», Министерство обороны США / Federal News Service, Inc. (defense.gov).

11. Брэд Темплтон, «Пороки облачных вычислений: переносимость данных и единый вход», представлено на конференции BIL, 2009 (vimeo.com).

12. Таль Зарски, «Прозрачные прогнозы», *University of Illinois Law Review* 2013, № 4: 1519-1520.

13. Солон Барокас, «Интеллектуальный анализ данных и дискурс о дискриминации», в *Трудах семинара по этике данных на конференции ACM по обнаружению знаний и интеллектуальному анализу данных*, Нью-Йорк, 2014.

14. См. в особенности: Джош Лауэр, «Хороший потребитель: кредитная отчётность и изобретение финансовой идентичности в Соединённых Штатах, 1840-1940», *Enterprise & Society* 11, № 4 (2010): 686-694 (doi: 10.1093/es/khq091); Лауэр, *Хороший потребитель: история кредитного наблюдения и финансовой идентичности в Америке* (Columbia University Press, готовится к публикации).

15. Энтони Гидденс, «Риск и ответственность», *Modern Law Review* 62, № 1 (1999): 1-10 (doi: 10.1111/1468-2230.00188). См. также развитие этой идеи в книге Ульриха Бека *Общество риска: на пути к новой современности* (SAGE, 1999).

16. Бен Коэн, «После "Сэнди" подключённые к сети жители Нью-Йорка снова обращаются к телефонам-автоматам», *Wall Street Journal*, 31 октября 2012 года.

17. Джеймс К. Скотт, *Оружие слабых: повседневные формы крестьянского сопротивления* (Yale University Press, 1987).

18. О разнообразных примечательных ответах на наблюдение см.: Гэри Т. Маркс, «Общественность как партнёр? Технологии могут сделать нас как помощниками, так и линчевателями», *IEEE Security and Privacy* 11, № 5 (2013): 56-61 (doi: doi.ieeecomputersociety.org); Маркс, *Под прикрытием: полицейское наблюдение в Америке* (University of California Press, 1989); Маркс, «Технологии и социальный контроль: поиск неуловимой серебряной пули продолжается», в *Международной энциклопедии социальных и поведенческих наук*, 2-е изд. (Elsevier, готовится к публикации); Кеннет А. Бамбергер и Дейрдре К. Маллиган, «Принятие решений о конфиденциальности в административных ведомствах», *University of Chicago Law Review* 75, № 1 (2008): 75-107 (ssrn.com); Кэтрин Дж. Стрэндберг и Даниэла Стэн Райку, *Конфиденциальность и технологии идентичности: междисциплинарный разговор* (Springer, 2006).

19. Скотт подробно развивает эту концепцию в книге *Господство и искусства сопротивления: скрытые сценарии* (Yale University Press, 1992).

20. Рассуждения о развитии идеи «монетизации» данных и о роли, которую она играет в современных компаниях и учреждениях, см.: Джина Нефф, «Почему большие данные нас не вылечат», *Big Data* 1, № 3 (2013): 117-123 (doi: 10.1089/big.2013.0029); Бриттани Фиоре-Сильфваст и Джина Нефф, «Коммуникация, посредничество и ожидания от данных: валентности данных в сообществах здоровья и благополучия», неопубликованная рукопись (на рецензировании в *International Journal of Communication*).

21. Google Inc., форма 10-Q Комиссии по ценным бумагам и биржам за период, завершившийся 31 октября 2009 года (подана 4 ноября 2009 года), с. 23, с SEC.gov (sec.gov).

22. Мартин Хайдеггер, *Вопрос о технике и другие эссе* (Garland, 1977).

