CARISSA VÉLIZ

PRIVACY IS POWER

Why and How You Should Take Back Control of Your Data

Серия «Цифровой социум»

КАРИССА ВЕЛИЗ

СИЛА КОНФИДЕНЦИАЛЬНОСТИ

Почему необходимо обладать контролем над своими персональными данными и как его установить

Перевод с английского Елизаветы Павловой

Ростов-на-Дону
ФЕНИКС
2023

УДК 004.05
ББК 32.973-018.2
КТК 216
В27

Опубликовано по договоренности с Peters Fraser и Dunlope Group Ltd и агентством The Van Lear Agency LLC

Велиз, Карисса.

В27 Сила конфиденциальности : почему необходимо обладать контролем над своими персональными данными и как его установить / Карисса Велиз ; пер. с англ. Е. Павловой. — Ростов н/Д : Феникс, 2023. — 238, [1] с. — (Цифровой социум).

ISBN 978-5-222-36627-1

По мере того как сбор личных данных набирает обороты, а их использование — силу, автор Карисса Велиз показывает, как крупные компании и правительства нарушают нашу конфиденциальность, границы личных данных, почему это важно и что мы можем и должны с этим сделать.

Когда вы выключаете будильник на телефоне ранним утром, целый ряд организаций и компаний сразу же узнает, когда вы просыпаетесь, где вы спали и кто находится рядом. Проверяя погоду, прокручивая ленту социальных сетей, просматривая «рекомендации» друзей — каждым из этих действий вы ставите под угрозу конфиденциальность своих личных данных.

УДК 004.05
ББК 32.973-018.2

ISBN 978-5-222-36627-1

Privacy is Power
Carissa Véliz

Оглавление

A mi madre, tierra firme que me dio alas.
Моей матери — земле, которая даровала мне крылья.

Введение

Они наблюдают за нами. Они знают, что я сейчас пишу эти строки. Они увидят, как вы их будете читать. Государственные органы и сотни корпораций следят за вами, и мной, и всеми, кого мы знаем. Каждый день, каждую минуту. Они отслеживают и записывают все, что могут: наше местоположение, наше общение, наши поисковые запросы в интернете, наши биометрические данные, наши социальные контакты, наши покупки и многое другое. Они хотят знать, кто мы, о чем мы думаем, в чем мы уязвимы. Они хотят предсказывать наше поведение и влиять на него. У них слишком много власти. Источник этой власти коренится в нас, в вас, в ваших персональных данных. Пора вернуть себе контроль. А вернуть контроль над жизнью своей и общества можно лишь через восстановление конфиденциальности.

Интернет в основном финансируется за счет сбора, анализа и торговли данными. Это своего рода экономика данных. Бóльшая часть этих данных носит персональный характер, то есть содержит информацию, которая касается лично вас. Торговля персональными данными как бизнес-модель все больше внедряется во всех институтах общества, превращая его в общество слежки, или капитализм слежки[1].

Уж простите, но, чтобы связаться с вами, мне пришлось прибегнуть к капитализму слежки. Как вы узнали об этой книге? Вы можете вспомнить, при каких обстоятельствах впервые услышали о ней или где увидели рекламу? Вы могли быть отмечены той или иной платформой как «интересующийся», то есть тот, кто ищет знания и новый опыт. А это означает, что вам, скорее всего, нравятся книги, которые заставляют задуматься. Или вы могли бы быть отмечены как «активист» — тот, кого волнуют социальные проблемы, кто увлекается политикой. Похоже на вас? Основная цель этой книги — расширить

ваши возможности, но большинство подобных способов использования ваших данных направлено на то, чтобы лишить вас возможностей.

Если вы никак не засветились перед покупкой этой книги, то это, вероятно, лишь вопрос времени. Если вы читаете ее на *Kindle*, *Google Books* или *Nook*, они уже засекают, как долго вы читаете каждое слово, где вы останавливаетесь, чтобы сделать перерыв, и какие места вы отмечаете. Если вы купили эту книгу в книжном магазине, смартфон в вашем кармане фиксировал весь ваш путь туда и то, сколько времени вы там провели. Музыка в книжном магазине могла посылать ультразвуковые импульсы на ваш телефон, чтобы идентифицировать его как принадлежащий вам и отслеживать ваши интересы и покупки. Если вы использовали дебетовую или кредитную карту, чтобы купить книгу, то, вероятно, эта информация продана брокерам данных, которые затем перепродали ее страховым компаниям, потенциальным работодателям, правительству, предпринимателям и всем остальным, кто может быть в ней заинтересован. Или вы даже могли привязать свою платежную карту к системе лояльности, которая отслеживает вашу историю покупок и использует эту информацию, чтобы попытаться продать вам больше товаров, которые, следуя заданному алгоритму, вы можете захотеть купить.

