Спутник и Погром - Криптохранители: интервью Павла Дурова о том, как на него давило ФБР (и как оно продавило других крипто-активистов в США). Перевод The Baffler
nopaywall

https://t.me/nopaywall
Александр Заворотний

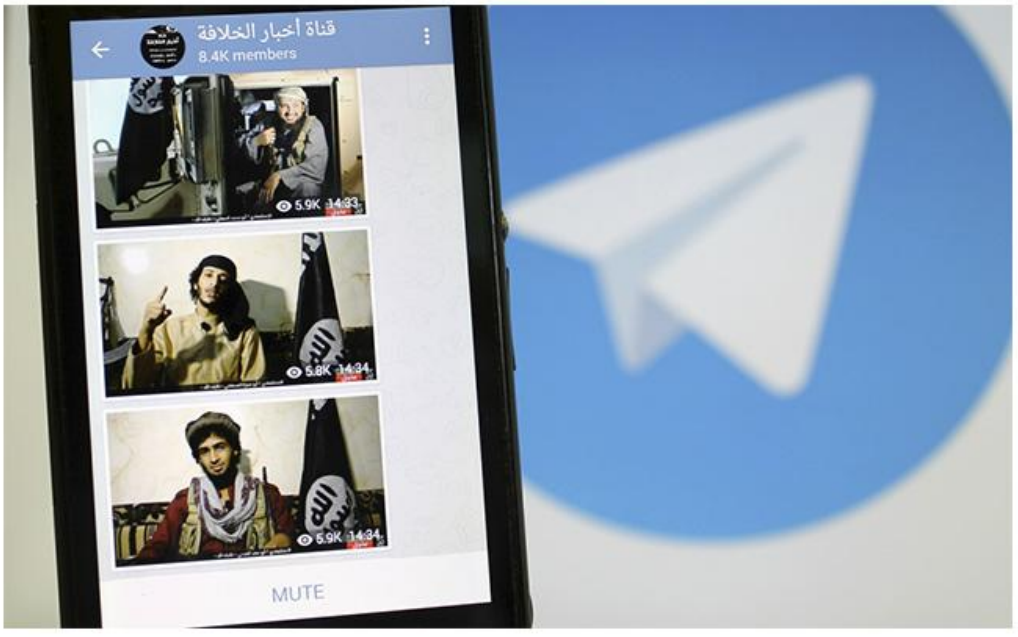
Полвосьмого вечера, понедельник, июнь, где-то в Северной Европе. Я сижу в банкетном зале престижного отеля и разговариваю с Павлом Дуровым — «русским Марком Цукербергом», молодым интернет-магнатом, который создал самую популярную социальную сеть в стране, а потом был вынужден уступить её Кремлю — и всё это в возрасте до 30 лет. Вскоре после того как знаменитый американский разоблачитель Эдвард Сноуден бежал в Россию, спасаясь от преследования, Дуров предложил ему работу, но потом и сам был вынужден покинуть страну из-за конфликта с российским правительством. Из-за ссоры с Кремлём его поначалу сочли кибердиссидентом, но впоследствии Дуров привлёк к себе настойчивое и агрессивное внимание американских спецслужб.

Группа богатых туристов толчётся в вестибюле, оживлённо болтая о достопримечательностях и музеях. Наша же беседа носит более мрачный характер. Мы с Дуровым говорим о смутном параноидальном мире, в котором живут одержимые криптобезопасностью сторонники неприкосновенности частной информации — мире, где правит шпионаж, всё не такое, каким кажется, а доверять нельзя никому.

Паранойя меня не удивляет. Последние три года я исследовал истоки инструментов кибербезопасности, ставших основой нынешнего могущественного движения за неприкосновенность информации в интернете: анонимайзеров, приложений для зашифрованного обмена сообщениями, неотслеживаемых облачных хранилищ для «борцов за правду» и сверхнадёжных операционных систем, которые, по слухам, не может взломать даже американское Агентство национальной безопасности. Они пользуются доверием журналистов с Пулитцеровской премией, хакеров, разоблачителей, а также всем известных людей и организаций, борющихся за неприкосновенность информации — от Эдуарда Сноудена и Фонда электронных рубежей (Electronic Frontier Foundation) до Американского союза гражданских свобод

(American Civil Liberties Union). Приложения вроде Tor и Signal обещают защитить пользователей от всевидящего американского аппарата слежки. А что же криптографы и программисты, разработавшее это «народное криптооружие»? Многие из них говорят, что ходят по краю бездны; это криптоанархисты, сражающиеся с властями, преследуемые и одолеваемые правительственными агентами невидимого фронта. Некоторые из них под предлогом преследований вовсе покинули Соединённые Штаты, отправившись в добровольную ссылку в Берлин.

