ДЖОН ФАСМАН

ОБЩЕСТВО КОНТРОЛЯ

КАК СОХРАНИТЬ КОНФИДЕНЦИАЛЬНОСТЬ В ЭПОХУ ТОТАЛЬНОЙ СЛЕЖКИ

ИДЕАЛЬНАЯ АРХИТЕКТУРА КОНТРОЛЯ

ПОЛИЦЕЙСКИЙ НАДЗОР И ОБЩЕСТВЕННАЯ БЕЗОПАСНОСТЬ

НАРУШЕНИЯ ПРАВ НА ЧАСТНУЮ ЖИЗНЬ

БОМБОРА
ИЗДАТЕЛЬСТВО

Джон Фасман

Общество контроля. Как сохранить конфиденциальность в эпоху тотальной слежки

Серия «КиберБез. Лучшие книги о безопасности в сети»

http://www.litres.ru/pages/biblio_book/?art=69622183
ISBN 978-5-04-192173-6

Аннотация

«Общество контроля» – масштабное исследование Джона Фасмана, вашингтонского корреспондента журнала The Economist. Оно посвящено правовым, политическим и моральным проблемам, неизбежно возникающим в обществе, где каждый из нас постоянно находится под наблюдением. Технологии распознавания лиц, автоматические считыватели автомобильных номеров, летающие дроны, алгоритмы прогнозирования поведения – все это попадает в фокус внимания автора, заставляя его задуматься о том, кому может быть выгодно

массовое использование технологий слежки и как оно влияет на нашу жизнь.

В формате PDF A4 сохранён издательский дизайн.

Содержание

Пролог 7
1. Технология и демократия 18
Конец ознакомительного фрагмента. 53

Джон Фасман
Общество контроля. Как сохранить конфиденциальность в эпоху тотальной слежки

WE SEE IT ALL:
Liberty and Justice in an Age of Perpetual Surveillance
Jon Fasman

*** * ***

ПАМЯТИ ДЖОРДЖА ЭТУЭЛЛА КРИМСКИ И СИДНИ МЕТЦГЕР

Как война с наркотиками способствовала милитаризации полиции, так теперь война с терроризмом форсирует сбор полицейской разведывательной информации, и личная жизнь

миллионов американцев находится под угрозой.
Адам Бейтс
Институт Катона

Пролог

Идеальная архитектура контроля

Иногда будущее раскрывает себя как настоящее.

10 февраля 2020 года я летел из Нью-Йорка в Лас-Вегас. Президентская кампания началась всерьез. Как корреспондент The Economist в Вашингтоне и соведущий нашего нового американского политического подкаста «Сдержки и противовесы», я почти каждую неделю ездил по стране и освещал предвыборную кампанию – с первых дней нового года и до тех пор, пока COVID-19 не захлопнул все на свете. Неделей раньше я был в Нью-Гемпшире, а еще до этого в Айове, и собирался провести три дня в Неваде, а затем пять в Южной Каролине, ненадолго заскочив перед этим домой, чтобы постирать одежду и убедиться, что жена и дети все еще узнают меня в лицо и не поменяли замки.

Внутренние и международные рейсы «Дельты» отправляются из одного и того же терминала в аэропорту Кеннеди. Почти у всех выходов на посадку висели плакаты с рекламой терминалов распознавания лиц от компании «Дельта» – вертикальные синие экраны с контуром лица, вписанного в четыре угла видоискателя цифровой камеры. Над картинкой

красовался лозунг: «Один взгляд – и ты в деле». Надпись на баннере чуть ниже гласила: «Теперь вы можете проходить на посадку с помощью Delta Biometrics, нового способа удобной навигации по аэропорту». А в самом низу, на уровне ног, мелким шрифтом: «Посадка с использованием технологии распознавания лиц не является обязательной. Пожалуйста, при возникновении любых вопросов или для прохождения альтернативных процедур обратитесь к сотруднику. Посетите delta.com, чтобы ознакомиться с нашей политикой конфиденциальности».

Месяцев за восемь до этого я летел в Кито и проходил на посадку через биометрический терминал «Дельты» в Атланте. Это была странная новинка: обычные камеры наблюдения не работали, и большинство пассажиров нашего рейса, включая меня, шли мимо камер распознавания лиц, а потом бортпроводник проверял наши билеты. Но система, видимо, работала достаточно хорошо – или скоро будет работать достаточно хорошо – для того, чтобы «Дельта» запустила ее агрессивную рекламу. Я замечал выходы на посадку с распознаванием лиц в Миннеаполисе и Детройте. В конце 2019 года «Дельта» объявила, что установит терминалы в Солт-Лейк-Сити. Около 93 % клиентов проходят процедуру без проблем, говорится в пресс-релизе «Дельты», а 72 % предпочитают ее стандартной посадке.

Признаки амбиций авиакомпании «Дельта» можно найти в нижнем тексте баннера, где упоминается не только посад-

ка, но и возможность *удобной навигации по аэропорту*. И действительно, в пресс-релизе компании рекламировалось *распознавание лица от порога до выхода на посадку*: вы можете использовать свое лицо, чтобы зарегистрироваться на рейс, сдать багаж, пройти контроль безопасности и сесть в самолет. Все очень удобно. Если вы прилетели из-за границы, у авиакомпаний уже есть ваша паспортная фотография – либо в их собственной базе данных, либо в базе Таможенно-пограничной службы.

Мое отношение к этой программе очень ясное: я отказываюсь от нее. Надеюсь, после прочтения этой книги вы поступите так же. Распознавание лиц ставит под угрозу наши гражданские свободы. Пользуясь им добровольно, вы превращаете его в нечто повседневное. Чем чаще вы сами выбираете эту систему, тем чаще она будет применяться такими способами и в таких местах, которых вы никогда бы не выбрали. Всякий раз, когда у вас есть шанс уклониться от ее прохождения, вы должны им пользоваться: необходимо сделать все возможное, чтобы замедлить распространение систем распознавания лиц.

После того как я разместил в интернете фотографию этого рекламного баннера, один мой друг заметил, что «Дельта» хотя бы предоставляет пассажирам выбор. Этот друг летел рейсом «Сингапурских авиалиний» в Токио, и его обязали пройти на борт через терминал распознавания лиц. Это было относительно ново: до июля 2017 года я работал в Синга-

пуре по заданию The Economist и по несколько раз в месяц летал этими авиалиниями. Тогда они не использовали систему распознавания лиц. Будущее – уже сегодня.

Приземлившись в Лас-Вегасе, я увидел сообщения от нескольких друзей. Они спрашивали, что я думаю о сегодняшнем выпуске The Daily, ежедневного новостного подкаста «Нью-Йорк таймс». По их совету я послушал подкаст, пока ехал с одной встречи на другую. Это была аудиоверсия ужасающей истории, которую за пару недель до этого раскрыла Кашмир Хилл[1]. Уже около десяти лет Хилл пишет о технологиях и защите данных. Она проницательный, вдумчивый и интересный писатель и потрясающий репортер – одна из немногих, чьи истории со временем становятся не только длиннее, но и лучше.

Этот конкретный материал касался небольшой компании под названием Clearview AI, которая разработала приложение для распознавания лиц. Пользователь делает снимок любого встречного и загружает в приложение, а система сообщает, кто изображен на фотографии. При этом используется база данных фирмы Clearview, содержащая более трех миллиардов изображений из общедоступных источников, в том числе с YouTube и других широко используемых ресурсов – в семь с лишним раз больше, чем в базе ФБР.

---

[1] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It", *New York Times*, January 18, 2020, www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Иными словами, если вы американец, вероятность, что вы находитесь в базе данных, доступной для ФБР, – один к двум. Если живете в стране первого мира, скорее всего, находитесь в Clearview. Любой, у кого есть приложение Clearview на телефоне, может за несколько секунд узнать, кто вы такой. Проделав несложный поиск, он выяснит гораздо больше: адрес, работодателя, имена друзей и членов семьи – в общем, получит любую информацию о вас, которая может находиться в интернете.