Экономика данных и повсеместная слежка, которая ее подпитывает, застали нас врасплох. Технологические компании не информировали пользователей о том, как они используют их данные, не говоря уже о том, чтобы запросить их разрешение.

Они не спрашивали и у правительства. Не было принято никаких законов, регулирующих использование цифровых следов, которые оставляют ничего не подозревающие граждане, занимающиеся своими делами во все более оцифрованном мире. А когда мы поняли, что происходит, система слежки уже была выстроена. Бóльшая часть нашей конфиденциальности была потеряна. Однако еще не поздно вернуть себе контроль. С приходом пандемии коронавируса конфиденциальность столкнулась с новыми угрозами, поскольку реальная жизнь переместилась в интернет и нас попросили отказаться от наших

личных данных во имя общественного блага. Настало время хорошенько задуматься о том, в каком мире мы хотим жить, когда пандемия сойдет на нет. Мир без обеспечения конфиденциальности опасен.

Конфиденциальность — это возможность хранить определенную личную информацию (ваши мысли, опыт, разговоры, планы) исключительно в своем ведении. Людям нужна конфиденциальность, чтобы иметь возможность отдохнуть от бремени общения с другими. Нам нужна конфиденциальность, чтобы свободно осваивать новые идеи и формировать собственное мнение. Конфиденциальность защищает нас от нежелательного давления и злоупотребления властью. Она необходима нам, чтобы оставаться самостоятельными личностями; для правильной работы демократических институтов нужно, чтобы граждане сохранили самостоятельность. Наша жизнь, переведенная в данные, является «сырьем» для экономики слежки. Все, на что мы надеемся, чего боимся, о чем читаем и что пишем, наши отношения, наши болезни, наши ошибки, наши покупки, наши слабости, наши лица, наши голоса — все идет на «корм» информационным стервятникам, которые собирают, анализируют и продают эти данные тому, кто предложит самую высокую цену. Среди людей, собирающих наши персональные данные, слишком много тех, кто делает это в неблаговидных целях: чтобы выдать наши секреты страховым компаниям, работодателям и правительству, продать какие-то вещи, которые нам не нужны, натравить нас друг на друга в попытке разрушить общество изнутри, дезинформировать нас и подорвать наши демократии. Экономика слежки превратила граждан в пользователей и субъектов данных. Но всему есть предел! Те, кто нарушил наше право на конфиденциальность, злоупотребили нашим доверием, и пришло время отключить их от источника власти — наших данных.

Уже поздно препятствовать развитию экономики данных, но мы еще можем вернуть себе конфиденциальность. На карту поставлены наши гражданские свободы. Выбор общества в отношении конфиденциальности повлияет на то, как будут проводиться политические кампании и зарабатывать корпорации, повлияет на власть, которой

могут обладать правительства и частный бизнес, на развитие медицины, на достижение целей общественного здравоохранения, на риски, которым мы подвергаемся, и, что не менее важно, на соблюдение наших прав в повседневной жизни.

Эта книга — о состоянии дел с конфиденциальностью сегодня, о том, как возникла экономика слежки и почему мы должны прекратить торговлю персональными данными, о том, как мы можем это сделать. В первой главе будет показано, как сильно в рамках экономики данных ограничивается конфиденциальность личности в течение одного только дня. Во второй главе речь пойдет о том, как развивалась экономика данных, чтобы мы могли понять, как оказались в такой ситуации и как можно из нее выбраться. В третьей главе мы поговорим о том, что конфиденциальность — это форма власти, и тот, кто обладает наибольшим количеством персональных данных, будет властвовать над обществом. Если мы передадим наши персональные данные коммерческим структурам, у власти будут богачи. Если мы передадим наши данные правительствам, мы получим одну из форм авторитаризма. И только если люди сохранят свои данные при себе, общество будет свободным. Конфиденциальность имеет значение, потому что она дает гражданскому обществу силу.

Капитализм слежки неприемлем не только потому, что она создает и усиливает нежелательную асимметрию власти, но и потому, что она торгует токсичным веществом.

В четвертой главе я расскажу о том, почему персональные данные токсичны и отравляют нашу жизнь, наши институты и общество. Нам нужно положить конец экономике данных, как мы положили конец рабовладению. Экономические системы, опирающиеся на нарушение прав человека, недопустимы. В пятой главе мы поговорим о том, как общество может выключить экономику слежки. В шестой главе речь пойдет о том, что лично вы можете сделать, чтобы вернуть контроль над своими персональными данными и вашими демократическими институтами.