Во всяком случае, так они видят сами себя. Моя же информация показывает иную действительность. Как мне удалось выяснить, копаясь в финансовой документации и запросах по Закону о свободе информации (FOIA), многие из этих самопровозглашённых онлайн-радикалов оказались военными подрядчиками на окладе того самого аппарата национальной безопасности США, с которым они якобы борются. Их бунтарские криптотехнологии при ближайшем рассмотрении тоже оказались самопальными «потёмкинскими деревнями» в мире безопасных цифровых коммуникаций. Более того: подобное программное обеспечение, как оказалось, финансировалось правительством США. Ежегодно Пентагон, Госдепартамент и масса организаций, раскрученных ЦРУ, выделяют крипторадикалам миллионы долларов. Изучение этого сообщества доставило мне массу проблем: военные подрядчики распространяли клевету и угрожали моей жизни и жизни моих коллег; СМИ публиковали высосанные из пальца истории о моём сексизме, а агенты ЦРУ платили за подрыв доверия к криптографии. Так что к своим источникам я уже давно научился подходить со скептицизмом и осмотрительностью — особенно к таким скандально известным, как Дуров, который попал в неприятную историю со своим Telegram, ставшим наиболее популярным приложением для обмена сообщениями в ИГИЛ.



Интернет-магнат в бегах

Дуров, попросивший меня скрыть место нашей встречи из-за конфликта с российским правительством, тоже осторожничал. И с полным на то правом.

Тридцатидвухлетний мультимиллионер — и, если верить СМИ, самый радикальный интернет-магнат России. В 2006 году, в возрасте всего 22 лет, он стал одним из основателей ВКонтакте, социальной сети по образцу и подобию Facebook'а, которая по популярности в России и бывших советских республиках превзошла сам Facebook.

Но компания недолго была под его контролем. В 2011 году, когда массовые протесты против правящей партии Владимира Путина стали возможными во многом благодаря координации через социальные сети, правительство решило ужесточить контроль над ВКонтакте. Дуров сопротивлялся и неоднократно устраивал акты неповиновения: публиковал фотографии документов, в которых от компании требовалось блокировать определённые политические группы, и открыто высмеивал ФСБ.

Но Кремль упорствовал и, в конечном итоге, добился своего. Дуров устал от огня на подавление, который вело российское государство, прибегая к различной тактике: полицейским налётам на квартиру Дурова; странному шантажу с, по его словам, поддельным видео, на котором он на чёрном Мерседесе сбивает гаишника; сфабрикованным обвинениям, которые заставили его уехать из страны. Так что в 2014 году молодой создатель соцсети был вынужден продать свои 20% ВКонтакте концерну, возглавляемому узбеком Алишером Усмановым, — жутковатым олигархом, преданным Владимиру Путину. Без своего детища Дуров уже не мог претендовать на роль Цукерберга в российской политике.

Он покинул Россию и, сделав стратегическое вложение денег в Сент-Китс и Невис, стал гражданином этой карибской страны. В последние три года он вёл жизнь независимого мультимиллионера, странствующего по земному шару и живущего в роскошных отелях, пренебрегая покупкой земли и недвижимости. Дуров мог делать всё, что заблагорассудится, так что в изгнании он со своим старшим братом Николаем работал над новым крупным проектом, тратя время и деньги — а его состояние оценивается примерно в 300 млн долларов — на разработку нового приложения для обмена сообщениями, Telegram.

У Telegram примерно 100 млн пользователей во всех странах мира, что вдесятеро меньше, чем у WhatsApp, его ближайшего конкурента, принадлежащего Facebook. Но Telegram добился успеха в довольно неожиданных местах: например, он крайне популярен в Иране и Узбекистане. В Европе у него тоже немало пользователей и растущее число поклонников из числа российских журналистов. Кроме того, Telegram приглянулся «Аль-Каиде» и ИГИЛ, которые считают его наиболее безопасным мессенджером из доступных на рынке. Эти террористические группировки используют зашифрованные чаты Telegram для координации нападений, а каналы — для распространения пропаганды, привлечения экстремистов-одиночек и сообщений об ответственности за удачные теракты. Telegram засветился в ходе терактов во Франции, Германии, Турции, и, в последнем случае, в родном для Дурова Санкт-Петербурге, где террорист-одиночка совершил взрыв на станции метро, который унёс жизни 15 человек и искалечил ещё многих.

Как понимать намёки

Неудивительно, что российское правительство вновь заинтересовалось Дуровым. Представители российских спецслужб оказывали на него давление, пытаясь заставить делиться информацией под угрозой блокировки сервиса. Но российское правительство не одиноко в попытках припереть Дурова к стене. Американцы тоже хотят в этом поучаствовать.

Пока официантка приносит тарелку с хлебом и закусками — нарезанным кальмаром и тартаром из тунца — Дуров объясняет, что в последние несколько лет ФБР пытается

заставить его пойти на тайное сотрудничество, причём дело дошло до подкупа одного из разработчиков. Ранее он никогда публично не упоминал о проблемах с ФБР.
Дуров говорит, что давление началось в 2014 году, вскоре после продажи доли ВКонтакте. Тогда агенты ФБР начали постоянно допрашивать его на американской границе. Иногда его задерживали для дополнительного допроса при въезде, иногда перехватывали его, чтобы «поболтать», пока он спешил на самолёт. Поначалу ФБР интересовала его работа над ВКонтакте и отношения компании с российскими спецслужбами, включая действия при получении от властей запроса на информацию. «Эти вопросы ставили меня в неловкое положение, — говорит Дуров, — становиться американским „кротом“ мне совершенно не хотелось, так что я ограничился самым минимумом информации, который уже был известен СМИ».