Пока я это пишу, приложением Clearview пользуются сотни правоохранительных органов, а также некоторые частные компании (Clearview отказался сообщить, какие именно), в том числе инвесторы этой фирмы и их друзья. Например, магнат продуктовой сети Джон Кациматидис случайно увидел свою дочь на свидании с неизвестным парнем[2]. Джон попросил официанта сфотографировать парня и затем прогнал фото через Clearview. Через несколько секунд приложение сообщило ему, с кем обедает его дочь, – незнакомец оказался венчурным капиталистом из Сан-Франциско. Кроме того, Кациматидис использовал эту систему в своих магазинах для выявления воров, которые крали мороженое. («Люди воровали наши Haagen-Dazs, – жаловался он. – Это была большая проблема».)

---

[2] Kashmir Hill, "Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich", *New York Times*, March 5, 2020, www.nytimes.com/2020/03/05/technology/clearview-investors.html.

Полицейским нравится система Clearview: по их словам, она помогает быстро идентифицировать подозреваемых. Но такое удобство не должно определять ценность или законность продукта. Есть много вещей – например, бессрочное содержание под стражей без предъявления обвинения или отмена habeas corpus, – несовместимых с таким свободным и открытым обществом, которое облегчило бы работу правоохранительных органов.

Хотя основными клиентами Clearview сегодня являются полицейские, ничто не мешает компании продавать это приложение всем, кто хочет его купить. И похоже, основатель фирмы, которая была одним из первых инвесторов Clearview, смирился с такой возможностью. Он сказал Кашмир Хилл: «Я пришел к выводу, что, поскольку информации становится все больше, конфиденциальности не будет никогда. Законы должны определять, что является допустимым, но запретить технологии невозможно. Конечно, они могут привести к мрачному будущему или чему-то подобному, но запретить их не получится». Предполагаю, если технологии, создающие мрачное будущее или что-то подобное для всех на свете, обогащают автора этого высказывания – пусть уж будет мрачное будущее.

Facebook[3] и другие социальные сети запрещают веб-скрейпинг своих изображений, но Clearview все равно этим занимается. Эрик Шмидт, бывший исполнительный дирек-

[3] Принадлежит Мете, которая признана экстремистской на территории РФ.

тор Google, в 2011 году сказал, что распознавание лиц было единственной технологией, созданной Google, и, посмотрев на нее, компания решила остановиться, потому что такие технологии могут использоваться *очень плохо*[4].

Основатель Clearview Хоан Тон-Тат не выказывал подобных сомнений. В «Дейли» он не казался плохим, но его слова звучали самодовольно, грубо и равнодушно. По словам Хилл, она спросила Тон-Тата о последствиях создания технологии, которая возвестила бы конец общественной анонимности, и он ответил: «Мне придется над этим подумать». Логично было подумать заранее, но Тон-Тат, по-видимому, не видел для этого оснований.

Сегодня от прихотей таких людей, как Тон-Тат, зависят наша частная жизнь и многие гражданские свободы. Я уверен, что Марк Цукерберг, сидя в своей комнате в общежитии Гарварда, вовсе не мечтал создать платформу, которая помогла бы России подорвать американскую демократию, но сделал он именно это. Скорее всего, он мечтал построить что-то великое и изменить мир – добиться успеха, оставить свой след. Это он тоже сделал. И сегодня несет фидуциарную ответственность перед своими инвесторами за максимизацию их прибыли. Перед остальными людьми у него нет таких обязательств. Если наши гражданские свободы ставят под угрозу прибыль бизнесов, торгующих технологиями слежки, предприниматели вольны всякий раз выбирать прибыль.

---

[4] Hill, “Secretive Company”.

Причина не в том, что они плохие люди. В конце концов, даже руководители крутых зеленых компаний, таких как Burt's Bees и Tom's of Maine (ныне дочки компаний Clorox и Colgate-Palmolive), тоже больше заботятся о максимизации прибыли, чем о гражданских свободах незнакомцев. Но технология Clearview AI и – в более широком смысле – панoптические возможности современных технологий слежки в сочетании с недорогим и постоянным хранением информации (особенно в эпоху возрождающегося авторитаризма и институциональной слабости в развитых странах) создают невиданную угрозу нашей демократии. Другими словами: нашей свободе угрожают не те люди, которые покупают больше зубной пасты или отбеливателя, а те, которые покупают продукты Clearview.

Мы обязаны постоять за себя, заявить о наших гражданских свободах и о том, каким хотим видеть этот мир. Нужен ли нам мир, в котором любой незнакомец может сфотографировать нас и узнать о нас все? Если нет, мы должны предотвратить появление такого мира. В следующих главах я надеюсь показать вам, зачем это делать и как.

Эта книга выросла из серии статей, которые я написал для The Economist в первой половине 2018 года. В них говорится, как технологии меняют систему правосудия – в частности, работу полиции, тюрем и судов[5]. Я решил сосредо-

[5] John Fasman, "Data Detectives", *The Economist*, Technology Quarterly: Justice, June 2, 2018.

точиться на полиции и ее технических специалистах, потому что полиция – это, пожалуй, самое осязаемое и привычное проявление государственной власти. Если я скажу, что у Агентства национальной безопасности или правительства Китая есть технология наблюдения, позволяющая подслушивать и сохранять все наши разговоры по мобильным телефонам или отслеживать передвижения, вы, возможно, возмутитесь, но вряд ли удивитесь. Но, надеюсь, вас возмутит и шокирует, если узнаете, что эта возможность есть у каждого полицейского управления – и нет практически никакого надзора за тем, как она используется. Говоря о полиции, я действительно имею в виду государственную власть.

Когда я делал репортажи для The Economist, распознавание лиц было в значительной степени теорией – оно еще не стало частью жизненного опыта большинства людей. Некоторые полицейские департаменты запускали скромные тестовые программы. Где-то такие системы использовались для ограниченного круга задач, например, в 2017 году округ Вашингтон в Орегоне начал таким способом выявлять подозреваемых. Сегодня эти системы появились в терминалах аэропортов. Даже если завтра Clearview разорится, то же самое будет делать другая фирма.

Некоторые критики утверждают, будто эта технология ненадежна, и так оно и есть, особенно в Америке и Европе для цветных людей. Но суть не в этом. Распознавание лиц опасно, когда оно ненадежно: это может привести к аресту

невинных людей. Но и когда надежно – все равно опасно, поскольку позволяет правительствам публично отслеживать нас в любое время. И оно становится все надежнее. Считыватели номерных знаков умеют следить за нашими автомобилями, и такие приборы можно устанавливать на любом количестве полицейских машин и городских фонарных столбов – в зависимости от политической прихоти и бюджета. Устройства, которые имитируют узлы сотовой связи и обманывают наши телефоны, вынуждая их показывать, кому мы звонили, что писали и какие веб-сайты искали, теперь помещаются в багажнике автомобиля.

Нас окружают архитектура и инфраструктура тотальной государственной слежки. Мы знаем, как это выглядит в Китае, где сейчас больше государственных камер наблюдения, чем людей в Америке. Китай использует все возможности, чтобы подавлять свободу слова и самовыражения, следить за инакомыслящими и содержать более миллиона мусульман в современных концлагерях (а если и на свободе, то под сплошным неусыпным наблюдением).

Самый острый и тревожный вопрос, который я услышал, готовя материал для этой книги, задала Кэтрин Крамп, профессор права Калифорнийского университета в Беркли, руководитель семинара права, технологий и государственной политики и содиректор Центра права и технологий Беркли. «Сейчас мы можем получить идеальную архитектуру контроля, – сказала она мне, – как у Китая. Какие демократиче-

ские практики нам нужны, чтобы мы не стали Китаем?» Настоящая книга представляет собой скромную попытку ответить на этот вопрос.

