Хакер - Цифровой паноптикон. Настоящее и будущее тотальной слежки за пользователями
nopaywall

https://t.me/nopaywall
Андрей Письменный

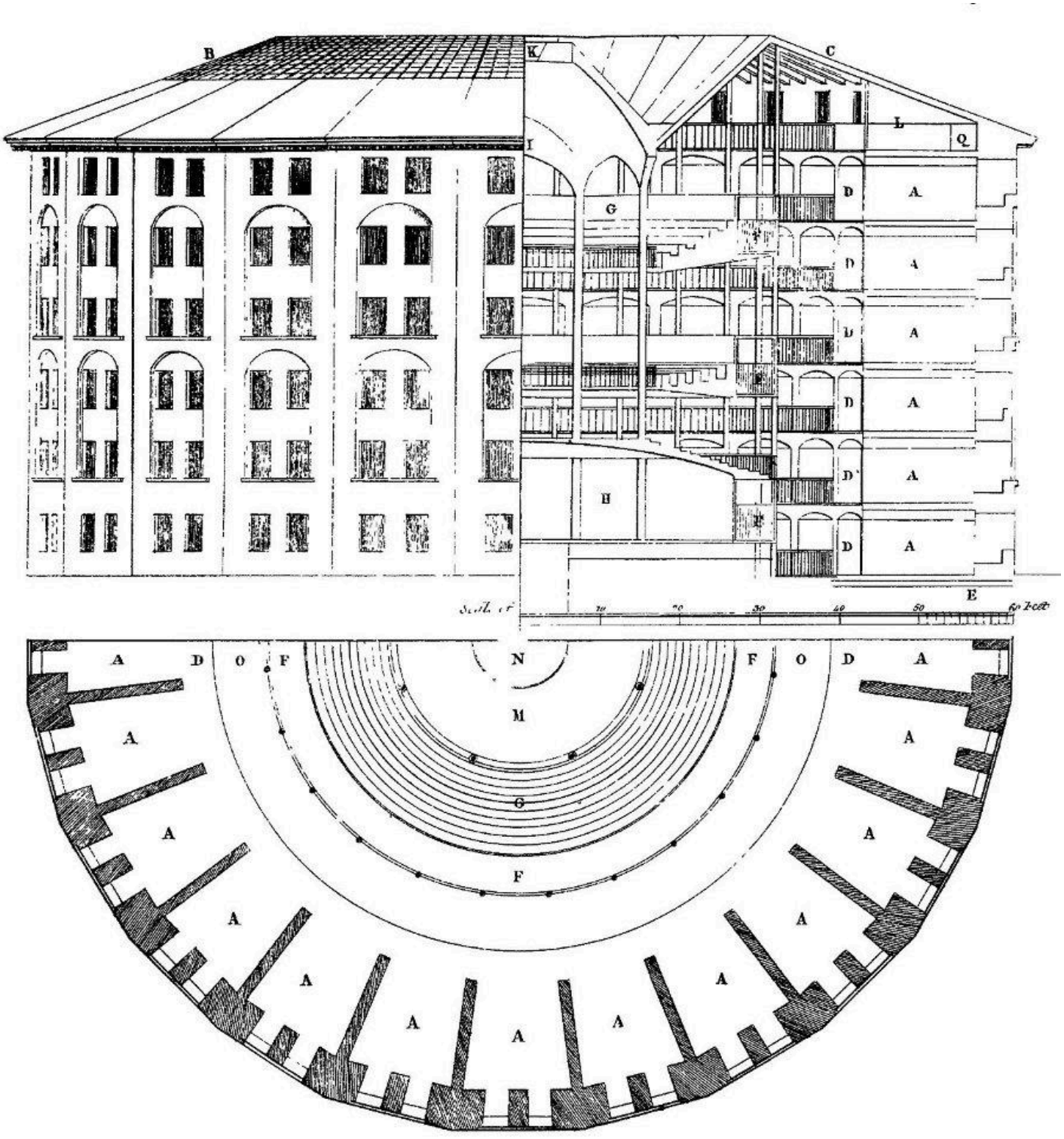
Содержание статьи

Даже если ты тщательно заботишься о защите своих данных, это не даст тебе желаемой приватности. И чем дальше, тем больше у компаний и правительств возможностей собирать и использовать самую разную информацию, а уж идентифицировать по ней человека — вообще не проблема. На нескольких занятных примерах мы разберем, как это происходит и к чему потенциально может привести.