> Как они узнали адрес? — задаётся вопросом Дуров, — отследили сим-карту? Следовали за мной из аэропорта? Получили информацию от Uber? Не знаю

Позднее офицеры ФБР переключились на вопросы о Telegram. Где он расположен? Как работает? Как ФБР можно связаться с Дуровым в будущем? Агенты слали Дурову дружелюбные электронные письма, предлагая не стесняться обращаться к ним в случае каких-либо проблем или нужды в помощи. Все эти заигрывания Дуров игнорировал, но ФБР явно чего-то хотело. Вопрос только в том, чего именно. В 2016 году обнаружился ответ. В мае этого года он летел из Европы в Сан-Франциско на ежегодную конференцию Google I/O. В первое же утро, в восемь часов, два агента ФБР нанесли неожиданный визит в дом в Маунтин-Вью, который Дуров снял через Airbnb. «Как они узнали адрес? — задаётся вопросом Дуров. — Отследили сим-карту? Следовали за мной из аэропорта? Получили информацию от Uber? Не знаю».
Как бы там ни было, но оба агента явно действовали по заданию. «С порога они начали задавать вопросы о Telegram, и меня это обеспокоило», — говорит Дуров, объясняя, что непрошенным гостям не понадобилось много времени, чтобы перейти к сути дела:

им был нужен негласный канал для слива информации, чтобы получать от Telegram данные по тем или иным пользователям в случае террористической угрозы; агенты даже пришли уже с готовыми и вроде бы официальными документами. «Они показали постановление суда и заявили: “Мы весьма уважаем ваши взгляды на личную информацию и криптографию; уважаем то, над чем вы работаете. Но терроризм существует, он представляет собой серьёзную проблему, а на нас лежит долг по защите общества. Надеемся, что вы нас поймёте правильно. Мы хотим наладить процесс обмена информацией, чтобы получить от вас помощь в случае террористической угрозы”», — пересказывает Дуров. В ходе двадцатиминутного разговора агенты дали явно понять, что надеются на начало длительного и плодотворного сотрудничества.
Telegram зарегистрирован в Великобритании под названием Telegram Messenger LLP — в свою очередь, этой компанией владеют две другие, из Британских Виргинских островов и Белиза. Данные мессенджера тоже дробятся и распределяются по различным государствам — это часть общей стратегии Дурова, которая в теории позволит затруднить законный доступ к данным пользователей настолько, насколько это вообще возможно. На территории США Telegram юридически не присутствует, так что у ФБР нет законных оснований чего-либо требовать от Дурова или его компании. Дуров говорит, что понял: постановление суда было уловкой, чтобы заставить его сотрудничать, но он подыграл и пообещал, что свяжется с агентами после того, как юристы Telegram ознакомятся с документом.
Тем не менее, по словам Дурова, этот случай заставил его призадуматься. «В РФ ребята из ФСБ, с которыми я имел дело, на меня особого впечатления не произвели. Хватка у них так себе, профессионализм тоже не на высоте. В США же ФБР выглядит совсем иначе. Люди, говорившие со мной, были весьма компетентны. Говорили на нескольких языках. Они исследовали суть дела и точно знали, какие вопросы задавать. Одним словом, первоклассные специалисты. Тогда я понял, что Америка выделяет на безопасность такие средства, что это просто пугает. Американские спецслужбы намного более эффективны».

Найди крота

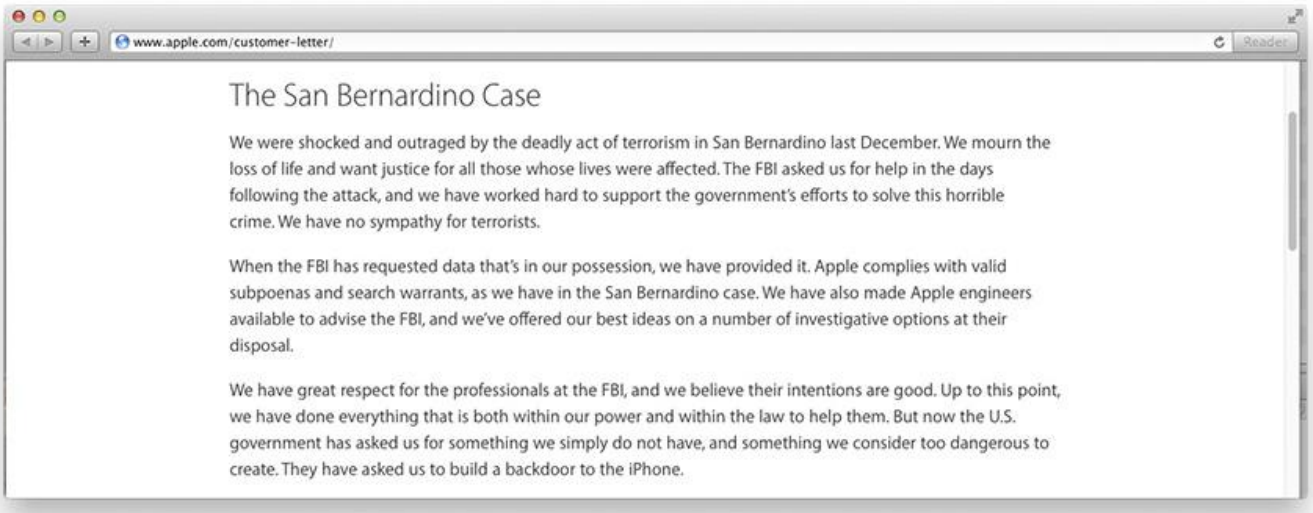
Агенты ФБР ушли, но забывать о них было нельзя. Как говорит Дуров, они взяли под прицел и разработчика Telegram, который прилетел на конференцию Google и остановился в том же доме в Маунтин-Вью, что и Дуров (пресс-секретарь ФБР отказался обсуждать подробности дела Дурова с изданием *The Baffler*).
В аэропорту агенты киберподразделения ФБР уже останавливали и допрашивали разработчика, но позднее ему назначили ещё одну встречу в одном из кафе Сан-Франциско. Агенты, встретившие разработчика, засыпали его общими вопросами об архитектуре Telegram и работе криптоалгоритма, при этом щедро расточая похвалы