1. Технология и демократия

Какой объем государственного надзора и контроля вы готовы терпеть во имя общественной безопасности?

Я сижу на переднем сиденье полицейского внедорожника. За рулем – участковый надзиратель, очень добродушный лейтенант Лео Каррильо. Он родился и вырос в Даун-Нек, когда-то португальском районе Ньюарка Айронбаунд. Лео уже двадцать лет служит копом в Ньюарке, и его знаний об этом городе хватило бы на целую энциклопедию. Сзади сидит Марк Ди Ионно. До того как стать офицером по связям с общественностью в полицейском управлении, он двадцать шесть лет писал статьи для Newark Star-Ledger. Марк крутой, умный и опытный, с грубоватым, но добродушным характером и твердой речью. Все эти качества вместе создают завидное впечатление, что перед вами персонаж из рассказов Дэймона Раньона.

Мы ездим по городу уже около четырех часов, и каждый перекресток вызывает в памяти моих спутников массу историй. Вот пиццерия, где застрелили Вилли Джонсона. Вот угол, где женщина пошла за молоком для своих троих детей

и была ранена в перестрелке. Сюда родители возили нас за покупками, а теперь здесь склад, видавший лучшие времена. А это Хоукс Лаунж, дверь заколочена (похоже, там ремонт), а раньше здесь было довольно мрачно.

Это вечер пятницы. Через неделю будет летнее солнцестояние, и Ньюарк гордо чистит перышки. Самый крупный город штата Нью-Джерси имеет паршивую репутацию. Если вы не из тех счастливчиков, кто хорошо знает Ньюарк, он, вероятно, покажется вам достойным и смеха, и сочувствия. Возможно, вызовет те же ассоциации, что и Детройт, и Янгстаун: насилие, постиндустриальный упадок и заброшенность. Ньюарк – это Ржавый пояс[6] по духу, экономике и обстоятельствам, если не по местоположению: он деиндустриализировался вместе с остальным северо-востоком, и уходящую из него промышленность ничто так и не смогло заменить.

Но что вам никто никогда не скажет и что вы не поймете сами, пока не проведете здесь некоторое время – это насколько прекрасно, особенно в один из таких долгих и теплых июньских вечеров, отложить, пусть и временно, все ваши ссоры с Богом и ближними и греться в этом «жидком золоте». Здания в стиле ар-деко в центре города выглядят так, будто их искупали в меде. Прыгать через заросшие пустыри

[6] Ржавый пояс, известный также как Индустриальный или Фабричный пояс, – часть Среднего Запада и Восточного побережья США, в котором с начала промышленной революции и до 1970-х годов были сосредоточены сталелитейное производство и другие отрасли американской тяжелой промышленности. – *Прим. ред.*

без костюма химзащиты и ботинок на толстой подошве не хочется, но с противоположной стороны улицы эти заросли выглядят как квадратики лесистого рая – со всеми цветущими сорняками и лениво жужжащими пчелами.

Проезжая мимо парка Викуахик – трехсотакрового пространства на юге, созданного сыновьями человека, который спроектировал Центральный парк Нью-Йорка, – мы слышим, как смеются и играют в пятнашки маленькие дети. Окрестности там аккуратные и уютные, пригород напоминает эпоху трамваев и скромных доходов: трехэтажные дома, разделяющие их лужайки и по автомобилю у каждого подъезда.

В этом многообещающем американском районе середины прошлого века вырос Филип Рот. Перед домом его семьи на Саммит-авеню есть мемориальная доска. Это скромный милый дом в нескольких милях к западу от парка. На протяжении всей карьеры Рот поддерживал с Ньюарком романтические (если не серьезные) отношения. Но его, безусловно, лучшее высказывание о Нью-Джерси и литературных амбициях прозвучало в романе «Другая жизнь»: «Набирая из ресторана свой домашний номер, Генри вспомнил, как после лекции, во время вопросов, один студент спросил Натана, пишет ли тот ради бессмертия. Натан рассмеялся и дал ответ, достойный его покойного брата: “Если ты из Нью-Джерси, ты можешь написать тридцать книг, получить Нобелевку, дожить до седых волос и девяноста пяти лет – и все равно

маловероятно, хотя и не невозможно, что, когда ты умрешь, в твою честь назовут стоянку с туалетом на шоссе Джерси Тернпайк. И поэтому тебя будут долго помнить, но в основном маленькие дети, которые сидят на заднем сиденье машины, а потом наклоняются вперед и просят: папа, пожалуйста, остановись у Цукермана – мне нужно пописать". Для писателя из Нью-Джерси это самое реальное бессмертие, на какое только можно рассчитывать»[7].

Группы детей постарше бродят по переулкам, начинают свои выходные у магазинов и на тротуарах, крича, флиртуя и выпячивая грудь, как это делают подростки повсюду, зависшие в этом неловком прыжке между играми в сквере и взрослой жизнью. На одном углу мы останавливаемся, когда высокий, гордый и блестяще лысый отец одной рукой хватает под мышку малыша, а другую протягивает мальчишке постарше, чтобы перейти улицу. Он кивает и улыбается знакомому через дорогу. В вечернем воздухе разносятся звуки и запахи кухонь. Обычный летний вечер – такой длинный, что кажется вечным, и настолько совершенный, что может быть только мимолетным.

Когда мы проезжаем мимо пустых домов Сета Бойдена – невысоких кирпичных зданий, ныне заброшенных и заколоченных, – смартфон лейтенанта Каррильо громко чирикает. Приложение сообщает, что примерно минуту назад в нескольких кварталах от нас было произведено семь выстре-

[7] Philip Roth, *The Counterlife* (New York: Farrar, Straus and Giroux, 1986), 237.

лов. Каррильо нажимает пальцем иконку на экране. Тут же открывается карта перекрестка, где, по мнению приложения, были произведены эти самые выстрелы, и звучит аккомпанемент – семь быстрых хлопков: два, короткая пауза, потом три, опять пауза, и еще два. Это не похоже на перестрелку из двух или нескольких пистолетов: все хлопки звучат одинаково, будто все пули выпущены из одного и того же оружия, с одного и того же места.

Приложение называется ShotSpotter, и по состоянию на декабрь 2019 года его использовали полицейские управления более чем в ста городах Америки[8]. Предпосылка довольно проста: в этих городах массивы установленных акустических датчиков обучены распознавать выстрелы и сообщать о них полиции в реальном времени. В Ньюарке датчики обычно устанавливаются на светофорах и выглядят как белые бриллианты. Когда такие датчики распознают что-то похожее на выстрел, они определяют его местоположение на карте города, а затем предупреждают акустических аналитиков ShotSpotter. Те подтверждают, что датчики зафиксировали именно выстрел, а не звук металлической двери или выхлопной трубы грузовика. Затем в полицию поступает оповещение: сколько выстрелов, из скольких стволов и где.

Каррильо становится серьезным, ускоряется и включает полицейский радиоканал. Каждый перекресток мы проезжа-

[8] ShotSpotter, 2020 Annual Report, available at https://ir.shotspotter.com/annual-reports.

ем с сиреной и мигалкой. От диспетчера пока ничего, но по мере приближения к месту происшествия видим подъезжающие со всех сторон полицейские джипы.

Приложение сообщает, что стреляли с территории огромного кладбища, примыкающего к школе. Кладбище окружено высоким сетчатым забором, увенчанным тремя рядами ржавой колючей проволоки. Мы тормозим перед запертыми воротами. Кроме нас, у края дороги уже припарковано семь полицейских машин. Двое офицеров стоят на возвышенности за школой и осматривают кладбище: не бежит ли кто. Остальные патрулируют периметр.