Тот самый паноптикон

Начнем мы не с современности, а с восемнадцатого века, из которого к нам пришло слово «паноптикон». Изначально его придумал изобретатель довольно странной вещи — тюрьмы, в которой надзиратель мог постоянно видеть каждого заключенного, а заключенные не могли бы видеть ни друг друга, ни надзирателя. Звучит как какой-то мысленный эксперимент или философская концепция, правда? Отчасти так и есть, но

автор этого понятия британец Джереми Бентам был настроен предельно решительно в своем стремлении построить паноптикон в реальности.



Бентамовские чертежи паноптикона

Бентам был буквально одержим своей идеей и долго упрашивал британское и другие правительства дать ему денег на строительство тюрьмы нового типа. Он считал, что непрерывное и незаметное наблюдение положительно скажется на исправлении заключенных. К тому же такие тюрьмы было бы намного дешевле содержать. Под конец он уже и сам был готов стать главным надзирателем, но денег на строительство собрать так и не удалось.

Вдохновленная паноптиконом тюрьма на Кубе. Заброшена с 1967 года

С тех пор в разных странах было построено несколько тюрем и других заведений, вдохновленных чертежами Бентама. Но нас в этой истории, конечно, интересует другое. Паноптикон почти сразу стал синонимом для общества тотальной слежки и контроля. Которое, кажется, строится прямо у нас на глазах.

33 бита энтропии

Исследователь Арвинд Нараянан предложил полезный метод, который помогает измерить степень анонимности. Он назвал его «33 бита энтропии» — именно столько информации нужно знать о человеке, чтобы выделить его уникальным образом среди всего населения Земли. Если взять за каждый бит какой-то двоичный признак, то 33 бита как раз дадут нам уникальное совпадение среди 6,6 миллиарда.

Однако следует помнить о том, что признаки обычно не двоичны и иногда достаточно всего нескольких параметров. Возьмем для примера базу данных, где хранится почтовый индекс, пол, возраст и модель машины. Почтовый индекс ограничивает выборку в среднем до 20 тысяч человек — и это цифра для очень плотно населенного города: в Москве на одно почтовое отделение приходится 10 тысяч человек, а в среднем по России — 3,5 тысячи.