23. Подробнее о Сноудене см.: Гленн Гринвальд, Юэн Макаскилл и Лора Пойтрас, «Эдвард Сноуден: разоблачитель, стоящий за откровениями о слежке АНБ», theguardian.com, 11 июня 2013 года (theguardian.com); Ладар Левисон, «Секреты, ложь и электронная почта Сноудена: почему меня вынудили закрыть Lavabit», theguardian.com, 20 мая 2014 года (theguardian.com); Гленн Гринвальд, *Негде спрятаться: Эдвард Сноуден, АНБ и государство наблюдения США* (Metropolitan Books, 2014); Кэтрин Дж. Стрэндберг, «Дом, дом в Сети и другие последствия техносоциальных изменений для Четвёртой поправки», *University of Maryland Law Review* 70, апрель 2011: 614-680 (ssrn.com).

24. Идея «клептографии» в её более широком определении даёт полезный способ понять этот подход. Первоначальное, более узкое определение - использование криптосистем типа «чёрный ящик», реализованных на закрытом аппаратном обеспечении, - см. в работе: Адам Янг и Моти Юнг, «Клептография: применение криптографии против криптографии», в *Достижениях криптологии - Eurocrypt '97*, под ред. Вальтера Фуми (Springer, 1997). Более широкое определение - убеждение противника применять такую форму криптографии, которую вы заведомо можете взломать, либо использование худших альтернатив из соображений доступности или удобства - см. в работе: Филип Халлам-Бейкер, «Соображения безопасности для защиты от PRISM», черновик 3.4 Рабочей группы по инженерным задачам Интернета (IETF), 2013 (tools.ietf.org).

25. Арвинд Нараянан, «Что случилось с криптографической мечтой? Часть 2», *IEEE Security and Privacy* 11, № 3 (2013): 68-71 (doi: doi.ieeecomputersociety.org).

Глава 4

1. О TrackMeNot см. cs.nyu.edu.

2. Гэри Т. Маркс, «Гвоздь в ботинке: нейтрализация нового наблюдения и сопротивление ему», *Journal of Social Issues* 59, № 2 (2003): 369-390 (doi: 10.1111/1540-4560.00069).

3. См.: Джеймс Эдвин Махон, «Определение лжи и обмана», в *Стэнфордской философской энциклопедии* (plato.stanford.edu); Джон Финнис, «Моральная, политическая и правовая философия Фомы Аквинского», в *Стэнфордской философской энциклопедии* (plato.stanford.edu).

4. Сиссела Бок, *Ложь: нравственный выбор в общественной и частной жизни* (Vintage Books, 1999).

5. Джозеф Т. Мейеровиц и Ромит Рой Чоудхури, CacheCloack, 2009 (cachecloak.co.uk).

6. См. также: Крис Джей Хуфнэгл, Ашкан Солтани, Натаниэль Гуд и Дитрих Дж. Вамбах, «Поведенческая реклама: предложение, от которого невозможно отказаться», *Harvard Law & Policy Review* 6, август (2012): 273-296 (ssrn.com); Алисия М. Макдональд и Лорри Ф. Кранор, «Стоимость чтения политик конфиденциальности», *I/S* 4, № 3 (2008): 540-565 (lorrie.cranor.org); Кэтрин Дж. Стрэндберг, «Свободное падение: разрыв между предпочтениями потребителей и онлайн-рынком», *University of Chicago Legal Forum* 95 (2013): 95-172 (ssrn.com); Крис Джей Хуфнэгл и Ян Уиттингтон, «Бесплатно: учёт издержек самой популярной цены Интернета», *UCLA Law Review* 61 (2014): 606-670 (ssrn.com).

7. См.: Джозеф Туроу, Крис Джей Хуфнэгл, Дейрдре К. Маллиган, Натаниэль Гуд и Йенс Гроссклагс, «Федеральная торговая комиссия и конфиденциальность потребителей в наступающем десятилетии», *I/S* 3, № 3 (2007): 723-749 (ssrn.com); Джозеф Туроу, *Ваше ежедневное "я": как новая рекламная индустрия определяет вашу идентичность и вашу ценность* (Yale University Press, 2013).

8. Исайя Берлин, *Кривое древо человечества: главы из истории идей* (Princeton University Press, 2013), 2.

9. Дэниел Дж. Солов и Пол М. Шварц, *Основы права конфиденциальности*, 2-е изд. (International Association of Privacy Professionals, 2013).