С одной стороны, в этой сцене не было ничего необычного: в полицию поступил сигнал о стрельбе, сотрудники выехали на место происшествия и попытались найти стрелявшего. Но кое-что всего десять лет назад показалось бы нам немыслимым. Десяток офицеров прибыли на место происшествия не потому, что адрес им дал диспетчер или лейтенант, а потому, что это сделали их смартфоны.

Возможно, не стоит удивляться, что иногда телефоны отдают приказы правоохранителям. В конце концов, мы все так живем. Но за день до поездки с лейтенантом Каррильо я провел некоторое время с его начальником Энтони Эмброузом, руководителем отдела общественной безопасности Ньюарка. (Мэр Ньюарка Рас Барака объединил городскую полицию, пожарную и аварийную службу в одну структуру, которую теперь возглавляет Эмброуз.)

Большой, лысый, широкоплечий, с типичным говором уроженца Джерси, Эмброуз идеально подходит на эту роль. Он поступил на работу в полицейское управление Ньюарка в 1986 году. Как он сам объяснил, в те времена единственное, что можно было компьютеризировать, это бензиновый насос на заправке. Полицейские вели учет своих действий в служебном журнале при помощи шариковой ручки. Диспетчеры записывали задания на картонных карточках, которые затем хранились три года. Чтобы обозначить место происшествия, офицер втыкал в настенную карту канцелярскую кнопку и подкрашивал ее: красный цвет означал убийство, черный – грабеж.

Эмброуз рассказывает об этих подробностях с ироничной нежностью, но без ностальгии. По его словам, переход к цифровой информации и хранению облегчает работу полиции: с помощью компьютера можно отлично вести записи, вычерчивать схемы преступлений и определять координаты транспортных средств. Он добавил: в прежние времена сбор досье на жертву убийства, включая не только имя, адрес и возраст, но любые аресты, приговоры и задержания, а также известных сообщников и членов семьи, занимал пару добрых дней. Теперь вся эта информация доступна по одному щелчку мыши на планшете офицера или встроенном автомобильном компьютере.

И все же, по его словам, в итоге большинство полицейских просто обслуживают компьютер. Полиция перестала дей-

ствовать на упреждение. Системы GPS отслеживают движение офицера. Компьютеризированная диспетчерская служба фиксирует, что он делает и как долго. Поскольку отслеживается, записывается и оценивается каждая минута и каждый шаг, сотрудники полиции вряд ли станут тратить неструктурированное время на то, чтобы пройтись по своему району и ближе познакомиться с людьми.

Трудно определить, как прекращение этой практики влияет на уровень преступности – ведь несостоявшиеся разговоры подсчитать или измерить невозможно. Но стоит хотя бы поинтересоваться, что именно мы теряем, когда учреждение живет и умирает по одной и той же шаблонной схеме. После одного судебного постановления о неконституционности политики в сфере задержания и обыска Управление полиции Нью-Йорка (NYPD) выпустило новые инструкции, которые позволяли показывать ожидаемую положительную статистику[9]. Это, конечно, не аргумент против технологий, но показывает их ограниченность.

---

[9] Если сотрудник полиции останавливает и обыскивает кого-либо, не имея веских оснований для ареста, это не является неконституционным действием при условии, что у сотрудника есть обоснованные подозрения в том, что человек совершил, совершает или собирается совершить преступление. Но, как объяснила судья Шира Шейндлин из Окружного суда Соединенных Штатов по Южному округу Нью-Йорка в деле *Флойд против города Нью-Йорк*, 959 F. Supp. 2d 540 (2013), «на практике правила поощряют преследование молодых чернокожих и испаноязычных мужчин, поскольку они чаще всего фигурируют в поступающих жалобах на преступления. Это форма расового профилирования» и, следовательно, противоречит конституции.

Есть и другие ограничения, которые стоит учитывать. ShotSpotter можно похвалить за многое. Информация о выстрелах слишком часто теряется. Периодически стрельба происходит в пустынных местах, и ее никто не слышит, а тот, кто все-таки слышит, ожидает, что в полицию позвонят другие. Может быть, люди, слышавшие выстрел, не привыкли доверять полиции и поэтому ни о чем не сообщают. Возможно, они опасаются возмездия. Но никто не хочет жить в районах, где часто происходит насилие с применением огнестрельного оружия. Если ShotSpotter может помочь в поимке преступников, которых иначе бы не поймали, – он служит добру, верно?

Но если мыслить шире? Что может произойти, когда полицейских направляет не командир и не звонок озабоченного гражданина, а частная компания, использующая запатентованную технологию? Если бы мы спросили офицеров, сканировавших кладбище, почему они там находятся, они ответили бы: нас прислал телефон. Что это означает для подотчетности и автономии правоохранительных органов? Возможно, жители всех девяноста городов, где используется ShotSpotter, вполне могут делегировать некоторые диспетчерские решения от самих полицейских непрозрачному алгоритму обнаружения выстрелов, предлагаемому коммерческой компанией. Но есть вероятность, что у граждан другое мнение. И в этом случае они заслуживают, чтобы им дали слово.

* * *

Рассмотрим еще одну технологию раскрытия незарегистрированных преступлений – службу мониторинга, предлагаемую компанией Росса Макнатта Persistent Surveillance Systems. Эта технология родилась на полях сражений в Ираке как способ выявления людей, которые устанавливали самодельные взрывные устройства для убийства американских солдат.

Макнатт, возглавивший Центр быстрых разработок при ВВС США, установил камеры на дроны и облетел ими город Эль-Фаллуджа, записывая увиденное. Если вам двадцать или тридцать лет, у вас может не быть никаких особых ассоциаций с иракским городом Эль-Фаллуджа. Но те, кто помнит начало катастрофического вторжения Америки в Ирак после терактов 11 сентября 2001 года, не забыли и ожесточенных боев за контроль над этим городом.

«Мы увидели, как взрывается бомба, – объяснял мне Макнатт, – проследовали за людьми, которые ее заложили, и вернулись в прошлое, чтобы посмотреть, откуда они взялись. Мы существенно помогли установлению мира и стабильности в Эль-Фаллудже».

Когда Макнатт вышел на пенсию, он решил использовать эту технологию для раскрытия убийств в Америке. Он рассудил, что большинство убийств остаются нераскрытыми, за-

частую по причинам, о которых я упоминал выше. *Всевидящее небесное око* позволило бы полиции видеть больше. Степень ее информированности больше не зависела бы от бдительности граждан. Это дало бы полицейским машину времени: они могли бы увидеть убийство, а затем отмотать видеокадры назад, чтобы выяснить, откуда взялись убийцы.

Хотели бы, чтобы такая технология летала над вашим городом? А над вашим районом? А если она летает не над вами, а над другим городом, который вы давно не посещали из-за высокого уровня преступности? Кто решает, над чьими домами будет летать дрон? Есть ли у жителей право голоса? И если *да,* как сопоставить их желания с желаниями остальных горожан?

Правила, регулирующие использование, просмотр и хранение отснятого материала, – насколько они строгие? Действительно ли мы хотим создать именно такой прецедент? Сегодня на кадрах Макнатта люди выглядят как неразличимые точки, но что произойдет, когда камеры станут лучше или дроны полетят ниже? Точки превратятся в узнаваемых людей. Что произойдет, когда в городе появится начальник полиции с хорошо скрываемой мстительной жилкой и захочет преследовать тех, кто его критикует? Может ли полиция использовать эти дроны для отслеживания и записи акций против жестокости полиции и за общественную безопасность, а затем направить машину времени на протестующих: а не сделали ли они в прошлом что-либо, заслуживающее

ареста?

Все эти вопросы можно свести к одному фундаментальному, о котором вы должны помнить, читая эту книгу: *какой объем государственного надзора вы готовы терпеть ради общественной безопасности?*

Это непростые вопросы, и со временем они не станут проще.