за его глубокие познания. Вскоре дошло и до настоящей цели: получения доступа, за что они были готовы заплатить. Дуров не сообщил имя этого разработчика, но поделился историей, которую ему рассказал подчинённый. ФБР хотела заключить соглашение, по которому разработчик тайно передавал бы информацию о внутренних механизмах Telegram вроде новых функций и других компонентов архитектуры, могущих представлять интерес. Соглашение было бы сугубо конфиденциальным, а вознаграждение — высоким. «Для вас это определённо будет стоить того», — заявили они. По их словам, разработчик «консультировал» бы ФБР — не слишком завуалированный эвфемизм для очевидного подкупа. «Агенты ФБР намекнули на примерную сумму, — говорит Дуров, прожёвывая хлеб, — порядка десятков тысяч долларов».

После того как разработчик отказался от предложения, агенты встретились с ним ещё раз, попросив никому, и в особенности начальнику, не рассказывать об их разговоре. «Они были весьма прямолинейны, — замечает Дуров, — Павлу ничего не говори, это наша тайна».

Он пожимает плечами и улыбается. Кажется, сделка у ФБР сорвалась. «Своим разработчикам мы платим очень хорошо, — говорит Дуров в маленьком приступе начальственного самодовольства, — наши разработчики — миллионеры. Разумеется, такими предложениями их не подкупить».

Значит, ФБР пытается превратить сотрудника Дурова в «крота»? Я думал, что Дуров не преминет раздуть этот случай. Компании из Кремниевой долины и озабоченные криптобезопасностью цепляются за любую возможность предстать жертвами угнетения со стороны правительства и частенько преувеличивают самые мелкие инциденты, чтобы добавить себе очков в этом противостоянии. Возьмём, например, случай, когда компания Apple раздула запрос ФБР о разблокировке единственного телефона (использованного в ходе теракта в Сан-Бернардино, когда погибли 14 человек) в противостояние тирании властей — и это при том, что в то же самое время Apple подчинилась требованиям Китая о предоставлении данных (в конечном итоге ФБР получило необходимые данные по Сан-Бернардино, прибегнув к услугам сторонних хакеров). Или вот недавно разработчик, работавшая на Tor, — проект для анонимности в интернете, финансируемый Пентагоном — сбежала в Германию после того, как агент ФБР оставил визитку в доме её родителей.



Специальная страничка на сайте Apple про инцидент в Сан-Бернардино и вмешательство ФБР

С учётом либертарианских взглядов Дурова и его близости к таким кругам я подумал, что он начнёт неистовствовать против тирании, но он был удивительно, даже обескураживающе уравновешен и рассудителен. Разумеется, он был обеспокоен и огорчён давлением со стороны ФБР и обещал противостоять всем попыткам американского правительства получить доступ к данным Telegram. Но случившееся его не удивило. В конце концов, для таких целей ФБР и существует. «Американцы, в сущности, делают свою работу. Ведь если смотреть с их точки зрения… Вот молодой парень, его приложением пользуются террористы. Надо выяснить, кто он такой. Что у него за команда. Это всё логично. Ничего сверхъестественного я в этом не вижу, — говорит он. — Когда это случилось, я, конечно, мог поднять большой шум. “Поглядите, американцы на меня давят!”. Но я подумал, что это было бы слишком претенциозно и мелодраматично».

Так зачем рассказывать об этом сейчас? Дуров говорит, что просто хотел подчеркнуть факт, который обычно совсем упускают из виду в пылу драматической борьбы обитателей Кремниевой долины с федеральными властями: случай с Telegram показателен с точки зрения способов, которыми власти пытаются повлиять на сферу больших данных. «Я заговорил об этом лишь чтобы отметить, что американские спецслужбы действуют упорно и настойчиво, и они лишь выполняют свои обязанности. Вас перехватят в аэропорту. Заявятся незваными по адресу, который вроде бы знали только вы. Попробуют подкупить разработчиков. В общем, ФБР очень тщательно делает свою работу, а ведь мы с командой провели в Америке лишь пару дней», — говорит он. Если ФБР так настойчиво действует в отношении Telegram, не останавливаясь даже перед подкупом сотрудников в краткосрочной деловой командировке, то как же американское правительство ведёт себя по отношению к компаниям со штаб-квартирой

в США? «Я не могу представить, как мне или кому-то другому удалось бы в таких условиях заниматься приложениями, ориентированными на сохранение личной информации. Начнут они с требований делиться данными по терроризму, а потом постепенно дойдут бог весть до чего».

Шифрование или смерть!