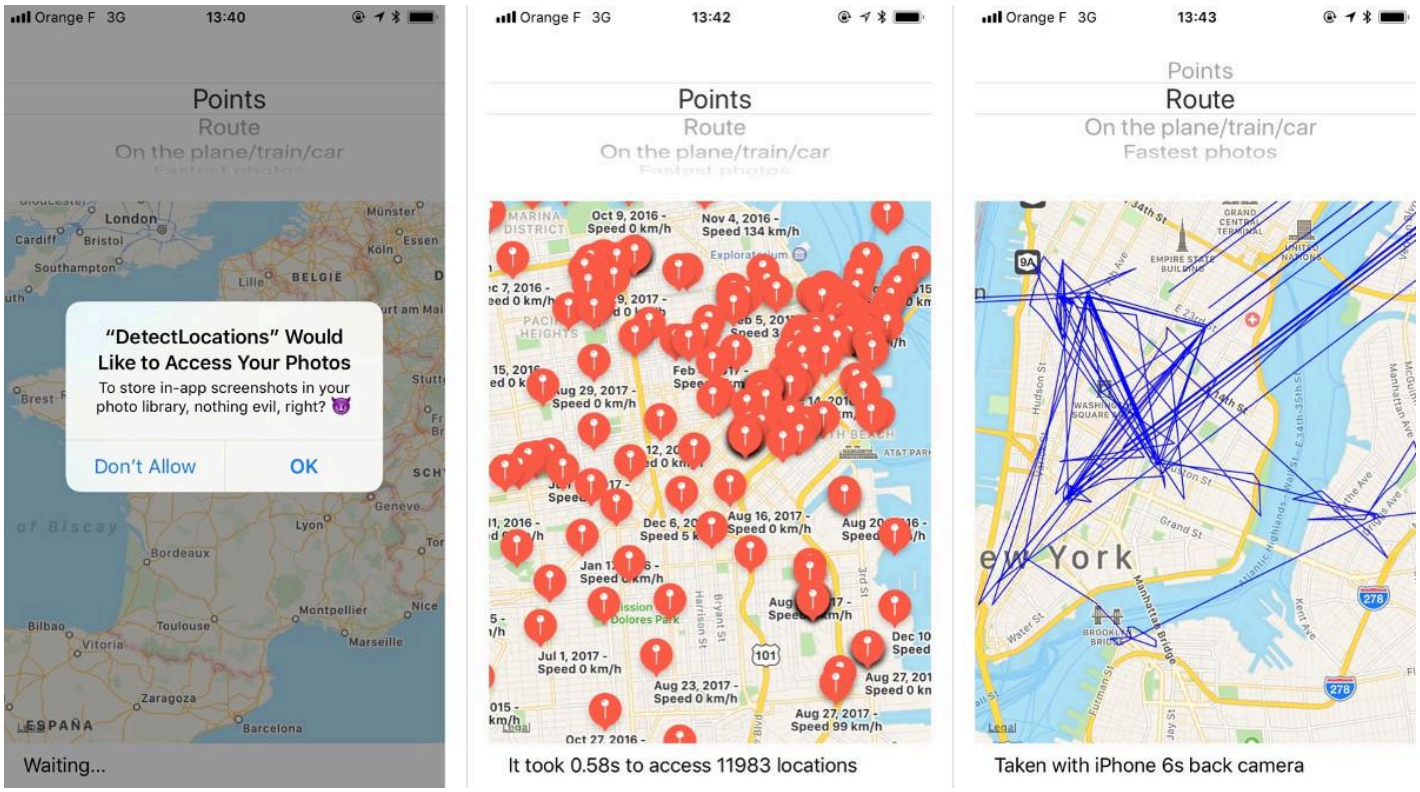
Пол ограничит выборку вдвое. Возраст — уже до нескольких сотен, если не десятков. А модель машины — всего до пары человек, а зачастую и до одного. Более редкая машина или мелкий населенный пункт могут сделать половину параметров ненужными.

Скрипты, куки и веселые трюки

Вместо почтового индекса и модели машины можно использовать версию браузера, операционную систему, разрешение экрана и прочие параметры, которые мы оставляем каждому посещенному сайту, а рекламные сети усердно все это собирают и с легкостью отслеживают путь, привычки и предпочтения отдельных пользователей.

WWW

Подробнее о методах фингерпринтинга (не путать с фингерингом) читай в статьях «Тотальная слежка в интернете — как за тобой следят и как положить этому конец» и «Фингерпринтинг браузера. Как отслеживают пользователей в Сети». Также можешь проверить свой браузер при помощи Am I Unique — мы также писали о нем и о схожих сервисах. Узнаешь много интересного!
Или вот другой занятный пример, уже из мира мобильных приложений. Каждая программа для iOS, которая получает доступ к фотографиям (например, чтобы наложить на них красивый эффект), имеет возможность за секунды просканировать всю базу и засосать метаданные. Если фотографий много, то из данных о геолокации и времени съемки легко сложить маршрут твоих перемещений за последние пять лет. Proof of concept можешь посмотреть в репозитории Феликса Краузе.



detect.location

Существуют и более известные, но при этом не менее неприятные вещи. Например, многие счетчики посещаемости вроде «Яндекс.Метрики» позволяют владельцам сайта, помимо прочего, записывать сессию пользователя — то есть писать каждое движение мыши и нажатие на кнопку. С одной стороны, ничего нелегального тут нет, с другой — стоит посмотреть такую запись своими глазами, и понимаешь, что тут что-то не так и такого механизма существовать не должно. И это не считая того, что через него в определенных случаях могут утечь пароли или платежные данные.