Мы не являемся свидетелями гибели конфиденциальности. Это только начало борьбы за защиту персональных данных в эпоху цифровых технологий. Слишком многое поставлено на карту, чтобы позволить конфиденциальности исчезнуть. Под угрозой находится не только она, но и сам наш образ жизни. Слежка угрожает свободе, равенству, демократии, автономии, творчеству и интимной жизни. Нам снова и снова лгут, и наши данные крадут, чтобы использовать против нас. Хватит. С капитализмом слежки пора заканчивать. На это потребуются некоторое время и усилия, но мы можем вернуть и вернем себе конфиденциальность. В этой книге написано, как это сделать.

Глава 1

СТЕРВЯТНИКИ ДАННЫХ

Если вы читаете эту книгу, то, вероятно, уже знаете, что ваши персональные данные собираются, хранятся и анализируются. А представляете ли вы масштабы проникновения в вашу частную жизнь? Давайте рассмотрим ваш день с самого начала.

Что вы делаете в первую очередь, просыпаясь утром? Наверное, проверяете свой телефон. Вуаля — это первые данные, которые вы теряете за день. Взяв телефон в руки, вы информируете целую кучу назойливых людей — производителя вашего смартфона, владельцев всех приложений, которые вы установили на свой телефон, вашего мобильного оператора, а также разведывательные службы, если вы оказались объектом интереса, — о том, во сколько вы просыпаетесь, где вы спали и с кем (если человек, с которым вы делите постель, тоже держит рядом с собой телефон).

Если вы постоянно носите умные часы, то вы потеряете какую-то личную информацию даже до того, как проснетесь, поскольку часы фиксируют каждое ваше движение в постели — включая, конечно же, любую сексуальную активность.

Предположим, что ваш работодатель предоставил вам эти часы в рамках оздоровительной программы для сотрудников по сокращению затрат на медицинскую страховку. Можете ли вы быть уверены, что ваши данные не будут использоваться против вас? Вы уверены, что ваш работодатель не увидит их?[1] Когда работодатель передает вам устройство, он остается его законным владельцем — будь то фитнес-браслет, ноутбук или телефон — и может получить доступ к данным с этого устройства в любое время без вашего разрешения[2].

После того как вы проверите, каким был ваш пульс в ночное время (слишком частый — вам нужно больше тренироваться), и отправите эти данные на ваш смартфон, вы встанете с постели и отправитесь

чистить зубы электрической зубной щеткой. Специальное приложение оповестит вас о том, что вы чистите зубы реже, чем нужно.

Вы проспали сегодня утром, и ваша супруга уже уехала на работу. Вы идете на кухню и ищете сахар для кофе, но понимаете, что он закончился. Вы решили спросить свою соседку, не одолжит ли она вам немного сахара. Стоя перед ее дверью, вы замечаете, что это не совсем обычная дверь — в нее вмонтирована видеокамера. Когда соседка открывает дверь, она поясняет, что это новый умный дверной звонок. Если это дверной звонок от *Ring* — компании, принадлежащей *Amazon*, — то сотрудники *Ring*, вероятно, посмотрят эту видеозапись, чтобы пометить объекты вручную с целью научить программное обеспечение выполнять задачи распознавания. Эти видео хранятся в незашифрованном виде, что делает их чрезвычайно уязвимыми для взлома[3]. *Amazon* получила патент на использование программного обеспечения для распознавания лиц в дверных замках. Компания *Nest*, принадлежащая *Google*, уже использует распознавание лиц в своих камерах. В некоторых городах, таких как Вашингтон, округ Колумбия, полиция хочет регистрировать и даже субсидировать частные камеры видеонаблюдения[4]. Бог знает, где хранятся видеоматериалы с умных дверных звонков и для чего они будут использоваться.

У вашей соседки нет сахара — а может, она не хочет вам его давать после того, как вы насмехались над ее новым дверным звонком. Вы вынуждены довольствоваться несладким кофе. Вы включаете телевизор (конечно же, смарт-телевизор), чтобы отвлечься от его горечи. По телевизору идет ваше любимое шоу — постыдное увлечение, в котором вы никому не признаетесь.

Вам звонят. Это ваша жена. Вы выключаете звук телевизора.

— Почему ты все еще дома?

— Откуда ты знаешь?

— Мой телефон подключен к нашему интеллектуальному счетчику. И я могу видеть, когда используется электричество.

— Я проспал, — говорите вы.

Ее не очень убедило ваше объяснение, но ей уже надо бежать.