В июне 2013 года Эдвард Сноуден организовал утечку данных, потрясшую весь мир. Сотрудник Агентства национальной безопасности США, работавший с большими данными Вашингтона и юридического колосса Booz Allen Hamilton, рассказал об американском аппарате слежки в интернете и помог пролить свет на симбиоз Кремниевой долины и правительства США.
Документы, которые он похитил из центра АНБ на Гавайях, содержали первые действительные доказательства, что самые уважаемые американские технологические компании — включая Google, Facebook, и Apple — тесно сотрудничали с правительственными агентами, тайно сливая информацию с собственных серверов в интересах АНБ и ФБР. Масштабная утечка данных, организованная Сноуденом, поставила вопрос о неприкосновенности информации в интернете с невиданной ранее остротой.

Об этом внезапно заговорили в новостных программах, начались расследования *Frontline*, посыпались Пулитцеровские премии. Забушевали протесты против слежки, в интернете собирались подписи, а государственные надзорные службы и организации по защите прав потребителей строчили массы отчётов. В 2013 году мы, казалось, были на пороге появления массового движения, которое поможет людям

добиться принятия законов о защите неприкосновенности информации и не только ограничит правительственную слежку, но и загонит в рамки бесконтрольный сбор данных компаниями из Кремниевой долины. Но всё пошло иначе.

Четыре года спустя стало очевидно, что энергию, ярость и потенциал гражданских протестов перенаправили в узкое русло. Новый консенсус, озвучиваемый Кремниевой долиной, гласит, что для защиты от слежки нам надо всего лишь скачать приложение для криптозащиты данных и запустить его на своём iPhone. Вместо поисков политического и демократического решения того правительственно-корпоративного кризиса, который отравляет наше общество, движение за неприкосновенность информации оказалось в либертарианской колее. В кратчайшие сроки сторонники неприкосновенности данных позабыли о том, что народ и политики могут изменить мир к лучшему, и погнались за явной фантазией: мол, если каждый получит в своё распоряжение могучее криптооружие, то сможет бросить вызов и корпорациям, и всесильным организациям вроде АНБ; сможет использовать технологии для защиты информации на своих условиях.

Сам Эдвард Сноуден стал главным трубадуром такого подхода, не упуская возможности заявить, что гражданская политика бессмысленна, а вот использование технологических штучек — то, что надо. Вопрос с коммерческой слежкой, которой активно занимаются компании из Кремниевой долины, он фактически проигнорировал, заявив *The Washington Times*, что «Twitter никого не держит под прицелом». Напротив, Сноуден рассматривает частные компании вроде Apple и Facebook в качестве союзников — как малые островки безопасности в бушующем море интернета. В его глазах частные разработчики и специалисты по программному обеспечению — настоящие защитники граждан, которых он призывает восстать против правительственного гнёта. «Если мы хотим получить достойное будущее, его придётся создавать самим. Политика многого не даст, и, как показывает история, политический путь — самый ненадёжный способ добиться перемен… в конце концов, закон — это лишь буквы на бумаге. Они не восстанут, чтобы защитить ваши права», — заявил он посетителям оклендской конференции *Fusion*'s 2016 Real Future Fair в видеообращении из Москвы. Для Сноудена, превратившегося из разоблачителя в политического философа, политические движения и гражданские акции — сплошное легкомыслие, не дающее никаких реальных гарантий; напротив, криптозащита и компьютерные технологии — надёжные инструменты, основанные на законах математики и физики. «Технологии работают не так, как законы, — заявил беглый разоблачитель гостям Real Future Fair, — технологии не признают юрисдикций».

Это абсурдная позиция. Заменим слово «технология» на «штурмовую винтовку», и речь Сноудена прозвучит весьма уместно на республиканской Конференции консервативных политических действий (CPAC). Но на Real Future Fair Сноудену аплодировали стоя. Хотя почему бы и нет? С того момента, как о Сноудене заговорили, его

техноцентристский взгляд на мир поддержал целый хор лавроносных журналистов, активистов, левой интеллигенции и могущественных организаций вроде Фонда электронной свободы (EFF) и Американского союза защиты гражданских свобод (ACLU). Кремниевая долина тоже выступила за взгляды Сноудена. Легион отважных разработчиков предложил целый ряд крайне узких технических решений по обеспечению безопасности, заявляя, что это убережёт пользователей от правительственной слежки. При этом они сами бесстыдно следят за теми же самыми пользователями с целью извлечения прибыли.

Как бы там ни было, но призыв Сноудена вооружаться криптооружием вдохновил Дурова на создание Telegram. «Я далек от политики и не могу лоббировать запреты на тотальную слежку, — писал он в октябре 2013 года, через несколько месяцев после того, как Сноуден прибыл в Москву и незадолго до того, как сам Дуров был вынужден покинуть Россию, — но есть кое-что, что мы — IT-предприниматели и программисты — можем сделать. Мы можем разрабатывать и финансировать технологии, нацеленные на то, чтобы тотальная слежка стала технически невозможной».

В Америке первоначальный импульс перенести борьбу со слежкой на территорию самой Кремниевой долины потух и переродился в нечто странное и жалкое: активисты начали сотрудничать с Google и Facebook, чтобы противостоять АНБ с помощью криптотехнологий. Смысла в этом ровно столько же, сколько в объединении с Blackwater (или Xe, или Academi, или как там сейчас называют себя эти подрядчики Пентагона) против американской армии. Но тенденция вести политику программными средствами усилилась после избрания Дональда Трампа президентом. Борцы за гражданские права, защитники неприкосновенности информации и деморализованные либералы наперебой восклицают, что шифрование — даже то, которое предлагают монстры слежки из Кремниевой долины, — надёжный способ защититься от тоталитарной администрации Трампа.