* * *

«Мы уверены, что можно обезвреживать рецидивистов в самом начале их карьеры, – сказал мне Макнатт. – Если остановить преступника после того, как он выстрелил в первого человека, а не в десятого, можно спасти многих людей. Мы снижаем уровень насилия, раскрывая преступления, которые иначе было бы невозможно раскрыть. И, раскрывая, показываем, что система работает: если вы совершите серьезные преступления, вас поймают и осудят. Вот где срабатывает сдерживание».

Кто с этим не согласится? Ловить убийц, которые иначе ушли бы от правосудия, укреплять веру в эффективность системы уголовного права, удерживать людей от совершения новых преступлений – такие цели поддержит каждый.

Но любой ли ценой мы готовы это поддерживать? Дроны Persistent Surveillance могут кружить над огромной полосой города, наблюдая и фиксируя всех – и даже тех (а зная стати-

стику, мы скажем, что в первую очередь именно тех) людей, которые вовсе не подозреваются в совершении каких-либо преступлений.

Сейчас это звучит хуже, чем есть на самом деле. Я позже объясню: разрешение камер этой компании чрезвычайно низкое, и люди похожи на маленькие точки. Невозможно сказать, как они выглядят, во что одеты, что держат в руках, какого цвета у них волосы или кожа. Но технология камер слежения постоянно совершенствуется. Пусть компания Макнатта принципиально хранит верность съемкам с низким разрешением, но ничто не мешает другой фирме установить на дроны камеры с высоким разрешением и отправить их в полет над городом.

Как сказал мне Макнатт, Persistent Surveillance реагирует на сообщения о преступлениях, когда полицейские выясняют, что в районе наблюдения произошла стрельба и они сосредоточиваются на поисках стрелявшего и перестают преследовать неосторожных пешеходов. Но опять же, пешеходами может заняться другая компания. С помощью этой технологии можно и бороться с преступностью, и выяснять, кто записался на аборт. Или пришел на встречу анонимных алкоголиков. Или посещает церкви, синагоги, мечети – и как часто. Технология может проследить путь человека домой с политической демонстрации. Вы возразите: мол, полиция тоже умеет следить за нами в общественных местах. Но если бы вас несколько дней преследовала полицейская машина,

вы заметили бы ее. А эта технология невидима и не обнаружима.

Полицейское управление Балтимора (BPD) использовало Persistent Surveillance на протяжении большей части 2016 года. Это частное тестирование проводилось на средства Джона и Лоры Арнольдов, филантропов из Техаса, которые финансируют различные инновации в области уголовного правосудия. Управление не обязано было получать разрешение городского совета и даже информировать его, оно этого и не сделало. О системе стало известно только после того, как Bloomberg Businessweek написал о ней статью и потребовал от представителя BPD объяснений: почему программа слежения, о которой никто не знал, удивительным образом не является секретной программой слежения[10].

Во время пробного запуска BPD сообщило: если изображения, собранные Persistent Surveillance, не связаны с каким-либо текущим делом, они хранятся всего сорок пять дней. Но позже в том же году начальник полиции Балтимора сообщил городскому Управлению общественных защитников, что все изображения, записанные/отснятые во время пилотного запуска программы, сохранены, заархивированы и, следовательно, доступны – независимо от того, были ли они предоставлены BPD для использования в расследовани-

---

[10] Monte Reel, "Secret Cameras Record Baltimore's Every Move from Above", *Bloomberg Businessweek*, August 23, 2016, www.bloomberg.com/features/2016-baltimore-secret-surveillance.

ях[11]. Это противоречие подчеркивает еще одну повторяющуюся тему этой книги: решающее значение имеет политика использования таких ресурсов, но без независимого аудита и реальных наказаний за ее несоблюдение она мало чего стоит.

Макнатт долго говорил со мной о своем стремлении успокоить людей, опасающихся вторжения в частную жизнь, и о том, что для отснятого материала существует аудиторский след. А это означает, что если некий офицер войдет в систему с целью заглянуть в дом своей бывшей девушки, операторы об этом узнают. Я считаю, что Макнатт искренне тревожится за общественную безопасность и конфиденциальность. Но в целом основатели компаний не заходят дальше этого при оценке потенциального вреда технологий слежения.

Макнатт также рассказал о своих беседах с Американским союзом гражданских свобод (ACLU). К его чести, он попытался представить свою позицию этой группе в ее штаб-квартире в Вашингтоне, округ Колумбия, утверждая, что изображения с низким разрешением не несут угрозы для частной жизни граждан. Но из этого ничего не вышло. Согласно статье в Bloomberg Businessweek, Джей Стэнли, эксперт по вопросам конфиденциальности и политический аналитик из ACLU, почувствовал себя свидетелем того, как де-

[11] Jay Stanley, "Baltimore Aerial Surveillance Program Retained Data Despite 45-Day Privacy Policy Limit", American Civil Liberties Union, October 25, 2016, www.aclu.org/blog/privacy-technology/surveillance-technologies/baltimore-aerial-surveillance-program-retained.

баты о неприкосновенности частной жизни или безопасности в Америке перетекают в неизведанные воды. Стэнли сказал себе: «Вот где происходит все самое главное. Наконец к нам пришла технология, и Большой Брат уже здесь».

Кто-то возразит: Макнатт тоже является гражданином этой страны и не больше нас с вами хочет стать объектом навязчивой слежки. Но финансовые мотивы, соблазны успеха и фидуциарные обязательства перед акционерами способны творить с принципами человека странные вещи. Ремесленники, начиная с Виктора Франкенштейна, подтвердят: творения могут жить собственной жизнью, зачастую совершенно не такой, какой ее воображали их создатели. Джек Дорси, вероятно, не собирался делать веб-сайт, на котором американцы бесконечно плевались бы друг в друга ложью и желчью, но он создал именно такой веб-сайт.

Очевидно, что эксперимент Балтимора с Persistent Surveillance был реализован плохо. Полицейские управления не должны развертывать подобные системы активного наблюдения, скрывая от всех этот факт. Однако, несмотря на разногласия, дроны проделали хорошую работу, и, как я объясню позже, они снова будут летать. Примерно за триста часов полета они засняли на пленку двадцать три выстрела, из них пять со смертельным исходом. Наши телефоны отслеживают наше местоположение. Файлы cookie позволяют рекламодателям узнавать наши привычки. Полицейские, передвигаясь пешком и на колесах, видят, как мы ходим по сво-

им делам. Дроны снимают городские улицы, а не обстановку наших домов, они видят нашу общественную жизнь, а не частную – ну что нам стоит появиться в виде неразличимой точки на кадрах с дронов, если ловят стрелков и убийц, которых в противном случае никто бы не поймал?

Или подумайте о том, что происходило, пока я вычитывал редактуру этой рукописи, используя последний шанс автора внести в книгу существенные правки. Это была середина мая 2020 года, и, как и прочие жители Восточного побережья, я уже чуть более двух месяцев сидел взаперти. Почти 90 000 американцев умерли от COVID-19 – более четверти из них в моем родном штате Нью-Йорк. Несмотря на обширные меры предосторожности, мой отец подхватил вирус в легкой форме и несколько недель болел дома. Его симптомы после этого держались еще пару месяцев.

Америка и Южная Корея подтвердили первые случаи заболевания COVID-19 в один и тот же день, но на момент написания моей статьи в Южной Корее от вируса умерло всего 260 человек. Население Америки в шесть с лишним раз превышает население Южной Кореи, но погибших у нас было в 330 раз больше. Это в значительной степени связано с тем, насколько обширно отслеживаются контакты между людьми в Южной Корее с помощью приложений – и в этом задействованы такие уровни правительственного надзора, мониторинга и сбора информации, которых многие американцы просто не потерпят. Даже просьбу носить маски в обще-

ственных местах некоторые люди восприняли в штыки.