Вы задаетесь вопросом, впервые ли за вами шпионят через ваш умный счетчик. Умные счетчики — это не только угроза конфиденциальности в отношении людей, с которыми вы живете в одном доме. Они являются заведомо небезопасными устройствами[5]. Преступник может взломать устройство, узнать, когда вы находитесь вдали от дома, и ограбить ваше жилище[6]. Кроме того, данные с интеллектуальных счетчиков хранятся и анализируется поставщиками энергоуслуг. Некоторые из этих данных могут быть весьма конфиденциальными. Например, сведения о вашем энергопотреблении могут оказаться настолько точными, что по ним без труда можно определить, какой телевизионный канал вы смотрите[7]. Эти данные можно продать или поделиться ими с заинтересованными третьими лицами.

Ваш сын-подросток внезапно входит и прерывает ваши мысли. Он хочет о чем-то поговорить с вами. О чем-то весьма щепетильном. Возможно, это проблема, связанная с наркотиками, сексом или издевательствами в школе. Вы не выключаете телевизор. Он работает без звука, в фоновом режиме. Ваш смарт-телевизор, вероятно, собирает информацию с помощью технологии, называемой «автоматическое распознавание контента» (*ACR*). Он пытается идентифицировать все, что вы смотрите по телевизору, и отправляет данные производителю, третьим лицам или и тем и другим. Это как минимум. Некоторые телевизоры могут подслушивать ваши разговоры и передавать их третьим лицам. Исследователи обнаружили, что один смарт-телевизор *Samsung* подключался к более чем 700 различным интернет-адресам за 15 минут[8]. Даже если вы думаете, что выключили телевизор, он может быть еще включен. Спецслужбы, такие как ЦРУ и МИ-5, могут сделать так, чтобы ваш телевизор выглядел так, будто он выключен, в то время как вас записывают[9].

Если у вас было время ознакомиться с политикой конфиденциальности электронных устройств, которые вы покупаете, то вы заметили, что паспорт вашего телевизора *Samsung* содержит следующее предупреждение: «Имейте в виду, что, если вы произносите слова, которые

включают личную или другую конфиденциальную информацию, эта информация может быть передана третьим лицам»[10].

После того как ваш сын поделится своими самыми сокровенными мыслями с вами, производителем вашего телевизора и сотнями неизвестных третьих лиц, он уйдет в школу, где его конфиденциальность еще больше пострадает благодаря наблюдению школы за тем, как он использует интернет[11]. А вы включаете звук телевизора. Идет реклама. Вы думаете, что наконец-то сможете уединиться. Но вы ошибаетесь. Без вашего ведома неслышимые звуковые маячки передаются через рекламу на телевидении и радио (а также через музыку в магазинах) и улавливаются вашим телефоном. Эти звуковые сигналы работают как файлы *cookie*, позволяя различным организациям определять местоположение ваших гаджетов и покупательское поведение в зависимости от места, где вы находитесь. То есть они помогают организациям отслеживать вас на разных устройствах. Благодаря этому ультразвуковому обмену информацией между устройствами компания может убедиться, что человек, который видит определенную рекламу продукта утром по телевизору, через час увидит ее на своем ноутбуке, а затем купит этот продукт в магазине по соседству или закажет в интернете[12].

Вам поступает еще один звонок. На этот раз коллега:

— Эй, не знаю, как это произошло, но я только что получил запись очень личного разговора, который был у тебя с твоим сыном. Похоже, его прислала ваша цифровая помощница Алекса.

Вы благодарите его за то, что дал вам знать, и вешаете трубку, задаваясь вопросом, могла ли Алекса отправить этот разговор другим людям в вашем списке контактов. В ярости вы связываетесь с *Amazon*. Они объясняют: «Наверное, какое-то слово в разговоре по звучанию напомнило слово “Алекса”. Затем программа подумала, что вы говорите “отправить сообщение”. Должно быть, программа спросила: “Кому?” — и какое-то высказывание интерпретировалось как имя»[13]. Иногда умные помощники активируются, когда идет телешоу, в котором произносят слово, похожее на слово их запуска. Если бы у вас

был включен телевизор в течение всего дня, это могло бы произойти до девятнадцати раз в день (не считая времени, когда реальное слово для запуска помощника произносится по телевидению)[14]. Когда Алекса отправила личный разговор пользователя из Портленда, штат Орегон, случайному контакту, пользователь поклялся никогда больше не включать устройство[15]. Вы идете еще дальше и разбиваете его об стену. Ваша жена вас за это не похвалит.

Вы уже сильно опаздываете на работу. Вы садитесь в машину и едете в свой офис. Вы купили подержанный автомобиль у знакомого. Вероятно, это никогда не приходило вам в голову, но оказывается, что у этого человека есть доступ к вашим данным, потому что он никогда не отключал свой телефон от автомобильного приложения[16]. Кроме того, ваш автопроизводитель собирает всевозможные данные о вас: о местах, которые вы посещаете, о скорости, с которой вы ездите, о музыкальных вкусах, движениях глаз, о том, находятся ли ваши руки на руле, и даже о том, какой у вас вес, — это легко измеряется вашим сиденьем. Вся эта информация среди прочего может оказаться в руках и у вашей страховой компании[17].