«Трамп стал президентом. Шифруйте письма, — призвал Макс Рид из *New York Magazine* в колонке, которую в марте опубликовала *New York Times*, — спустя несколько недель после того, как Дональд Трамп выиграл выборы, между моими друзьями наметился явный раскол. И речь не о политических разногласиях по поводу нового президента или философских рассуждениях о будущем страны; речь о том, какое приложение нам лучше использовать для обмена сообщениями…».

Авторы *Buzzfeed* выразили то же мнение: «Как защитить свою информацию в Америке Дональда Трампа: Простые методы защиты от более пристальной слежки государства», — писало издание, предлагая своим читателям из поколения 2000-х детальное руководство, как «уйти в тень» на просторах всемирной сети.

Что это за приложения? Кто их разработал? Действительно ли они работают? И тут ситуация принимает ещё более странный оборот.

Тайны и ложь

Невольные встречи Дурова с ФБР выявили неприятный факт из индустрии «больших данных»: современное движение за неприкосновенность информации практически всецело зависит от инструментов криптографии, выпестованных и оплаченных аппаратом внешней политики США — конгломератом правительственных учреждений и организаций, порождённых волной пропаганды времён Холодной войны, которую подняло ЦРУ.

В 1948 году ЦРУ получило карт-бланш на всевозможные тайные операции по сдерживанию и нейтрализации распространения коммунизма из СССР и стран Восточной Европы. В этой войне идеологий основным инструментом стала радиопропаганда, и ЦРУ использовало различные группировки для создания радиостанций с названиями вроде «Радио освобождения от большевизма» и «Радио Свободная Европа». В пятидесятые и шестидесятые годы ЦРУ расширило свою радиосеть для использования в операциях против коммунистических, левых и иных подозрительных сил, которые могли распространять опасную бациллу большевизма в Азии и Латинской Америке.

Замысел был в том, чтобы не дать тамошним государствам свободно распоряжаться собственной информационной сферой, а также во влиянии и господстве над умами людей для продвижения американских интересов. По мнению самого ЦРУ, эта тайная пропагандистская операция стала шедевром, и спецслужба до сих пор считает её одним из наиболее успешных проектов психологической войны, осуществлённых Соединёнными Штатами.

В конце концов пропагандистский спрут ЦРУ стал из тайного явным, и конгресс США преобразовал его в Наблюдательный совет по международному вещанию, федеральное агентство наподобие Госдепа. В наше время Наблюдательный совет с бюджетом почти в миллиард долларов управляет всей внешней пропагандой страны. О его существовании американская общественность имеет самое смутное представление, а между тем Наблюдательный совет ведёт спутниковые, телевизионные и радиопередачи почти в каждый уголок мира. И, как это было с ЦРУ почти семьдесят лет назад, миссия совета заключается именно в том, в чём американские политики нынче обвиняют Россию: финансирование новостей — частью объективных, а частью искажённых — в интересах борьбы за геополитическое господство.

Ньюсрум в Middle East Broadcasting Networks, Inc., которую финансирует Наблюдательный совет

Но и это далеко не всё. По мере распространения интернета по миру он превратился в могущественный инструмент влияния, и американское правительство принялось безжалостно использовать своё преимущество над конкурентами под знаменем «интернет-свобод». Политика, принятая госсекретарём Хиллари Клинтон, вовсе не сводилась к трансляции новостей. Её целью стало превращение этой технологии всемирной связи в оружие для ослабления противников, свержения недружественных правительств и поддержки оппозиционных движений от Китая и России до Ирана, Сирии и Ливии. «Администрация Обамы является мировым лидером по продвижению „теневых“ сотовых и интернет-систем, которые диссиденты могут использовать для борьбы с авторитарными правительствами, пытающимися заглушить их голос цензурой или блокировкой сетей связи», — заявила the *New York Times* в 2011 году, когда впервые начала разворачиваться программа «Свободный интернет».

В рамках этой программы можно рассказать и о тайных проектах по созданию независимых сотовых сетей в других государствах, и чисто шпионскую историю, как в пятиэтажном магазине на вашингтонской Л-стрит группа молодых предпринимателей, напоминающих музыкантов-любителей, запихивала обманчиво-невинные устройства в прототип «интернета в чемодане»… Такой чемодан можно тайно пронести через границу и быстро создать беспроводную сеть с выходом в интернет на значительной территории.

Дальше, как водится, больше. В последующие годы Наблюдательный совет при поддержке госдепартамента развернул «Свободный интернет» в программу с годовым бюджетом в 50 млн долларов, в рамках которой финансируются сотни проектов во множестве стран — Китае, Кубе, Вьетнаме, России. Сюрреализм продолжает нарастать: эта программа была предназначена для проецирования влияния на другие

страны, но при этом каким-то образом оказалась во главе американского движения за конфиденциальность в интернете. По ней финансируются активисты и частные исследователи, ведётся сотрудничество с EFF, ACLU и даже компаниями вроде Google. Куда ни посмотри, в глаза бросаются программы для защиты конфиденциальности, профинансированные этой организацией. К их числу принадлежат и наиболее распиаренные ныне продукты: Tor, платформа для анонимного посещения интернета, включая так называемую «тёмную паутину», и Signal, приложение для обмена сообщениями, которое активно отстаивает Эдвард Сноуден. Чтобы эти приложения оставались на плаву, правительство потратило миллионы долларов.