10. См.: Дэниел Дж. Солов, «Самоуправление конфиденциальностью и дилемма согласия», *Harvard Law Review* 126 (2013): 1880-1903 (ssrn.com); Лорен Э. Уиллис, «Почему бы не сделать конфиденциальность настройкой по умолчанию?», *Berkeley Technology Law Journal* 29 (2014): 61-134 (ssrn.com); Джеймс Гриммельманн, «Саботаж Do Not Track», *The Laboratorium*, 19 июня 2012 года (laboratorium.net).

11. Подробнее о Сноудене см.: Гленн Гринвальд, Юэн Макаскилл и Лора Пойтрас, «Эдвард Сноуден: разоблачитель, стоящий за откровениями о слежке АНБ», theguardian.com, 11 июня 2013 года (theguardian.com); Ладар Левисон, «Секреты, ложь и электронная почта Сноудена: почему меня вынудили закрыть Lavabit», theguardian.com, 20 мая 2014 года (theguardian.com); Гленн Гринвальд, *Негде спрятаться: Эдвард Сноуден, АНБ и государство наблюдения США* (Metropolitan Books, 2014); Джошуа Итон и Бен Пивен, «Хронология откровений Эдварда Сноудена», theguardian.com, 5 июня 2013 года (america.aljazeera.com).

12. Джон Ролз, *Теория справедливости* (Harvard University Press, 1971).

13. Там же, 173.

14. Артур Рипстейн, *Равенство, ответственность и право* (Cambridge University Press, 1999).

15. Йерун Ван Ден Ховен и Эмма Руксби, «Распределительная справедливость и ценность информации: подход в широком смысле Ролза», в *Информационных технологиях и моральной философии*, под ред. Джона Уэкерта (Cambridge University Press, 2008), 376.

16. См.: danah boyd, *Всё сложно: социальная жизнь сетевых подростков* (Yale University Press, 2014); Колин Купман, «Взаимосвязанные сетью сообщества: формирующиеся политические условия Интернета», доклад, представленный на конференции *Ars Synthetica: антропология современности*, Санта-Круз, 2009.

17. Франсиско Голдман, *Искусство политического убийства: кто убил епископа?* (Grove, 2007).

18. Анатоль Франс, *Красная лилия* (Borgo, 2002), 64.

19. Филип Петтит, *Республиканизм: теория свободы и государственного управления* (Oxford University Press, 1997), 73, 79.

20. См.: Виктор Майер-Шёнбергер и Кеннет Кукьер, *Большие данные: революция, которая изменит то, как мы живём, работаем и мыслим* (Houghton Mifflin Harcourt, 2013), 94; Солон Барокас, «Интеллектуальный анализ данных и дискурс о дискриминации», в *Трудах семинара по этике данных на конференции по обнаружению знаний и интеллектуальному анализу данных*, 2014; Таль Зарски, «Прозрачные прогнозы», *University of Illinois Law Review* 2013, № 4 (2013): 1519-1520.

21. Петтит, *Республиканизм*, 80, 272.

22. Ролз, *Теория справедливости*.

23. Майер-Шёнбергер и Кукьер, *Большие данные*; Туроу, *Ваше ежедневное "я"*.

24. Джереми Уолдрон, *Пытки, террор и компромиссы: философия для Белого дома* (Oxford University Press, 2012).

25. Туроу, *Ваше ежедневное "я"*; Хуфнэгл, Солтани, Гуд и Вамбах, «Поведенческая реклама».

Глава 5

1. *Напряги извилины*, «Мистер Биг», 18 сентября 1965 года.

2. См.: Синтия Дворк и Аарон Рот, «Алгоритмические основания дифференциальной конфиденциальности», *Foundations and Trends in Theoretical Computer Science* 9, № 3-4 (2014): 211-407 (doi: dx.doi.org); Синтия Дворк, Фрэнк Макшерри, Кобби Ниссим и Адам Смит, «Калибровка шума по чувствительности при конфиденциальном анализе данных», в *Трудах Третьей конференции по теории криптографии*, 2006 (doi: 10.1007/11681878_14).