Вы добираетесь на работу. Вы живете в Лондоне, а ваш офис находится прямо рядом с Вестминстером. Когда вы проезжаете мимо здания парламента, данные с вашего телефона могут быть перехвачены *IMSI*-ловушками — поддельными вышками сотовой связи, которые заставляют мобильные телефоны подключаться к ним. С момента подключения *IMSI*-ловушки собирают ваши идентификационные данные и сведения о вашем местоположении. Они также позволяют прослушивать телефонные разговоры, считывать текстовые сообщения и отслеживать просмотр веб-страниц[18]. Имеются доказательства того, что это оборудование используется полицией в Лондоне для слежки за людьми, например, во время мирных акций протеста и возле парламента Великобритании[19]. Самый популярный совет в интернете для тех, кто идет на акцию протеста: для защиты вашей конфиденциальности оставляйте телефон дома. Хотя *IMSI*-ловушки чаще всего используются правительством, они могут быть задейство-

ваны кем угодно, так как продаются частными компаниями, а также могут быть самодельными.

Пока с вашего телефона считываются данные, вы входите в свой офис. Коллега приветствует вас и смотрит на часы, давая понять, что он заметил ваше опоздание. Вы садитесь перед своим компьютером и пытаетесь сделать глубокий вдох, но у вас перехватывает дыхание при виде сотен непрочитанных писем[20]. Вы открываете первое. Оно от вашего босса: «Эй, я заметил, что тебя сегодня утром не было в офисе. Вовремя ли будет готов тот отчет, который я просил тебя сделать?» Да, вы планируете сдать отчет вовремя, но вам бы хотелось, чтобы ваш босс не дышал вам в затылок.

В следующем письме вас просят анонимно оценить работу ваших коллег. Босс твердо верит в пользу слежки на работе. Вы знаете, что он контролирует каждое ваше движение, следя за тем, посещаете ли вы собрания, семинары и даже неформальные ужины и посиделки в баре после работы. Вы знаете, что он следит за вашими страницами в социальных сетях, потому что ранее он высказал недовольство по поводу размещения вами политического контента. Вас тошнит при одной мысли о необходимости оценивать своих коллег и быть оцененным ими.

Еще одно письмо — от вашего любимого обувного бренда. Вы можете считать получение электронных писем безвредным для вашей конфиденциальности, но около 70% коммерческих писем и 40% всех электронных писем содержат трекеры[21]. Открытие электронного письма позволяет третьим лицам отслеживать вас в Сети и идентифицировать как одного и того же пользователя на разных устройствах. Трекеры могут быть встроены в цвет, шрифт, пиксель или ссылку. Даже обычные люди используют трекеры, чтобы знать, читаются ли их электронные письма, когда и где. Учитывая, что трекеры способны определить местонахождение человека, стервятники данных могут использовать их, чтобы найти вас.

Следующее письмо — от вашего брата. Он написал вам на рабочую почту, хотя вы просили его не делать этого. Работодатели, включая

университетское сообщество, имеют доступ к вашей электронной почте[22], и это одна из причин, по которой лучше никогда не использовать свою рабочую электронную почту в личных целях. В своем письме ваш брат сообщает, что получил набор для генетического тестирования потребителя в качестве подарка на день рождения и испробовал его на себе. Вам будет приятно узнать, пишет он, что ваша семья на 25 процентов итальянская. Плохая новость состоит в том, что у него имеется 30-процентный риск приобрести кардиологическое заболевание, а учитывая, что он ваш брат, это, вероятно, относится и к вам. Вы отвечаете ему: «Мне бы хотелось, чтобы ты сначала поинтересовался, не против ли я. Это и мои гены, и гены моего ребенка тоже. Разве ты не знал, что наша бабушка — итальянка? Если ты хочешь узнать больше о нашей семье, лучше спроси меня». В тревоге за свои генетические особенности вы смотрите политику конфиденциальности компании, которую использовал ваш брат. И вам она не очень нравится. Компания-разработчик теста может претендовать на право собственности на отправленный вами образец ДНК и использовать его по своему усмотрению[23]. Политика конфиденциальности компаний, занимающихся тестированием ДНК, обычно ссылается на «деидентификацию» или «псевдонимизацию» информации, чтобы успокоить людей. Однако генетические данные не так-то просто эффективно деидентифицировать. В самой природе генетических данных заложено то, что они могут однозначно идентифицировать людей и их семейные связи. Замена имен случайно сгенерированным идентификатором номера не спасает от повторной идентификации. В 2000 году компьютерные ученые Брэдли Малин и Латания Суини использовали общедоступные медицинские данные и информацию о конкретных заболеваниях, чтобы повторно идентифицировать 98–100% людей в анонимизированной базе данных ДНК[24].