Безопасность из странных рук

Когда у Павла Дурова отобрали ВКонтакте и принудили к бегству из России, западная общественность приветствовала его как героя, эдакого современного Сахарова, который сражался за свободу и поплатился своим бизнесом. Американские адепты криптобезопасности тоже приняли его с раскрытыми объятиями. Но очень скоро эта идиллия оказалась разрушена, и главным виновником стал Signal: мобильное криптоприложение, созданное мелкой и мутноватой компанией под названием Open Whisper Systems, также известной как Quiet Riddle Ventures LLC.
Изобрёл его некий радикальный криптограф по имени Мокси Марлинспайк (Moxie Marlinspike; хотя в реальности он, скорее всего, даже не Мэтью Розенфельд или Майк Бенхэм), дал путёвку в жизнь финансируемый Наблюдательным комитетом Фонд открытых технологий (в который с 2013 года закачали почти 3 млн долларов), а поддерживают на плаву правительственные вливания. Несмотря на тесные связи с организацией, отпочковавшейся от ЦРУ, апостолы американского движения за криптобезопасность поддержали приложение. «Использую Singal ежедневно. #назаметкуФБР», — сообщил Сноуден в своём твиттере легионам сторонников, которые незамедлительно бросились скачивать это приложение. Марлинспайк использовал похвалы Сноудена на полную катушку, гордо разместив вердикт бывшего сотрудника АНБ на вебсайте компании: «Используйте любые разработки Open Whisper Systems». Благодаря такой поддержке Signal стал самым массовым приложением для обмена сообщениями среди американских журналистов, политиков и активистов — от анархистов и марксистов до борцов за права афроамериканцев. Сейчас им полюбили пользоваться ещё и оппозиционеры при организации акций против Трампа. Signal триумфально вошёл даже в Кремниевую долину: Марлинспайк сотрудничает с руководством Facebook и Google, помогая интегрировать криптоархитектуру приложения в их собственные программы для общения через мобильные устройства, включая WhatsApp. Характерно, что интеграция Signal в WhatsApp удостоилась одобрения со стороны Наблюдательного совета; руководство пропагандистского органа

похвасталось, что профинансированные государством инструменты криптобезопасности будут использоваться миллиардом человек.

Несмотря на связи между Open Whisper и американскими властями, авторитетные борцы за конфиденциальность начали отговаривать людей пользоваться другими средствами. Это относится и к Telegram с его особыми криптографическими методами, созданными братом Павла Дурова, математиком Николаем. Даже Сноуден счёл за нужное отпугнуть пользователей от Telegram, посоветовав политическим активистам, журналистам, диссидентам, разоблачителям — короче, всем подряд — вместо этого использовать Signal или даже фейсбуковский WhatsApp. «Telegram по определению менее безопасен, чем WhatsApp, что делает его опасным для неспециалистов», — написал Сноуден в своём твиттере, отвечая на вопрос любопытствующего сторонника.

> Если вашим оппонентом выступает правительство Соединённых Штатов, неважно, какими крипто-приложениями вы пользуетесь

Но для приложения, призванного уберечь людей от пристального внимания американского правительства, у Signal слишком странная архитектура, которая уже заставила призадуматься иных экспертов по информационной безопасности. Алгоритм шифрования Signal считается безупречным, но его серверный модуль почему-то работает в облачной службе компании Amazon, которая, в свою очередь, является крупным подрядчиком ЦРУ. Кроме того, программа требует ввести настоящий номер мобильного телефона и предоставить доступ ко всем абонентам адресной книги, что как-то неожиданно для приложения по защите личной тайны. Наконец, Signal устанавливается на сотовый телефон через сервисы Google и Apple, а обе эти компании помогают АНБ вести слежку за пользователями. «У Google обычно есть корневой доступ, это принципиально. Google всё ещё сотрудничает с АНБ и другими спецслужбами, — пишет Сандер Венема, разработчик, ведущий для журналистов курсы по информационной безопасности. — Я почти уверен, что Google может использовать особые обновления или версии Signal для слежки за конкретными лицами, а те по наивности сами установят вредоносную программу на сотовый телефон».

А с учётом того, что Signal обычно пользуются политические активисты и журналисты, приложение превращается в чёткую метку: пусть оно шифрует сообщения, но ещё оно маркирует пользователей, которым есть что скрывать. Надпись большими буквами: «ЗА МНОЙ СТОИТ ПОНАБЛЮДАТЬ».

Как бы там ни было, но если вашим оппонентом выступает правительство Соединённых Штатов, неважно, какими криптоприложениями вы пользуетесь. Последний слив документов по хакерским инструментам ЦРУ на WikiLeaks показал, что отдел по мобильным устройствам этой спецслужбы разработал множество способов перехвата информации с телефона даже при использовании приложений вроде Signal, WhatsApp и даже Telegram. «Эти методы позволяют ЦРУ обойти шифрование WhatsApp, Signal, Telegram, Wiebo, Confide и Cloackman, встраиваясь в смартфоны и собирая аудио- и текстовые данные до применения шифрования», — отмечается на WikiLeaks.