И таких примеров масса — если ты интересуешься темой и читаешь «Хакер» дольше пары месяцев, то сам без труда припомнишь что-нибудь в этом духе. Но гораздо сложнее понять, что происходит с собранными данными дальше. А ведь жизнь их насыщенна и интересна.

Торговцы привычками

Многие собираемые данные на первый взгляд кажутся безобидными и зачастую обезличены, но связать их с человеком не так сложно, как представляется, а безобидность зависит от обстоятельств. Как думаешь, насколько безопасно делиться с кем-то ну, например, данными шагомера? По ним, в частности, легко понять, во сколько тебя нет дома и по каким дням ты возвращаешься поздно.

Однако грабители пока что до столь высоких технологий не дошли, а вот рекламщиков любая информация о твоих привычках может заинтересовать. Как часто ты куда-то

ходишь? По будням или по выходным? Утром или после обеда? В какие заведения? И так далее и тому подобное.
Только в США, по подсчетам журнала Newsweek, существует несколько тысяч фирм, которые занимаются сбором, переработкой и продажей баз данных (гиганты индустрии — Acxiom и Experian оперируют миллиардными оборотами). Их основной продукт — это разного рода рейтинги, которые владельцы бизнесов могут купить и в готовом виде использовать при принятии решений.
В желающих продать данные тоже нет недостатка. Любой бизнесмен, узнавший, что можно сделать немного денег из ничего, как минимум заинтересуется. И не думай, что главное зло здесь — бездушные корпорации. Стартапы в этом плане чуть ли не хуже: сегодня в них работают прекрасные честные люди, а завтра может остаться только пара циничных менеджеров, пускающих с молотка последнее имущество.
Автор Newsweek отмечает важный момент: данные, собираемые брокерами, часто содержат ошибки и рейтинг может выйти неверным. Так что если кому-то вдруг откажут в кредите или не захотят принимать на работу, то, возможно, ему стоит винить не себя, а безумную систему слежки, стихийно возникшую за последние пятнадцать лет.

Твой теневой профиль

В большинстве стран центр общественной жизни в онлайне — это Facebook, поэтому и разговоры о приватности в Сети часто крутятся вокруг него.
На первый взгляд может показаться, что Facebook неплохо заботится о сохранности личных данных и предоставляет массу настроек приватности. Поэтому технически подкованные люди часто списывают со счетов страхи и жалобы менее образованных в этом плане товарищей. Если кто-то случайно поделился с миром тем, чем делиться не хотел, значит, виноват сам — надо было вовремя головой думать.
В реальности Facebook и правда заботится о сохранности личных данных, но это скорее утверждение вроде известного в СССР афоризма «Нам нужен мир, и по возможности весь». Как и многие социальные сети и мессенджеры, Facebook пытается захватить и сохранить столько личных данных, сколько получится. Иногда последствия этого вырываются наружу.
Показательно исследование, которое недавно предприняла репортер Gizmodo Кашмир Хилл. Она искала пользователей Facebook, которые увидели в разделе «Вы можете знать этих людей» кого-то, кого не должны были видеть, или наоборот — их профиль труднообъяснимым образом попался кому-то малознакомому.
Среди примеров Хилл приводит:

- социального работника, которого клиент на второе посещение стал внезапно называть по прозвищу, хотя они не обменивались никакими данными;
- женщину, чей отец бросил семью, когда ей было шесть лет. Facebook посоветовал ей добавить в друзья любовницу, к которой он и ушел сорок лет назад;
- адвоката, который рассказал, что в ужасе удалил свой аккаунт, когда среди рекомендаций встретил члена защиты по недавнему делу, а с этим человеком он взаимодействовал только по рабочей почте, не привязанной к «Фейсбуку».

Удалить аккаунт в Facebook — это решительный, но в данном случае лишь ограниченно полезный шаг. Не сомневайся, что социальная сеть продолжит хранить все данные и использовать их для построения скрытого социального графа.
Причина всех перечисленных случаев одна: алгоритмы Facebook успешно связали воедино кусочки когда-то кем-то оставленной информации. Предположим, у одного твоего знакомого есть только твой номер телефона, а у другого — только имейл. Они оба дали «Фейсбуку» просканировать адресную книгу. Таким образом телефон и почта будут ассоциированы друг с другом. А также со всеми твоими телефонами, адресами, номерами в инстант-мессенджерах, никнеймами, которыми ты когда-либо пользовался и кому-то давал.