Вы задаетесь вопросом, что станет с генетическими данными вашего брата и будут ли они когда-либо использоваться против вас или вашего сына, если вы, например, подадите заявление на страховку или будете искать работу. Хуже всего то, что домашние генетические

тесты невероятно неточны. Около 40% результатов являются ложноположительными[25]. Возможно, ваш брат целиком выдал генетическую тайну семьи в обмен на полную ерунду, которая тем не менее будет рассматриваться страховыми компаниями и другими лицами как факт.

Пришло время для рабочей видеоконференции с клиентом, который просил подключиться через *Zoom*. Многие люди не слышали о приложении *Zoom* до пандемии коронавируса, когда оно стало самым популярным приложением для видео-конференц-связи. У вас имеется плохой опыт, связанный с этим приложением, например, когда вы отправили приватный текстовый чат вашему коллеге, высмеивая то, как был одет клиент, а затем осознали, что ваш клиент получил все тексты в расшифровке стенограммы в конце вызова. Теперь вы избегаете чата. Во время пандемии вы также с ужасом узнали, что каждое слово, сказанное во время вашего звонка, и каждый опубликованный документ стали частью данных, которые собирает *Zoom*[26]. У вас есть смутное представление о том, что *Zoom* улучшила свою конфиденциальность и политику безопасности сейчас, но можете ли вы доверять компании, которая утверждала, что внедрила сквозное шифрование, но не сделала этого[27]?

По окончании разговора, чтобы расслабиться, вы заходите в *Facebook*[*]. «Совсем ненадолго», — говорите вы себе. Возможно, фотографии приятных моментов с вашими друзьями поднимут вам настроение (что вряд ли). Поскольку вы подозреваете, что ваш начальник следит за тем, что вы делаете на вашем компьютере, вы используете свой личный телефон. *Facebook* уже столько раз нарушала наше право на неприкосновенность частной жизни, что исчерпывающий отчет заслуживает отдельной книги. Здесь я упоминаю только несколько способов вторжения в нашу частную жизнь.

Все, что вы делаете в *Facebook*, отслеживается — от движения вашей мыши[28] до того, что вы пишете и решаете удалить перед публикацией (ваша самоцензура)[29].

[*] Деятельность данной соцсети запрещена на территории Российской Федерации.

Вы начинаете просматривать раздел под названием «Люди, которых вы можете знать». Эта функция имела решающее значение в расширении социальной сети *Facebook*, которая «разрослась» со 100 миллионов участников, когда приложение вышло в 2008 году, до более 2 миллиардов в 2018 году. Среди тех, кого вы можете там увидеть, вы узнаете дальних родственников или людей, с которыми ходили в школу. Звучит не так уж и плохо. Я предлагаю вам не слишком углубляться в список возможных контактов. Если вы это сделаете, то, вероятно, обнаружите, что *Facebook* пытается связать вас с людьми, с которыми вы не хотите общаться.

Некоторые контакты между людьми чреваты проблемами — например, когда подлинные персональные данные работающих в секс-индустрии раскрываются их клиентам[30]. Или когда программа соединяет пациентов психиатра, не придавая никакого значения конфиденциальности. Указанный психиатр не дружил со своими пациентами в *Facebook*, но пациенты, вероятно, внесли его в свои списки контактов[31]. Среди прочих злополучных связей *Facebook* также предлагает добавить в друзья насильника — жертве (ранее сохранявшей анонимность), любовнику женщины — ее мужа, а человеку, пострадавшему от грабителя, — того самого грабителя[32]. Текущая миссия *Facebook* — «дать людям возможность для построения сообщества и собрать мир воедино». А как насчет того, чтобы дать людям возможность *отключиться* от токсичных или нежелательных отношений? «Собрать мир воедино» — звучит благородно, пока вы не спросите себя, хотите ли вы близости с навязываемыми вам людьми, которых вы боитесь, не любите или предпочитаете держать на расстоянии по профессиональным или личным причинам.

Facebook доказала отсутствие уважения к конфиденциальности в различном отношении и во многих случаях. Компания *Cambridge Analytica* проанализировала данные около 87 миллионов пользователей *Facebook* в политических целях. В 2018 году в результате взлома были украдены личные данные с 14 миллионов учетных записей[33].