3. Адам Шостак, *Моделирование угроз: проектирование ради безопасности* (Wiley, 2014).

4. danah boyd, *Всё сложно: социальная жизнь сетевых подростков* (Yale University Press, 2014), 65.

5. Там же, 69.

6. Джион Грин, «Оценка напильников, сейфов и хранилищ», в *Справочнике по предотвращению потерь и преступлений*, под ред. Лоуренса Феннелли (Elsevier, 2012), 358.

Библиография

Бамбергер, Кеннет А., и Дейрдре К. Маллиган. «Принятие решений о конфиденциальности в административных ведомствах». *University of Chicago Law Review* 75, № 1 (2008): 75-107 (ssrn.com).

Барбаро, Майкл, и Том Зеллер-младший. «Раскрыто лицо пользователя поиска AOL № 4417749». *New York Times*, 9 августа 2006 года.

Барокас, Солон. «Интеллектуальный анализ данных и дискурс о дискриминации». В *Трудах семинара по этике данных на конференции ACM по обнаружению знаний и интеллектуальному анализу данных*. Нью-Йорк, 2014.

Бек, Ульрих. *Общество риска: на пути к новой современности*. Лондон: SAGE, 1999.

Берлин, Исайя. *Кривое древо человечества: главы из истории идей*. Princeton University Press, 2013.

Бирнхак, Михаэль, и Йофи Тирош. «Обнажённый перед машиной: нарушает ли сканирование в аэропорту конфиденциальность?» *Ohio State Law Journal* 74, № 6 (2013): 1263-1306 (ssrn.com).

Бок, Сиссела. *Ложь: нравственный выбор в общественной и частной жизни*. Нью-Йорк: Vintage Books, 1999.

boyd, danah. *Всё сложно: социальная жизнь сетевых подростков*. Нью-Хейвен: Yale University Press, 2014.

Брин, Дэвид. *Прозрачное общество*. Нью-Йорк: Perseus Books, 1998.

Беркелл, Жаклин, и Александр Фортье. «Раскрытие политики конфиденциальности при поведенческом отслеживании на потребительских сайтах о здоровье». *Proceedings of the American Society for Information Science and Technology* 50, № 1 (2014): 1-9 (doi:10.1002/meet.14505001087).

Чеккато, Мариано, Массимилиано Ди Пента, Джасвир Награ, Паоло Фалькарин, Филиппо Рикка, Марко Торкиано и Паоло Тонелла. «Эффективность обфускации исходного кода: экспериментальная оценка». В *Трудах 17-й Международной конференции по пониманию программ*, 2009 (doi: 10.1109/ICPC.2009.5090041).

Честертон, Гилберт Кит. «Знамение сломанного меча». В *Неведении отца Брауна*. Лондон: Cassell, 1947.

Чо, Макс. «Сделайте себя непродаваемым - модель протеста против Facebook». Блог *Yale Law & Technology*, 10 мая 2011 года (yalelawtech.org).

Коэн, Фред. «Применение методов обмана: ханипоты и ложные цели». В *Справочнике по информационной безопасности*, том 3, под ред. Хоссейна Бидголи. Хобокен: Wiley, 2006.

Коэн, Джули Э. «Жизни под наблюдением: информационная конфиденциальность и субъект как объект». *Stanford Law Review* 52, май (2000): 1373-1437 (scholarship.law.georgetown.edu).

Дезериис, Марко. «Много денег, потому что меня много: проект Лютер Блиссетт и стратегия имени многократного использования». *Thamyris/Intersecting* 21 (2011): 65-93.

Домшайт-Берг, Даниэль. *Внутри WikiLeaks: моё время с Джулианом Ассанжем на самом опасном сайте мира*. Нью-Йорк: Crown, 2011.

Дуриш, Пол, Эмили Трошински и Шарлотта Ли. «Ответственность присутствия: новое осмысление систем, основанных на местоположении». В *Трудах конференции SIGCHI по человеческим факторам в вычислительных системах*, 2008 (doi: 10.1145/1357054.1357133).