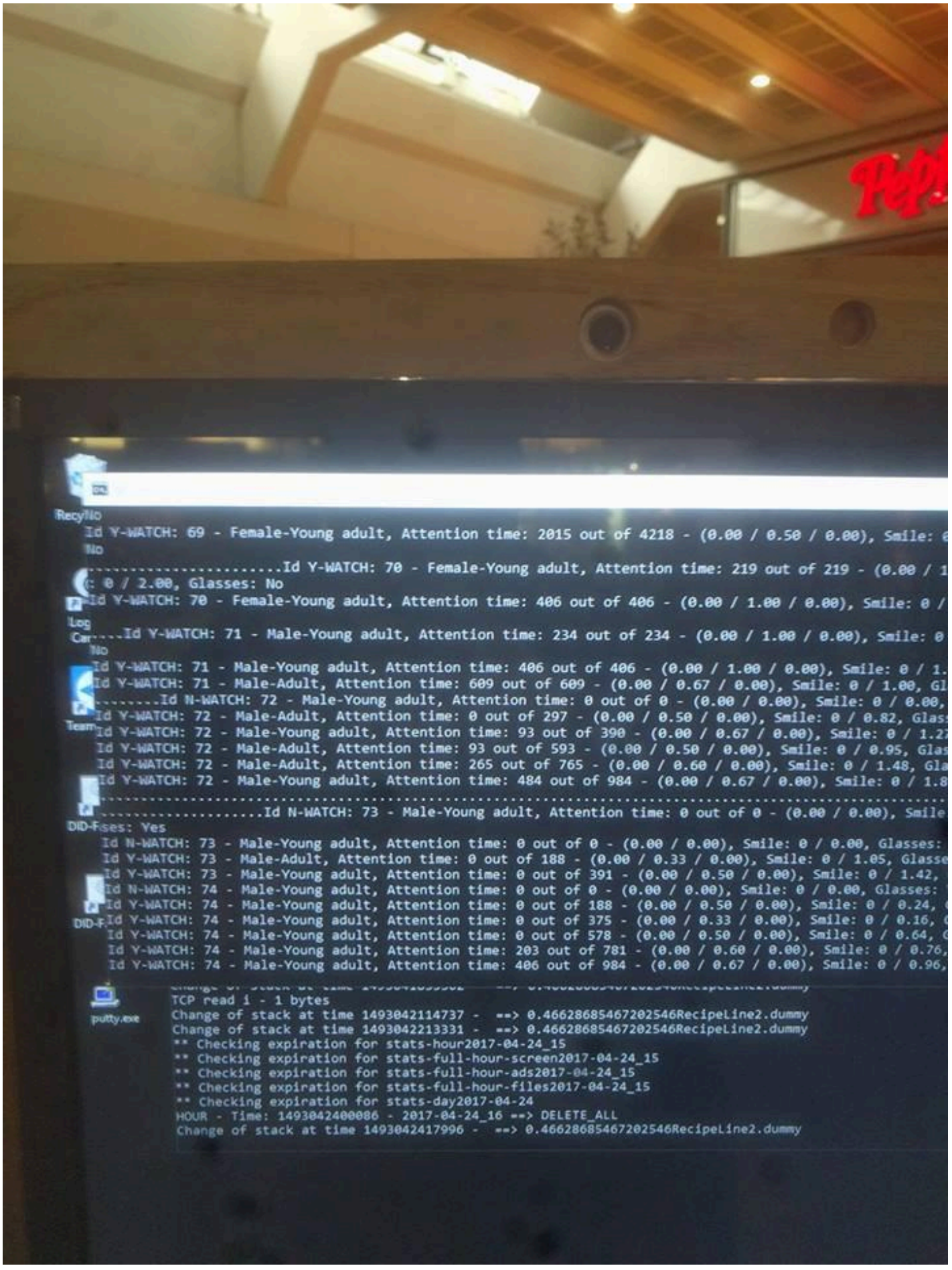
INFO

Похожее поведение было замечено и за «Телеграмом». Вот такой парадокс: мессенджер, который, с одной стороны, предоставляет удобные средства шифрования, с другой — не забывает сам захватить все, до чего дотянется.
Еще веселее то, что у «Фейсбука» уже так много данных, что, даже если отдельный человек никогда не имел аккаунта, его профиль все равно можно составить из информации, которую непрерывно оставляют другие люди. А «можно» в таких случаях значит, что так оно наверняка и происходит. Если алгоритмы соцсети увидят информационную дыру в форме человека, то они будут иметь ее в виду и дополнять новыми деталями.
Сотрудники Facebook страшно не любят словосочетание «теневой профиль». Конечно, приятно думать, что они просто собирают данные, которые помогут людям найти старых друзей, возобновить утерянные деловые контакты и все в таком духе. Чуть менее приятно — помнить о том, что все это делается ради того, чтобы более эффективно продавать рекламу. А уж постоянно воображать случаи шантажа, мести или мошенничества и вовсе не хочется.

Нам при этом совершенно не важно, чего хотят Цукерберг и его сотрудники. Да, скорее всего, он жалеет, что на заре своей карьеры назвал первых пользователей Facebook обидными словами dumb fucks за то, что те оставляли на его сайте личные данные. Но изменились ли с тех пор его взгляды на жизнь? И более важный вопрос — не становятся ли его слова все более правдивыми?

Не очень отдаленное будущее

Еще десять-пятнадцать лет назад все, о чем мы тут говорили, либо не существовало, либо не волновало большинство людей. Сейчас реакция публики потихоньку меняется, но, скорее всего, недостаточно быстро, и следующие десять-пятнадцать лет в плане приватности обещают стать крайне неприятными (или неприватными?).
Если сейчас следить проще всего в интернете, то с миниатюризацией и удешевлением электроники те же проблемы постепенно доберутся и до окружающего нас мира. Собственно, они уже потихоньку добираются, но это только начало.