Любопытно, что отношение к слежке не выглядело последовательным или тенденциозным: противодействие локдауну – и, вероятно, необходимости загружать приложения для отслеживания контактов – было гораздо более распространено среди правых, чем среди левых, как и симпатия к полиции. Многие левые обеспокоены возможной полицейской слежкой, но тоскуют по активному мониторингу здоровья, с помощью которого Южная Корея сдерживала распространение COVID-19. Скажу для протокола: я уж точно не тосковал по такого рода наблюдению. Но если бы приложение для отслеживания контактов было доступно – а я был бы уверен, что данные поступят только в государственные и местные департаменты здравоохранения и ни при каких обстоятельствах не будут доступны правоохранительным органам – я бы его скачал. Если оно станет доступно после того, как я напишу эти строки, и до того, как вы их прочтете, я его загружу, а затем удалю, как только сделаю прививку.

Некоторый сбор персональных данных необходим для отслеживания контактов, а отслеживание контактов необходимо для прекращения неконтролируемого распространения COVID-19. Но существует огромная разница между добровольным предоставлением ограниченной личной информации для целей общественного здравоохранения (и только органам общественного здравоохранения) и той разновидностью ползучего, невидимого полицейского наблюдения, ко-

торую я рассматриваю в этой книге. Если мы соглашаемся на первое (учитывая, что оно ограничено по объему и цели), мы не обязаны соглашаться на безграничное второе. Во всяком случае, отказ от скрытой слежки приобретает еще бóльшую важность перед лицом наблюдения, обусловленного пандемией.

* * *

Напомню, я начал углубляться в вопросы слежки и охраны правопорядка в начале 2018 года, когда опубликовал серию статей о том, как технологии меняют системы правосудия по всему миру. Серия началась с того же посыла, что и эта книга: технологии радикально меняют работу полиции, и мы еще не полностью оценили масштабы и последствия этих изменений. В каком-то смысле это утверждение банально, ведь технологии меняют практически каждый аспект нашей жизни. Новая революция еще молода, и мы пока не до конца ее осознали.

Но полиция – уникальная область. Полицейские – самые заметные представители государственной власти. Их работа состоит в том, чтобы обеспечивать нашу безопасность. Для этого они уполномочены наблюдать, допрашивать, избивать, заключать в тюрьму и убивать. То, как полиция использует свою власть, может иметь смертельные последствия, и ее сотрудники намеренно придают себе устрашающий вид.

Я патрулировал улицы вместе с полицейскими в Ньюарке, Лос-Анджелесе, Атланте и Вашингтоне (округ Колумбия), а также в Хай-Пойнте (Северная Каролина) и Ньюпорт-Ньюсе (Виргиния). Я разговаривал с офицерами из доброй дюжины других отделов и вообще знаком с десятками полицейских. Я смеялся с ними, спорил с ними, выпивал с ними и учился у них.

Но всякий раз, когда вижу полицейскую машину, припаркованную на обочине шоссе или приближающуюся к моему автомобилю, нервничаю, и, к сведению, я белый мужчина средних лет, которого никогда не арестовывали. Я чувствую внезапный всплеск адреналина: потные ладони, металлический привкус во рту. Несколько лет назад, когда я вез свою семью домой из Флориды в Атланту, где мы тогда жили, меня в маленьком городке в Южной Джорджии остановил офицер за превышение скорости на несколько миль. (Многие жители Атланты считают, что полиция Южной Джорджии с особой жестокостью штрафует машины с номерами округов Де-Калб или Фултон, то есть из Атланты.) Меня трясло, хотя я знал, что не совершил ничего, кроме невинного превышения скорости.

Кроме того, полиция нам очень знакома. Если я скажу, что прослушиванием наших телефонных разговоров и отслеживанием перемещений занимается, допустим, Агентство национальной безопасности (АНБ), вы, вероятно, поморщитесь и пожмете плечами. Но название АНБ вызывает

в воображении картину бесконечных рядов компьютерных мониторов в незнакомом офисном здании. Полиция – нечто более узнаваемое, повседневное, даже рутинное. В отличие от агентов АНБ, полицейские в нашем воображении – это люди с лицами.

Однако полиции доступны практически те же возможности наблюдения на уровне улиц, что и Агентству нацбезопасности, и надзор за ее деятельностью относительно небольшой. В Америке и других либеральных демократиях сложная переплетающаяся сеть законов и ожиданий, касающихся неприкосновенности частной жизни, никак не дотянется до полномочий по наблюдению и сдерживанию, доступных даже самому скромному полицейскому участку.

Например, полиция не может прослушивать ваши телефонные разговоры без ордера. Но в большинстве юрисдикций ваши метаданные, то есть содержимое телефона, не связанное с разговорами (в том числе данные абонентов, время и длительность звонков, SMS-сообщения, данные о просмотре веб-страниц, информация о вашем местоположении), защищены гораздо хуже, хотя в совокупности они дают полиции куда больше информации, чем телефонная прослушка: ведь теперь полиция знает, где вы были, с кем разговаривали, что искали в интернете.

По закону вся эта информация является общедоступной, поскольку вы поделились ею со своим оператором телефонной связи. *Доктрина третьей стороны* гласит: доброволь-

ная передача информации третьей стороне (банк, поставщик телекоммуникационных услуг) сводит на нет любые разумные ожидания в отношении конфиденциальности[12]. Поэтому полиция может без ордера получить, например, отчет о движении средств на вашем банковском счете. Суды стали более скептически относиться к этому принципу, но он остается в силе и сегодня, когда для мобильного и онлайн-общения в нем уже нет смысла.

Или рассмотрите публикации в социальных сетях. Они, конечно, общедоступны в разной степени, в зависимости от сервисов и настроек, но гораздо более общедоступны, чем, скажем, ваш личный дневник или сложенный лист бумаги, который вы запираете в тумбочке. Логично, что полиция будет использовать в расследованиях посты подозреваемых.

Офицер одного полицейского управления на Восточном побережье, сокрушенно качая головой, рассказал мне, как часто люди публикуют видео с кадрами собственных преступлений или фотографии, на которых они транжирят преступные доходы. Моя любимая история этого распространенного жанра произошла в Кентукки: парень опубликовал фотографию, на которой одной рукой показывает средний палец, а другой сливает бензин из полицейской машины (в

[12] Блог Lawfare, посвященный острым вопросам национальной безопасности, предлагает по-своему выдающуюся дискуссию о доктрине третьей стороны в заметке: Michael Bahar, David Cook, Varun Shingari, Curtis Arnold, “Third-Party Party-Crashing? The Fate of the Third-Party Doctrine”, October 19, 2017, www.lawfareblog.com/third-party-party-crashing-fate-third-party-doctrine.

итоге он провел ночь в тюрьме).

Но есть инструменты, при помощи которых власти в огромных масштабах извлекают данные (часто незаметно для пользователя и без его согласия) из сообщений в социальных сетях. Они получают не только содержимое сообщений и идентификаторы пользователей, но и их IP-адреса и адреса электронной почты, номера телефонов, данные о местоположении и историю социальных сетей.

В начале 2019 года ACLU подал в суд на федеральное правительство за то, что оно не ответило на запросы по Закону о свободе информации (FOIA) относительно мониторинга социальных сетей иммигрантов и заявителей на визу[13]. В июле того же года ФБР собирало предложения по созданию инструмента, который позволил бы агентству отслеживать людей по местоположению и искать по ключевым словам в режиме реального времени. Наверняка большинство людей понимают, что полиция может без ордера наблюдать за их общественной жизнью, однако они все еще обеспокоены массовой и безнадзорной слежкой, которую предлагает система Persistent Surveillance. Точно так же большинство наверняка сознает, что социальные сети находятся в открытом доступе и, следовательно, полиция вольна с чистой совестью изучать их при расследованиях, но многие все еще обеспокоены та-

---

[13] *ACLU против USDOJ*, Гражданский иск 19-cv-00920-EMC, поданный в Окружной суд Соединенных Штатов по Северному округу Калифорнии (Сан-Франциско) 6 сентября 2019 года.