Дуриш, Пол. «Коллективная информационная практика: исследование конфиденциальности и безопасности как социальных и культурных явлений». *Human-Computer Interaction* 21, № 3 (2006): 319-342 (doi:10.1207/s15327051hci2103_2).

Дворк, Синтия, и Аарон Рот. «Алгоритмические основания дифференциальной конфиденциальности». *Foundations and Trends in Theoretical Computer Science* 9, № 3-4 (2014): 211-407 (doi: 10.1561/0400000042).

Дворк, Синтия, Фрэнк Макшерри, Кобби Ниссим и Адам Смит. «Калибровка шума по чувствительности при конфиденциальном анализе данных». В *Трудах Третьей конференции по теории криптографии*, 2006 (doi: 10.1007/11681878_14).

Финкель, Меир. *О гибкости: восстановление после технологической и доктринальной неожиданности на поле боя*. Stanford University Press, 2011.

Финнис, Джон. «Моральная, политическая и правовая философия Фомы Аквинского». В *Стэнфордской философской энциклопедии*, под ред. Эдварда Н. Залты (plato.stanford.edu).

Фиоре-Сильфваст, Бриттани, и Джина Нефф. «Коммуникация, посредничество и ожидания от данных: валентности данных в сообществах здоровья и благополучия». На рецензировании в *International Journal of Communication*.

Франс, Анатоль. *Красная лилия*. Сан-Бернардино: Borgo, 2002.

Гантер, Виола, и Михаэль Штрубе. «Поиск оговорок путём погони за словами-лазейками: обнаружение оговорок с использованием тегов Википедии и поверхностных лингвистических признаков». В *Кратких докладах конференции ACL-IJCNLP*, 2009 (dl.acm.org).

Гарг, Санджам, Крейг Джентри, Шай Халеви, Мариана Райкова, Амит Сахай и Брент Уотерс. «Кандидатная обфускация неразличимости и функциональное шифрование для всех схем». Представлено на 54-м ежегодном симпозиуме IEEE по основаниям информатики, 2013 (doi: 10.1109/FOCS.2013.13).

Гэвисон, Рут. «Конфиденциальность и пределы права». В *Философских измерениях конфиденциальности: антология*, под ред. Фердинанда Дэвида Шумана. Cambridge University Press, 1984.

Гидденс, Энтони. «Риск и ответственность». *Modern Law Review* 62, № 1 (1999): 1-10 (doi:10.1111/1468-2230.00188).

Голдбергер, Лео, ред. *Спасение датских евреев: нравственное мужество в условиях стресса*. New York University Press, 1987.

Голдман, Франсиско. *Искусство политического убийства: кто убил епископа?* Нью-Йорк: Grove, 2007.

Грин, Джион. «Оценка напильников, сейфов и хранилищ». В *Справочнике по предотвращению потерь и преступлений*, под ред. Лоуренса Феннелли. Оксфорд: Elsevier, 2012.

Гринберг, Энди. *Эта машина убивает секреты: как разоблачители WikiLeaks, шифропанки и хактивисты стремятся освободить мировую информацию*. Нью-Йорк: Dutton, 2012.

Гринвальд, Гленн. *Негде спрятаться: Эдвард Сноуден, АНБ и государство наблюдения США*. Нью-Йорк: Metropolitan Books, 2014.

Хабинек, Томас. *Мир римской песни: от ритуализированной речи к общественному порядку*. Балтимор: Johns Hopkins University Press, 2005.

Хайдеггер, Мартин. *Вопрос о технике и другие эссе*. Нью-Йорк: Garland, 1977.

Хельмут, Фил, Марвин Карлинс и Джо Наварро. *Фил Хельмут представляет: читайте их и пожинайте плоды*. Нью-Йорк: HarperCollins, 2006.

Холмс, Дэвид И., и Ричард С. Форсайт. «Новый взгляд на "Федералиста": новые направления в установлении авторства». *Literary and Linguistic Computing* 10, № 2 (1995): 111-127 (doi: 10.1093/llc/10.2.111).