В течение многих лет *Facebook* позволяла поисковой системе *Microsoft Bing* видеть друзей своих пользователей без их согласия, и это дало *Netflix* и *Spotify* возможность читать и даже удалять личные сообщения пользователей *Facebook*[34]. В 2015 году приложение начало регистрировать все текстовые сообщения и звонки от пользователей *Android* без их согласия[35].

Facebook использовала распознавание лиц на ваших фотографиях, не получив от вас должного согласия. Когда при процедуре тэгирования вас спросили, предложив фотографию, «Это Джек?» и вы ответили «да», вы бесплатно помогли *Facebook* улучшить алгоритм распознавания лиц. *Facebook* подала заявку на патенты на системы для распознавания лиц покупателей в магазинах и соотнесения их с их же профилями в социальных сетях[36]. В довершение всего *Facebook* попросила пользователей указать их телефонные номера в качестве меры безопасности, а затем использовала эту информацию в собственных целях — для таргетинга рекламы и унификации данных со своим приложением для обмена сообщениями в *WhatsApp*[37]. В 2019 году телефонные номера миллионов пользователей *Facebook* были раскрыты и попали в онлайн-базу данных, потому что сервер, на котором они были размещены, не был защищен паролем[38]. Это лишь некоторые из событий, но полный список куда более длинный, и все, видимо, указывает на то, что нарушения нашего права на неприкосновенность частной жизни со стороны *Facebook* вряд ли прекратятся[39].

Facebook может показаться на первый взгляд простой социальной сетью, но на самом деле ее бизнес — это «торговля» влиянием через персональные данные. Это скорее платформа для персонализированной рекламы, чем социальная сеть. *Facebook* готова на многое, чтобы выудить как можно больше личных данных с минимальными затруднениями, чтобы можно было продать рекламодателям доступ к вашему вниманию. Исходя из прежнего опыта, если все это будет сходить *Facebook* с рук — а пока благополучно сходит, — она не просто перестанет спрашивать согласие на обработку персональных данных,

но даже не будет пытаться выяснить, кто получает ваши данные и как они используются, и все обещания о конфиденциальности будут нарушены. Защита неприкосновенности вашей частной жизни кажется самым низким приоритетом в списке *Facebook*. И вы даже не можете оставаться в стороне от этого жаждущего данных монстра, потому что у *Facebook* есть теневой профиль на вас, даже если вы и не являетесь его пользователем. Он следует за вами по Сети с помощью постоянных кнопок «Нравится» в *Facebook*, даже если вы их не нажимаете[40]. Неудивительно, что в докладе британского парламента было объявлено, что *Facebook* ведет себя как «цифровой гангстер» последние несколько лет[41].

После просмотра *Facebook* в течение некоторого времени и ощущения «жути» от друзей, которых он предлагает, и от рекламы, которую он вам показывает, вы решили закрыть его. Вы пытаетесь взяться за работу, но не можете сконцентрироваться, размышляя о том, как ваш босс, вероятно, контролирует каждое действие, которое вы выполняете на своем компьютере. К счастью для вас, наступает время обеда. Вот только вы не голодны, поэтому решаете пойти в ближайший магазин и купить своему сыну что-нибудь, что поможет ему почувствовать себя лучше.

Вы заходите в магазин одежды, чтобы найти рубашку. Традиционные офлайновые магазины уступают в выборе интернет-магазинам, потому что последние зачастую знают больше о клиентах. Так что реальные магазины теперь пытаются наверстать упущенное. Магазин, в который вы вошли, использует технологию, которая идентифицирует вас как вернувшегося покупателя через ваш мобильный сигнал *Wi-Fi*. Мобильные устройства отправляют уникальные идентификационные коды (или *MAC*-адреса), когда ищут сети для выхода в интернет. Магазины используют эту информацию для изучения вашего поведения[42]. Не довольствуясь только этим, они могут также использовать камеры для сбора данных о вас. Камеры способны помочь обозначить маршруты движения клиентов и изучить, что привлекает людей, как они ориентируются в магазине. Камеры стали настолько совершенными, что могут анализировать, на что вы смотрите и даже в каком

вы настроении, в зависимости от языка вашего тела и выражения вашего лица[43]. Магазин может также использовать распознавание лиц. Помимо прочего, распознавание лиц позволяет сверить ваше лицо с базой данных магазинных воров или известных преступников[44].

Вы выходите из магазина и проверяете свой телефон. Вам приходит напоминание о том, что вы записались на прием к врачу. У вас есть проблема со здоровьем, которая беспокоит уже несколько недель. Вы искали решение в интернете и надеялись, что проблема исчезнет сама собой, но этого не произошло. Вы никому не сказали об этом в своей семье, чтобы не вызывать ненужное беспокойство. Наши поисковые системы знают о нас больше, чем наши супруги: мы никогда не лжем им и не скрываем от них свои заботы.