Дуров признаёт, что у его криптографии есть свои ограничения. Но критика Telegram со стороны Сноудена его удивила и раздосадовала. По словам Дурова, они с братом крайне осторожно подходили к выбору криптографических методов, лоббируемых американскими экспертами, в особенности после того, как Сноуден опубликовал документы АНБ, из которых следовало, что агентство тайно платило RSA, влиятельной компьютерной компании, использовавшей несовершенные методы, которые АНБ умело взламывать. Дуровы задумались, может ли то же самое произойти с другими популярными алгоритмами шифрования. Ещё больше они встревожились, когда американские эксперты по криптографии начали публичные нападки на Telegram в СМИ. «Их критика строилась не на действительных слабостях нашего подхода, а только на том, что мы не использовали предпочитаемые ими алгоритмы, — говорит он, — поскольку никакого осмысленного диалога о криптографии не получилось, мы начали понимать, что они преследуют какую-то другую цель, а не поиск истины или повышение безопасности».

Но нападки продолжались. Сноуден и его союзники не только заявляли о доверии к Facebook — компании, которая занимается слежкой и сотрудничает с АНБ; они ещё и поддерживали приложение, финансируемое внешнеполитическим ведомством американского аппарата национальной безопасности. Это была полная бессмыслица. Дуров был потрясён. Он сказал мне, что не может понять, почему люди доверяют якобы антиправительственному приложению, оплаченному самим же правительством, от которого оно призвано защищать.

Я сказал, что полностью разделяю его недоумение. По мере изучения всех этих крипторадикалов, финансируемых различными отпрысками ЦРУ, я продолжал задавать один и тот же простой вопрос, на который никто не мог дать вразумительный ответ: если приложения вроде Signal действительно подрывают возможности АНБ по слежке за гражданами, то зачем американское правительство продолжает их финансировать? Я пытался представить, как подобный альянс между правительством и корпорациями

был бы воспринят представителями американских технических кругов и СМИ, если бы нечто похожее произошло в Советском Союзе. Скажем, КГБ профинансировал бы защищённую факсовую линию и предложил бы Александру Солженицыну и диссидентам-самиздатовцам использовать её, чтобы уберечься от внимания агентов КГБ. И Солженицын не только поверил бы КГБ, но ещё и посоветовал бы друзьям-диссидентам такую линию использовать: «Она совершенно безопасна». Затею КГБ на капиталистическом Западе беспощадно бы высмеяли, а Солженицына сочли бы в лучшем случае марионеткой, а в худшем — предателем. Как ни смехотворен этот союз технологий и государственных интересов под личиной диссидентства, в Америке он почему-то сработал.

Пока я излагал свои аналогии, Дуров согласно кивал: «Думаю, неслучайно, что мы оба понимаем всю наивность такого мышления, и оба родились в СССР».

Сила доверия

К чему бы я ни готовился при встрече с Павлом Дуровым, но только не к политическому взаимопониманию. Судя по тому, что я читал в прессе, наши с ним взгляды на политику диаметрально противоположны. Он либертарианец, который может бросить на улицу банкноту в 5000 рублей, чтобы понаблюдать, как прохожие отпихивают друг друга, чтобы её поднять; который может написать, что Гитлер и Сталин ничем не отличаются друг от друга в день, когда люди в бывших советских республиках отмечают победу над гитлеровской Германией.

Но на личном уровне он оказался приятным и даже застенчивым человеком. Для представителя мира криптографии он оказался большим реалистом в том, что касается ограничений в этой области. Фанатической веры в технологии, столь характерной для представителей американского движения за конфиденциальность информации, в нём совсем нет. И ещё одна черта: Дуров — боец.

Начнём с простого факта, что он открыто рассказал о подробностях попыток ФБР подкупить его команду и принудить Telegram к тайному сотрудничеству. Хотя сам Дуров попытался преуменьшить этот случай, на самом деле его значение велико. Несмотря на вынужденное бегство из России, он не уступил американским спецслужбам и решил сражаться на два фронта. Такой поступок необычен и производит глубокое впечатление. Большинство людей, которые вступают в конфликт с российским правительством и ищут безопасности на Западе под видом современных диссидентов, обычно начинают повторять западную пропаганду, становясь бездумными проводниками американских интересов даже в худшем их виде. Как участницы Pussy Riot, которые бежали из России и критиковали Владимира Путина, а потом скатились до фоточек с госсекретарём Хиллари Клинтон.

Что же касается криптографии, то нет никакой уверенности, что Telegram более безопасен, чем его конкуренты из Кремниевой долины. Но тем более нет уверенности в том, что финансируемая спецслужбами и озабоченная прибылью кампания за конфиденциальность на Западе может принести действительные результаты.

В реальности, которую вызвал к жизни Сноуден, защита частной информации оказалась возложена на криптоприложения. Из-за этого мы очутились в какой-то кошмарной параноидальной игре, где у простых граждан нет никакого влияния и они вынуждены всецело полагаться на людей и организации, создающие алгоритмы для этих криптотехнологий. Всё сводится к доверию. Можно ли доверять этим людям и организациям? Молодому русскому технократу, поссорившемуся с Кремлём? Бывшему американскому шпиону, сбежавшему в Россию? Модным криптоприложениям, оплаченным Госдепартаментом США? Google и Facebook, сотрудничающим с АНБ? Растерянность? Непонимание? Так выглядит движение за защиту личной информации в наше время.