Хуфнэгл, Крис Джей, и Ян Уиттингтон. «Бесплатно: учёт издержек самой популярной цены Интернета». *UCLA Law Review*, Школа права Калифорнийского университета в Лос-Анджелесе 61 (2014): 606-670 (ssrn.com).

Хуфнэгл, Крис Джей, Ашкан Солтани, Натаниэль Гуд и Дитрих Дж. Вамбах. «Поведенческая реклама: предложение, от которого невозможно отказаться». *Harvard Law & Policy Review* 6, август (2012): 273-296 (ssrn.com).

Хоу, Дэниел, и Хелен Ниссенбаум. «TrackMeNot: сопротивление наблюдению в веб-поиске». В *Уроках следа идентичности: анонимность, конфиденциальность и идентичность в сетевом обществе*, под ред. Иэна Керра, Кэрол Лакок и Валери Стивс. Oxford University Press, 2009.

Исаль, Микель, Гийом Урвуа-Келлер, Эрнст В. Бирсак, Паскаль Фельбер, Анвар Аль Хамра и Луис Гарсес-Эрисе. «Анатомия BitTorrent: пять месяцев в жизни торрента». В *Пассивном и активном измерении сетей*, под ред. Чади Бараката и Иэна Пратта. Берлин: Springer, 2004.

Дженкин, Тим. «Разговор с Вулой». *Mayibuye*, май-октябрь 1995 года (anc.org.za).

Кафка, Бен. *Демон письма*. Кембридж: MIT Press, 2012.

Келли, Кевин. *Вне контроля: новая биология машин, социальных систем и экономического мира*. Индианаполис: Addison-Wesley, 1994.

Купман, Колин. «Взаимосвязанные сетью сообщества: формирующиеся политические условия Интернета». Доклад, представленный на конференции *Ars Synthetica: антропология современности*, Санта-Круз, 2009.

Коппель, Моше, и Джонатан Шлер. «Проверка авторства как задача одноклассовой классификации». В *Трудах 21-й Международной конференции по машинному обучению*, 2004 (doi: 10.1145/1015330.1015448).

Лейн, Джулия, Виктория Стодден, Стефан Бендер и Хелен Ниссенбаум, ред. *Конфиденциальность, большие данные и общественное благо: схемы взаимодействия*. Cambridge University Press, 2014.

Лауэр, Джош. «Хороший потребитель: кредитная отчётность и изобретение финансовой идентичности в Соединённых Штатах, 1840-1940». *Enterprise and Society* 11, № 4 (2010): 686-694 (doi:10.1093/es/khq091).

Лауэр, Джош. *Хороший потребитель: история кредитного наблюдения и финансовой идентичности в Америке*. Нью-Йорк: Columbia University Press, готовится к публикации.

Лунд, Йенс, с ответом Иштвана Деака. «Легенда о короле Кристиане: обмен мнениями». *New York Review of Books* 30, № 5 (1990) (nybooks.com).

Ло, Ваньин, Ци Се и Урс Хенгартнер. «FaceCloak: архитектура конфиденциальности пользователей сайтов социальных сетей». В *Трудах Международной конференции IEEE 2009 года по конфиденциальности, безопасности, риску и доверию* (cs.uwaterloo.ca).

Махон, Джеймс Эдвин. «Определение лжи и обмана». В *Стэнфордской философской энциклопедии*, под ред. Эдварда Н. Залты (plato.stanford.edu).

Маркс, Гэри Т. «Гвоздь в ботинке: нейтрализация нового наблюдения и сопротивление ему». *Journal of Social Issues* 59, № 2 (2003): 369-390 (doi:10.1111/1540-4560.00069).

Маркс, Гэри Т. «Технологии и социальный контроль: поиск неуловимой серебряной пули продолжается». В *Международной энциклопедии социальных и поведенческих наук*, 2-е изд. Оксфорд: Elsevier, готовится к публикации.