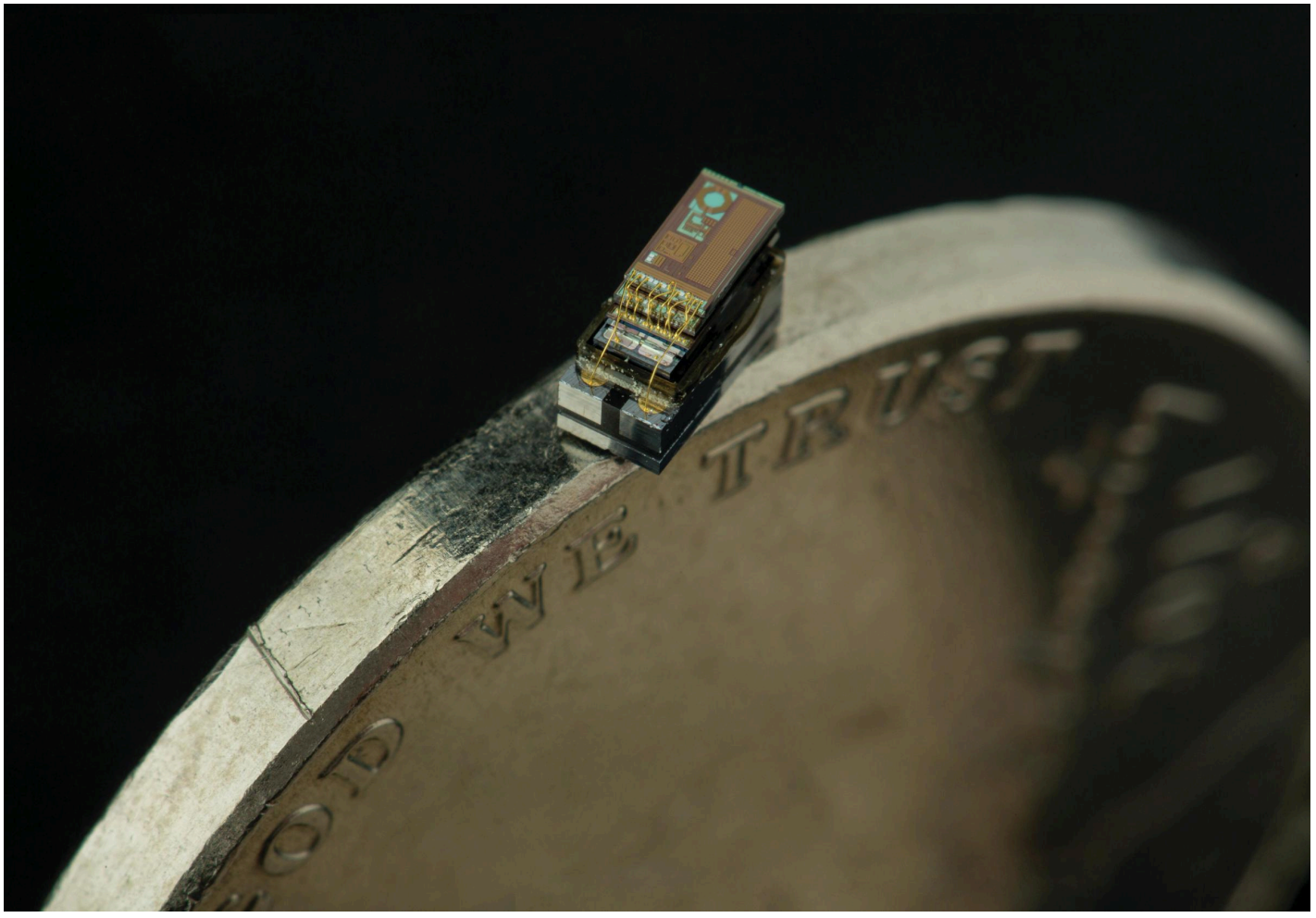


Недавно все охали и ахали от фотографии сглючившего рекламного стенда в пиццерии, который детектил лица. Волноваться надо было, когда эту штуку возили по выставкам

В статье «How low (power) can you go?» писатель Чарли Стросс отталкивается от закона Куми (вариации закона Мура, которая говорит, что энергоэффективность компьютеров удваивается каждые 18 месяцев) и рассчитывает минимально потребляемую мощность компьютеров 2032 года.

По грубым прикидкам Стросса выходит, что аналог нынешних маломощных мобильных систем на чипе с набором сенсоров через пятнадцать лет сможет питаться от солнечной батареи со стороной два-три миллиметра либо от энергии радиосигнала. И это без учета того, что могут появиться более эффективные батареи или другие способы доставки энергии.

Стросс рассуждает дальше: «Будем считать, что наш гипотетический компьютер с низким энергопотреблением при массовом производстве будет стоить 10 центов за штуку. Тогда покрыть Лондон процессорами по одному на квадратный метр к 2040 году будет стоить 150 миллионов евро, или 20 евро на человека». Столько же власти Лондона за 2007 год потратили на отдирание жвачки от дорог, так что вряд ли такой проект окажется городу не по карману.



Michigan Micro Mote — прототип крошечного компьютера с солнечной батареей. И это технологии 2015 года, а не 2034-го

Дальше Стросс обсуждает выгоды, которые может дать компьютеризация городских поверхностей, — от суперточных прогнозов погоды до предотвращения эпидемий. Рекомендую почитать со всеми подробностями, но в рамках этой статьи нас, конечно,

интересует другое: тот уровень тотального наблюдения, который может дать эта почти что «умная пыль» из научной фантастики.
«Носить худи уже не поможет», — с сарказмом отмечает Стросс. И действительно: даже если у вездесущих сенсоров не будет камер, они все равно смогут считывать каждую метку RFID или идентифицировать мобильные устройства с модулями связи. Да и собственно, почему не будет камер? Крошечные объективы, которые можно производить сразу вместе с матрицей, уже сейчас создаются в лабораторных условиях.