ким безосновательным, интенсивным, скрытым наблюдением в массовом масштабе.

В процессе написания этой книги я слышал, как часто ссорятся друг с другом полицейские и борцы за приватность. Полиция часто думает, будто активисты отличаются наивностью, навязчивостью и рефлекторной нелюбовью к полиции. Активисты часто думают, что полиция обманывает и стремится к контролю. На самом же деле они нужны друг другу. Активисты, как и все остальные, нуждаются в полиции для поддержания общественной безопасности, полиция нуждается в активистах, чтобы вести себя более ответственно. В значительной степени – хотя обе стороны признают это с крайней неохотой – они извлекают выгоду из работы друг друга.

Небольшое идеологическое примечание: я общался как с полицейскими, так и с аболиционистами (в том числе сторонниками отмены тюремного заключения) и читал их работы. Надеюсь, я правильно понимаю аболиционистов и могу точно сформулировать их основной аргумент: они считают, что социуму будет лучше без полиции, когда сообщества смогут сами устанавливать собственные стандарты преступного поведения и обеспечивать их коллективное соблюдение. Эта точка зрения мне симпатична, но я ее не разделяю. Считаю, что обществу нужны и полиция, и гражданский надзор за полицией. Если вы думаете иначе, надеюсь, виды активности и надзора, которые я одобряю в этой книге,

все равно покажутся вам полезными.

Полицейские скажут вам (как говорили мне): они не делают того, чего опасаются борцы за конфиденциальность. Не отслеживают невиновных людей и не составляют на них досье. Им неинтересно заглядывать в окна спален или следить за тем, какие политические митинги посещают граждане. Однако правоохранительные органы, конечно, всегда этим занимались, и новые технологии дают им возможность делать все это – и еще много чего – с минимальными затратами и усилиями.

Полиция должна иметь доступ к технологиям, которые считает необходимыми для выполнения своей работы. Но она также должна объяснять людям, которым служит, зачем эти технологии нужны и как будут использоваться. Полиция обязана вводить строгие правила использования таких технологий – с независимым аудитом, требованиями к публичной отчетности и штрафами за их несоблюдение. Я верю в строгий гражданский надзор за полицией не потому, что полицейские плохие люди, а потому, что наши гражданские свободы не должны зависеть от прихотей и предпочтений государства или от нашей способности предотвратить появление еще одного Дж. Эдгара Гувера. Граждане заслуживают права голоса в принятии решений об их защите.

Подавляющее большинство как полицейских, так и борцов за тайну частной жизни изо всех сил заботятся о безопасности и благополучии общества. Но это не значит, что

они всегда хотят одного и того же. Я уверен, например, что большинство полицейских предпочли бы минимальный контроль, а большинство активистов – максимальный. Но посадите их в одну комнату, а не перед телекамерами, и заставьте разговаривать друг с другом, а не друг о друге, и они быстро сгладят 90 % своих разногласий. А по оставшимся десяти почти всегда сумеют достичь приемлемого компромисса за счет постепенной, честной и кропотливой работы. Я знаю, что это правда, потому что видел, где и как это работает, и я отведу вас туда.

* * *

В этой книге я предлагаю схему, по которой граждане должны оценивать новые формы технологий наблюдения. Я применяю ее к полицейской практике. Но эти вопросы выходят далеко за рамки деятельности полиции. Возможно ли открытое либеральное общество, если нас можно будет отслеживать и записывать на каждом шагу? Имеем ли мы право на определенную степень публичной анонимности – право ожидать, что нас не будут отслеживать и контролировать, если не заподозрят в совершении каких-либо преступлений? Что государству позволено знать о нас? Как и с какой степенью надзора власти могут собирать эти знания? Иеремия Бентам когда-то придумал тюрьму, спроектированную таким образом, чтобы любой из охранников со своего поста мог видеть

каждого заключенного. Такой паноптикум так и не был построен, но, по сути, мы все сейчас живем в паноптикуме – и что нам с этим делать? В этой книге мы внимательно посмотрим на технологии, которые вызывают эти вопросы.

Начнем с изучения автоматических считывателей номерных знаков (ALPR) – камер, которые все чаще устанавливаются на полицейских машинах, а также в стационарных точках и на частных транспортных средствах. Когда такое устройство установлено на полицейском автомобиле, оно автоматически фиксирует каждый номерной знак, мимо которого этот автомобиль проезжает. Если полиция подозревает, что некая машина использовалась для совершения преступления, устройство легко ее обнаружит – и это хорошо. Но таким же образом в базу данных, разумеется, попадают номера автомобилей, в отношении которых подобных подозрений нет. По сути, это позволяет полиции вести детальный учет того, куда вы едете и когда, сколько там находитесь и куда движетесь дальше.

Эти устройства отслеживают ваши передвижения в общественных местах – никто не заглядывает к вам в дом сквозь занавески и не слушает телефонные разговоры. Но если бы у вас на улице круглые сутки стоял полицейский, изо дня в день записывая номера проезжающих автомобилей, вы бы его заметили. При этом вашему местному управлению полиции пришлось бы решить, что назначение офицеров на двадцать четыре часа в сутки для выполнения этой задачи явля-

ется оправданным использованием ресурсов. Система ALPR делает то же самое легко, незаметно и дешево.

Изображения номерных знаков часто попадают в базы данных, которыми пользуются несколько полицейских подразделений. Эти базы пополняются частными компаниями ALPR. Кто должен иметь право доступа к такой базе и в каких случаях? Какие меры безопасности ей необходимы? Что происходит в случае утечки данных? И еще более важный вопрос: имеем ли мы право заявить протест или просто вынуждены мириться с тем, что отныне полиция фиксирует все наши передвижения?

Затем в книге рассматриваются нательные камеры и камеры мобильных телефонов, которые дают полиции и гражданам новые способы смотреть друг на друга. Нательные камеры рекламировались как инструмент для обеспечения прозрачности: если раньше после спорной встречи полиции и гражданина судья изучал их противоречивые устные показания, теперь он может полагаться на видеодоказательства. Но кто решает, когда включать камеру? Что она показывает на самом деле и что упускает из виду? Что происходит с отснятым материалом? Кто может его видеть, сколько он хранится и с какими гарантиями? Кто решает, когда его удалять? И как его могут использовать? Это не академический вопрос: что происходит, когда по пути на акцию протеста вы минуете полицейского, а у него на одежде закреплен видеорегистратор с приложением для распознавания лиц?

В следующей главе обсуждаются дроны, которые дают полиции всевидящее небесное око. Более удобных технологий на свете почти нет. Дроны могут летать над пожарами, и при этом никакой пилот не рискует жизнью и здоровьем. Оснастите дрон термочувствительной камерой – и он безошибочно отыщет людей, заблудившихся зимой где-то в глуши. Но дроны могут с такой же легкостью подвергнуть город, как вы читали выше, постоянному наблюдению. И их несложно вооружить.

Затем я рассматриваю электронный мониторинг – технологию, которую большинство граждан знает как *мониторы на лодыжках*. Эта технология открывает огромные перспективы в качестве альтернативы тюремному заключению как для осужденных, так и для лиц, ожидающих суда (что политически более оправданно): людям лучше оставаться дома, поддерживать связь с семьей и, возможно, даже ездить каждый день на работу с разрешения суда, чем месяцами сидеть в криминогенной тюрьме. Но даже в качестве досудебной альтернативы тюрьме электронный мониторинг подвергает людей, еще не осужденных за преступления, постоянному и обременительному государственному надзору.