Маркс, Гэри Т. «Общественность как партнёр? Технологии могут сделать нас как помощниками, так и линчевателями». *IEEE Security and Privacy* 11, № 5 (2013): 56-61 (doi: doi.ieeecomputersociety.org).

Маркс, Гэри Т. *Под прикрытием: полицейское наблюдение в Америке*. Окленд: University of California Press, 1989.

Маслинский, Кирилл, Сергей Кольцов и Олеся Кольцова. «Изменения тематической структуры русскоязычного LiveJournal: влияние выборов 2011 года». Исследовательская работа WP BPR 14/SOC/2013, Национальный исследовательский университет, Москва, 2013.

Матеас, Майкл, и Ник Монтфорт. «Тёмный ящик: обфускация, странные языки и эстетика кода». В *Трудах 6-й ежегодной конференции по цифровому искусству и культуре*, 2005 (elmcip.net).

Майер-Шёнбергер, Виктор, и Кеннет Кукьер. *Большие данные: революция, которая изменит то, как мы живём, работаем и мыслим*. Нью-Йорк: Houghton Mifflin Harcourt, 2013.

Макдональд, Алисия М., и Лорри Ф. Кранор. «Стоимость чтения политик конфиденциальности». *I/S* 4, № 3 (2008): 540-565 (lorrie.cranor.org).

Мейеровиц, Джозеф, и Ромит Р. Чоудхури. «Скрывая звёзды фейерверками: конфиденциальность местоположения посредством камуфляжа». В *Трудах 15-й ежегодной международной конференции по мобильным вычислениям и сетям*. 2009.

Мур, Алан, и Дэвид Ллойд. *V значит вендетта*. Нью-Йорк: Vertigo/DC Comics, 1982.

Нараянан, Арвинд. «Что случилось с криптографической мечтой? Часть 2». *IEEE Security and Privacy* 11, № 3 (2013): 68-71 (doi: doi.ieeecomputersociety.org).

Нефф, Джина. «Почему большие данные нас не вылечат». *Big Data* 1, № 3 (2013): 117-123 (doi:10.1089/big.2013.0029).

Нипперт-Энг, Кристина Э. *Острова конфиденциальности*. University of Chicago Press, 2010.

Ниссенбаум, Хелен. *Конфиденциальность в контексте: технологии, политика и целостность общественной жизни*. Stanford University Press, 2009.

Оркатт, Майк. «Злоупотребления в Twitter преследуют выборы в Мексике». *MIT Technology Review*, 21 июня 2014 года (technologyreview.com).

Пархоменко, Екатерина, и Арч Тейт. «Разговор о блогах». *Index on Censorship* 37, февраль (2008): 174-178 (doi: 10.1080/03064220701882822).

Петтит, Филип. *Республиканизм: теория свободы и государственного управления*. Oxford University Press, 1997.

Раджендран, Джейявиджаян, Озгюр Синаноглу, Майкл Сэм и Рамеш Карри. «Анализ безопасности камуфлирования интегральных схем». Представлено на Конференции ACM по компьютерной и коммуникационной безопасности, 2013 (doi:10.1145/2508859.2516656).

Рао, Джосюла Р., и Панкадж Рохатги. «Может ли псевдонимность действительно гарантировать конфиденциальность?» В *Трудах 9-го симпозиума USENIX по безопасности*, 2000 (usenix.org).

Ролз, Джон. *Теория справедливости*. Кембридж: Harvard University Press, 1971.

Риган, Присцилла М. *Законодательное обеспечение конфиденциальности: технологии, общественные ценности и государственная политика*. Чапел-Хилл: University of North Carolina Press, 1995.

Райман, Джеффри Х. «По дороге в паноптикум: философское исследование рисков для конфиденциальности, создаваемых дорожными технологиями будущего». *Santa Clara High Technology Journal* 11, № 1 (1995): 27-44 (digitalcommons.law.scu.edu).

Рипстейн, Артур. *Равенство, ответственность и право*. Cambridge University Press, 1999.