Память толпы

То, к чему может потенциально привести распыление компьютеров ровным слоем по окружающей местности, Стросс называет словами panopticon singularity — по аналогии с технологической сингулярностью, которая подразумевает бесконтрольное распространение технологий. Это иная техногенная страшилка, которая означает повсеместное наблюдение и, как следствие, несвободу.
Можно вообразить, до каких крайностей дойдет, если технологии массовой слежки попадут в руки диктаторскому режиму или религиозным фундаменталистам. Однако даже если представлять, что такую систему будет контролировать обычное, не особенно коррумпированное и не слишком зацикленное на традиционных ценностях правительство, все равно как-то не по себе.
Другой потенциальный источник повсеместной слежки — это сами люди. Вот краткая история этой технологии:

- версия 1.0 — старушки у подъезда, которые всё про всех знают;
- версия 2.0 — прохожие, которые чуть что выхватывают из карманов телефоны, фотографируют и постят в соцсети;
- версия 3.0 — постоянно включенные камеры на голове у каждого.

Автомобильные видеорегистраторы, кстати, — это уже где-то 2.5. Как говорится, «вы находитесь здесь».
Поводы нацепить на голову камеру могут быть разные — например, стримить в Periscope или Twitch, пользоваться приложениями с дополненной реальностью или просто записывать все происходящее, чтобы иметь цифровую копию, к которой можно в любой момент обратиться за воспоминанием. Последнее применение называется «лайфлоггинг», я о нем уже подробно писал в «Хакере» три года назад.
Один из главных теоретиков лайфлоггинга — старший исследователь Microsoft Research Гордон Белл. В своей последней книге Your Life Uploaded Белл рассуждает о разных аспектах жизни общества, где все имеют документальные свидетельства всего

произошедшего. Белл считает, что это хорошо: не будет преступлений, не будет невинно наказанных, а люди смогут пользоваться сверхнадежной памятью машин.
А как же приватность? Можно ли в мире будущего сделать что-то втайне от других? Белл считает, что система должна быть построена таким образом, чтобы в любой момент можно было исключить себя из общественной памяти. Нажимаешь волшебную кнопочку, и право смотреть запись с тобой останется, к примеру, только у полиции. Удобно, правда?
Вот тут-то и понимаешь по-настоящему, где заканчивается та дорога, на которую встал Facebook со своими теневыми профилями. Если все будет как сейчас и люди продолжат радостно загружать свои данные, то волшебная кнопка выпадения из общей памяти просто ни на что не повлияет. Ну исключил ты себя, а интеллектуальный алгоритм тут же связал все обратно из косвенных признаков.

Что делать

…чтобы не наступило мрачное будущее, от которого вздрогнул бы даже Джордж Оруэлл?
Все мы думаем, что, наверное, кто-то там как-то, возможно, об этом позаботится. Активисты должны сказать «нет», правительства должны ввести законы, исполнительная власть — проследить, ну и так далее. Увы, истории известна масса случаев, когда эта схема неслабо сбоила.
Правительственные инициативы действительно есть — смотри, например, европейский GDPR — общий регламент по защите данных. Это постановление регулирует сбор и хранение личной информации, и с ним Facebook уже не отделается щадящим (с учетом гигантских оборотов) штрафом в 122 миллиона евро. Отваливать придется уже 4% от выручки, то есть как минимум миллиард.
Первый этап GDPR стартует 25 мая 2018 года. Тогда-то мы и узнаем, какие у него побочные эффекты, какие обходные маневры последуют и удастся ли в реальности чего-то добиться от транснациональных корпораций. В России уже имеется не самый успешный опыт с законом «О персональных данных». Характерно, что его скромные успехи мало кого печалят («пусть лучше следят Цукерберг и Пейдж с Брином, чем товарищ полковник»).
Да и в целом есть серьезные подозрения, что правительства хотят не столько пресечь слежку, сколько приложиться к ней, а в идеале — вернуть себе монополию. Так что гораздо лучше было бы, начни корпорации сами себя одергивать и регулировать. Увы, как мы видим на примере «Фейсбука», некоторые из них работают в ровно противоположном направлении.

Можем ли мы сделать что-то сами, кроме как судорожно пытаться скрыться, зашифровать, обфусцировать и поотключать все на свете? Я предлагаю начать с главного — стараться никогда не махать рукой и не говорить: «Ай, все равно все следят!» Не все равно, не все и не с одинаковыми последствиями. Это важно.