В книге исследуется распознавание лиц – из всех технологий, о которых я писал, оно, вероятно, представляет собой самую опасную и долговременную угрозу. Когда я начал свое исследование, распознавание лиц все еще было чем-то вроде журавля в небе, по крайней мере, для широкой публики. Се-

годня оно применяется в аэропортах и полицейских управлениях, оно стало частью китайской архитектуры контроля и репрессий. Его все чаще запрещают. Поначалу это казалось мне паникерством – теперь представляется здравым смыслом.

Затем я описываю алгоритмы, используемые в работе полиции и призванные предсказывать, где и когда произойдет преступление, а также алгоритмы, используемые судами при вынесении приговоров и призванные предсказывать, насколько велик риск повторного совершения преступления. Сторонники использования первых алгоритмов говорят, что система помогает им лучше распределять патрульные силы. Сторонники вторых утверждают, что она устраняет человеческий фактор при вынесении приговоров и принятии решений о предварительном заключении под стражу: судья, который, сознательно или нет, предвзято относится к подсудимым определенной этнической принадлежности, больше не сможет действовать в соответствии с этим предубеждением.

Но алгоритмы работают непрозрачно и опираются на данные, которые десятилетиями собирают люди со всей их предвзятостью. Они даже не пытаются избавиться от предубеждений, напротив, есть риск, что они зацементируют свои жесткие концепции во имя науки и объективности, и это лишь усложнит борьбу с шаблонными подходами.

В книге рассматривается шифрование и инструменты, которые помогают его обойти и тем самым лишают смысла за-

щиту конфиденциальности. Правительства и полиция часто утверждают, что им нужен *черный ход* к зашифрованным коммуникационным сервисам, таким как WhatsApp и Signal: плохие парни не должны иметь возможности хранить свои сообщения в секрете. Но ослабление защиты конфиденциальности подозреваемых ослабляет ее для всех нас.

И когда полиция сможет применять эти инструменты? Когда они начнут использовать Stingray, систему сбора метаданных всех телефонов на определенной территории? Полицейские будут применять эти средства, чтобы подслушивать тех, кого у них есть веские основания подслушивать. Но что происходит с остальными нашими данными, попавшими в эту сеть?

Я также разбираюсь в том, что может случиться, когда все эти технологии будут объединены и переданы в руки правительства, которое мало заботится о гражданских свободах своих граждан. Я не смог сделать репортаж из Китая по причинам, которые объясню позже, и поэтому отправился в Эквадор, чтобы изучить созданную китайцами систему управления чрезвычайными ситуациями, централизующую потоки с тысяч камер по всей стране. Она позволяет полиции, пожарным частям и станциям «скорой помощи» лучше реагировать на чрезвычайные ситуации. Но она так же эффективно осуществляет централизованный мониторинг: с ее помощью правительство может шпионить практически за кем угодно, в любое время и в любом общественном месте.

И, наконец, я расскажу о том, что сделали жители одного города – Окленда в штате Калифорния – для защиты своих гражданских свобод и налаживания более продуктивных отношений с полицией города. Их пример, я надеюсь, составляет сердцевину книги.

Некоторые могут обвинить меня в попытках запугивания. Виноват. Вероятно, вы напуганы. Но я хочу не только напугать вас. Я хочу, чтобы вы начали действовать – использовать доступную вам демократию наиболее эффективным способом. Полицейское государство уже здесь, и мы должны его остановить.

В конечном счете эта книга не столько о технологиях, сколько о демократии. Меня в меньшей степени интересует, как функционируют различные технологии наблюдения, и в большей – опасность, которую они представляют для граждан открытых либеральных демократий. Писать книгу о технологиях – дело рискованное, потому что они быстро устаревают, их вытесняют с рынка новые достижения. Но я верю, что мой основной тезис защитит эту книгу от такой судьбы, по крайней мере на какое-то время. Я хочу предоставить гражданам эвристику, структуру и инструменты, необходимые, чтобы в обозримом будущем решительно разобраться с технологиями наблюдения в любой их форме.

Надеюсь, во время чтения вы будете помнить о трех показателях для оценки новых технологий.

Во-первых, подумайте, на кого новая технология возлага-

ет *ответственность* за принятие решений. Если перед посадкой в самолет агент службы безопасности выводит вас из очереди в аэропорту для повторного обыска, вы знаете, кто принял это решение, и можете спросить, почему. Если то же самое делает машина, использующая распознавание лиц, – кто, в конце концов, решил, что вы должны пройти дополнительную проверку?

Если за несколько лет выяснится, что машины распознавания лиц в аэропорту города N отбирают для вторичного досмотра непропорционально большое количество людей с определенным цветом кожи – кто в этом виноват? Авиакомпания, использующая систему? Агенты, которые следуют рекомендациям машин? Программисты, создавшие алгоритм? Будут ли они все переводить стрелки друг на друга? Если пассажирка считает, что с ней обошлись несправедливо, к кому ей обращаться за возмещением ущерба?

Могут ли авиакомпании и агенты просто обвинять алгоритм? Если да, что происходит в этом случае? Технологические фирмы часто считают свои алгоритмы коммерческой тайной и опасаются, что раскрытие данных поставит их в невыгодное положение по отношению к конкурентам или позволит преступникам обмануть систему. Последнее всегда казалось мне крайне неправдоподобным: покажите мне грабителя или автоугонщика, который сознательно меняет *охотничьи угодья*, поскольку знает, какие районы полицейский алгоритм прогнозирования ежедневно помечает

как требующие особого внимания.

Что имеют право знать граждане об алгоритмах, решающих их судьбу? На мой взгляд, они должны получать очень много информации. Но значительная часть технологических компаний с этим не согласится, и до сих пор ни один механизм не заставил их открыть карты.

Во-вторых, подумайте, как влияет каждая новая технология на наши права и ожидания в отношении конфиденциальности. Какую информацию она собирает и как; как хранятся данные, кто может их видеть; кто может принять решение об использовании этой технологии и кому он подотчетен?

Stingray – это устройство, которое имитирует в сети базовую станцию (БС) сотовой связи, обманывая все телефоны в округе и заставляя подключаться к нему, а не к настоящей БС. Затем Stingray определяет уникальный абонентский номер каждого телефона и, следовательно, его владельца, а также местоположение, номера, на которые он звонит, номера, с которых звонят ему, и длительность соединения. Stingray также перехватывает текстовые сообщения и изучает активность человека в интернете, например, веб-сайты, на которые он заходит. Эти устройства полиция использует без ордера, хотя, например, изучить историю просмотров на вашем ноутбуке или заглянуть в ваш почтовый ящик без ордера невозможно.

Данные автоматических считывателей номерных знаков включают время и место создания изображений. Многие

управления полиции загружают эти фотографии в общие базы данных, где они хранятся рядом с кадрами, отснятыми другими полицейскими управлениями или частными лицами, например коллекторами. Федеральные и местные управления полиции со всей страны могут видеть, где бывал ваш автомобиль за последние несколько лет.

За исключением нескольких городов, обладающих развитой и надежной сетью общественного транспорта, который позволяет людям жить без автомобилей, в прочих местах эти снимки дают детальную картину жизни людей: куда они ездят, когда и как часто. Эти данные показывают, кому мы молимся, кого навещаем, где делаем покупки, к каким врачам ходим. Некоторые агентства годами хранят эти изображения у себя и даже в базах общего доступа. Полиции не нужны ордера, чтобы делать такие фотографии, в конце концов, съемка осуществляется в публичных местах, когда вы почти или совсем не ожидаете конфиденциальности. Кроме того, органам не всегда требуются какие-то особые основания для получения доступа к этим базам данных.

Конец ознакомительного фрагмента.