Скотт, Джеймс К. *Господство и искусства сопротивления: скрытые сценарии*. Нью-Хейвен: Yale University Press, 1992.

Шелл, Ханна Роуз. *Прятки: камуфляж, фотография и средства разведки*. Кембридж: Zone Books, 2012.

Шостак, Адам. *Моделирование угроз: проектирование ради безопасности*. Индианаполис: Wiley, 2014.

Солов, Дэниел Дж. «Таксономия конфиденциальности». *University of Pennsylvania Law Review* 154, № 3 (2006): 477-560 (doi: 10.2307/40041279).

Солов, Дэниел Дж. «Самоуправление конфиденциальностью и дилемма согласия». *Harvard Law Review* 126 (2013): 1880-1903 (ssrn.com).

Солов, Дэниел Дж. *Понимание конфиденциальности*. Кембридж: Harvard University Press, 2010.

Солов, Дэниел Дж., и Пол М. Шварц. *Основы права конфиденциальности*, 2-е изд. Портсмут: International Association of Privacy Professionals, 2013.

Стрэндберг, Кэтрин Дж. «Свободное падение: разрыв между предпочтениями потребителей и онлайн-рынком». *University of Chicago Legal Forum* 95 (2013): 95-172 (ssrn.com).

Стрэндберг, Кэтрин Дж. «Дом, дом в Сети и другие последствия техносоциальных изменений для Четвёртой поправки». *University of Maryland Law Review* 70, апрель (2011): 614-680 (ssrn.com).

Стрэндберг, Кэтрин Дж., и Даниэла Стэн Райку. *Конфиденциальность и технологии идентичности: междисциплинарный разговор*. Нью-Йорк: Springer, 2006.

Темплтон, Брэд. «Пороки облачных вычислений: переносимость данных и единый вход». Представлено на конференции BIL, 2009 (vimeo.com).

Тубиана, Венсан, и Хелен Ниссенбаум. «Анализ политики хранения журналов Google». *Journal of Privacy and Confidentiality* 3, № 1 (2011): 3-26 (repository.cmu.edu).

Цзэн, Лин, и И-Мин Цо. «Рискованная защита паука с помощью заметных ложных целей, внешне похожих на него самого». *Animal Behaviour* 78, № 2 (2009): 425-431 (doi: 10.1016/j.anbehav.2009.05.017).

Туроу, Джозеф. *Ваше ежедневное "я": как новая рекламная индустрия определяет вашу идентичность и вашу ценность*. Нью-Хейвен: Yale University Press, 2013.

Туроу, Джозеф, Крис Джей Хуфнэгл, Дейрдре К. Маллиган, Натаниэль Гуд и Йенс Гроссклагс. «Федеральная торговая комиссия и конфиденциальность потребителей в наступающем десятилетии». *I/S* 3, № 3 (2007): 723-749 (ssrn.com).

Ван ден Ховен, Йерун, и Эмма Руксби. «Распределительная справедливость и ценность информации: подход в широком смысле Ролза». В *Информационных технологиях и моральной философии*, под ред. Джона Уэкерта. Cambridge University Press, 2008.

Уолдрон, Джереми. *Пытки, террор и компромиссы: философия для Белого дома*. Oxford University Press, 2012.

Уэстин, Алан Ф. «Наука, конфиденциальность и свобода: проблемы и предложения для 1970-х годов. Часть I - современное влияние наблюдения на конфиденциальность». *Columbia Law Review* 66, № 6 (1966): 1003-1050 (jstor.org).

Уиллис, Лорен Э. «Почему бы не сделать конфиденциальность настройкой по умолчанию?» *Berkeley Technology Law Journal* 29 (2014): 61-134 (ssrn.com).

Янг, Адам, и Моти Юнг. «Клептография: применение криптографии против криптографии». В *Достижениях криптологии - Eurocrypt '97*, под ред. Вальтера Фуми, 62-74. Берлин: Springer, 1997.

Зарски, Таль. «Прозрачные прогнозы». *University of Illinois Law Review* 2013, № 4: 1519-1520.