Вы идете к врачу. Пока вы ждете приема, вам приходит уведомление: ваша сестра опубликовала новую фотографию вашей маленькой племянницы. Ее пухлые ручки вызывают улыбку. Вы думаете о том, что нужно предупредить сестру об опасности размещения фотографий детей в интернете. Вы решаете сказать ей, что наши онлайн-фотографии задействуются для создания алгоритмов распознавания лиц, которые затем используются во всевозможных гнусных целях — от слежки за уязвимыми группами населения авторитарными режимами до разоблачения порноактеров и идентификации незнакомцев в метро в России[45]. Но вас отвлекает неотразимая улыбка племянницы. Ее фотографии иногда становятся главным событием вашего дня и тем, что дает силы терпеть экономику слежки, даже если вы знаете, что привлекательный контент, такой как милые младенцы, — это именно то, чем питаются стервятники данных. Тем временем медсестра оповещает, что врач готов вас принять. Доктор задает деликатные вопросы, записывает ваши ответы на свой компьютер и назначает вам несколько анализов. Вам интересно, куда могут попасть эти данные, ведь медицинская информация часто продается. Продавцы данных[46] — торговцы персональными данными — могут получать медицинские сведения из аптек, больниц, кабинетов врачей, приложений для здоровья и поисковых запросов в интернете. Ваши медицинские данные могут также попадать в руки аналитиков, страховых компаний или

потенциальных работодателей[47]. Или *NHS* (Национальная служба здравоохранения Великобритании) может решить пожертвовать ваши записи такой компании, как *DeepMind*, принадлежащей *Alphabet* (материнской компании *Google*). Передача данных может производиться без вашего согласия, без выгоды для вас от такого вторжения в частную жизнь и без каких-либо юридических гарантий, что *DeepMind* не свяжет ваши данные с вашей учетной записью *Google*, тем самым еще больше нарушая вашу конфиденциальность[48].

Вы также можете стать жертвой утечки данных. В 2015 году в США были взломаны более 112 миллионов медицинских записей[52]. Вы даже можете стать жертвой вымогательства. В 2017 году преступники получили доступ к медицинским записям из клиники и шантажировали пациентов; в итоге они опубликовали более 25 000 фотографий людей, в том числе обнаженных, и личные данные, включая сканы паспортов и номера страховых полисов[50].

Когда все эти мысли проносятся в вашей голове, вы испытываете искушение лгать своему врачу, скрывая конфиденциальную информацию, которая (вы надеетесь) не обязательно нужна, чтобы поставить точный диагноз. Вы даже можете почувствовать желание вообще не сдавать назначенные анализы, даже если они вам необходимы.

После посещения врача вы возвращаетесь домой, чтобы собрать вещи в рабочую поездку в США. Весь день за вами следили приложения на вашем телефоне. Если вы разрешаете приложениям определять ваше местоположение, чтобы вы могли получать местные новости, прогноз погоды или другую подобную информацию, десятки компаний получат сведения о том, где вы находитесь. В некоторых случаях приложения обновляют и получают данные о вашем местоположении более 14 000 раз в день. Реклама с геотаргетингом — это бизнес, стоимость которого оценивается в 21 миллиард долларов[51].

Среди множества компаний, торгующих данными о вашем местоположении, особое место занимают телекоммуникации. Завидуя успеху Кремниевой долины, телекоммуникационные компании стремятся конкурировать на рынке торговли данными[52]. Ваш мобильный телефон постоянно подключается к ближайшей сотовой вышке. В результате

16+

Популярное издание

Карисса Велиз

СИЛА КОНФИДЕНЦИАЛЬНОСТИ

Почему необходимо обладать контролем над своими персональными данными и как его установить

Ответственный редактор *Ирина Ремеева*
Выпускающий редактор *Галина Логвинова*
Технический редактор *Татьяна Ткачук*
Переводчик *Елизавета Павлова*

Формат 70×90/16. Бумага офсетная.
Тираж 3000 экз. Заказ

Издатель и изготовитель: ООО «Феникс».
Юр. и факт. адрес: 344011, Россия, Ростовская обл.,
г. Ростов-на-Дону, ул. Варфоломеева, д. 150
Тел/факс: (863) 261-89-65, 261-89-50

Изготовлено в России. Дата изготовления: 03.2023. Срок годности не ограничен.
Отпечатано в АО «ТАТМЕДИА»
Филиал «Полиграфическо-издательский комплекс "Идел-Пресс"».
Юр. адрес: 420097, Россия, Республика Татарстан, г. Казань, ул. Академическая, д. 2
Факт. адрес: 420066, Россия, Республика Татарстан, г. Казань, ул. Декабристов, здание 2