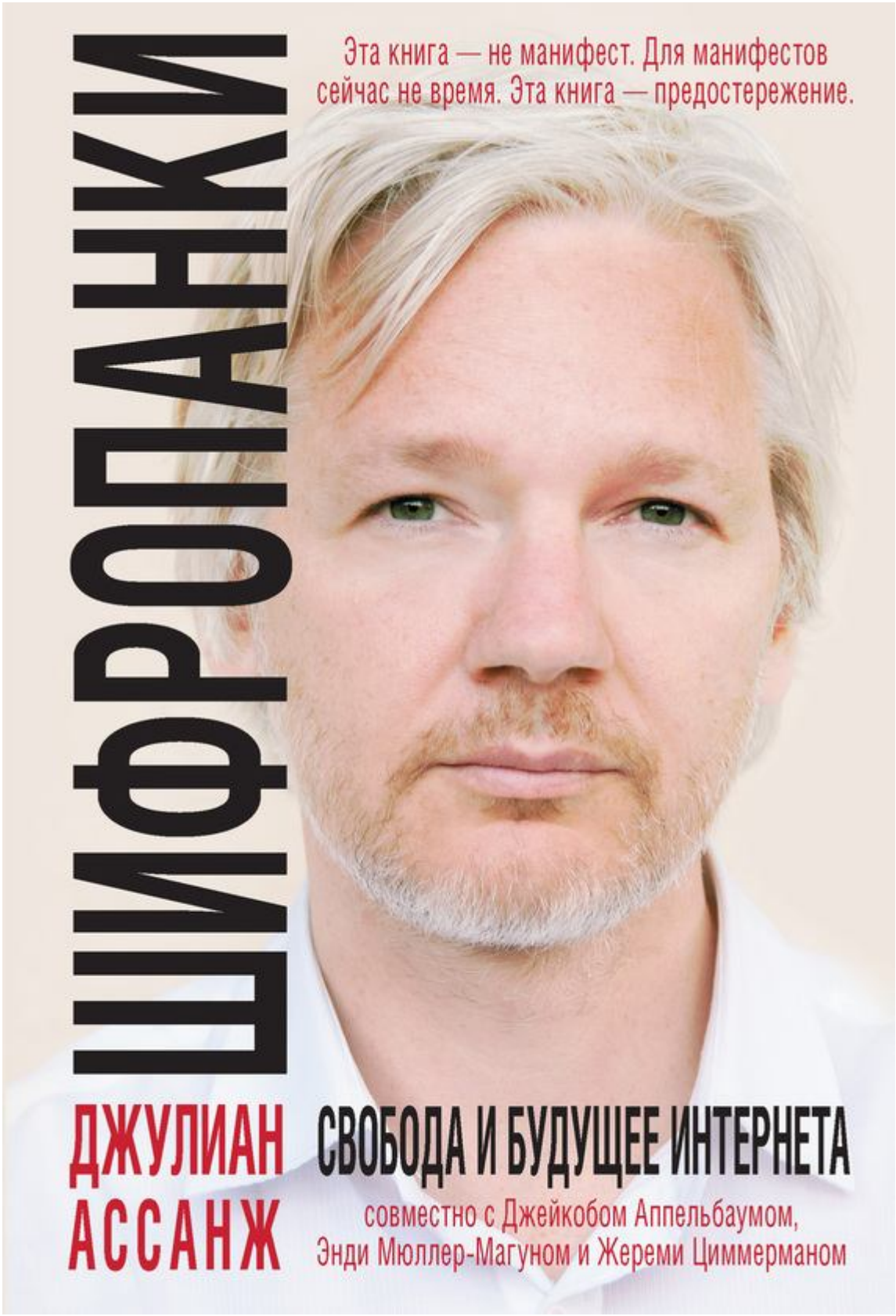
Джейкоб Аппельбаум Джулиан Ассанж Энди Мюллер-Магун Жереми Циммерман
Шифропанки: свобода и будущее Интернета



Азбука Бизнес, Азбука-Аттикус; Москва; 2014

ISBN 978-5-389-0797

Аннотация

Весна интернета позади. Из объединяющего пространства, свободного от цензуры, Сеть превратилась в орудие глобального контроля. Государства все жестче отслеживают поступки своих граждан, подавляя любые нежелательные действия и не только их. Владеет Сетью тот, кто контролирует ее структуры – волоконно-оптические линии связи, спутники, серверы, разбросанные по городам мира. Тотальный характер мощнейшей машины контроля пока очевиден не всем пользователям интернета. Джулиан Ассанж и его соратники по движению шифопанков призывают к борьбе за свободу обмена информацией. Их оружие – криптография. Их знаменитый проект WikiLeaks вступил в конфликт почти со всеми влиятельными державами планеты.

Эта книга – предостережение. Объявлен общий сбор под знамена шифрования.

Перевод: Николай Караев

Джулиан Ассанж совместно с Джейкобом Аппельбаумом, Энди Мюллер-Магуном, Жереми Циммерманом Шифропанки: свобода и будущее интернета

Интернет – это угроза всей человеческой цивилизации

Интернет – это угроза всей человеческой цивилизации.

Джулиан Ассанж

Интернет способствовал революциям по всему миру, однако в данный момент полным ходом идет подавление Сети. В эпоху, когда киберпространство осваивают целые сообщества, программы массовой слежки разворачиваются в масштабах планеты. Наша цивилизация стоит на развилке. Одна дорога ведет к будущему, в котором есть «приватность для слабых и прозрачность для сильных»; другая – к интернету, благодаря которому власть перейдет от народов к неподконтрольному никому комплексу спецслужб и их союзников – транснациональных корпораций.

Шифропанки – это активисты, пропагандирующие массовое использование сильной криптографии для защиты наших основных свобод от агрессоров. Джулиан Ассанж, главный редактор и вдохновитель проекта WikiLeaks, стал лидером шифропанковского движения в 1990-х. Сегодня Ассанж сводит вместе мятежных мыслителей и активистов с передового рубежа битвы за виртуальный мир, чтобы обсудить в своевременной и весьма важной новой книге, что именно сделает интернет со всеми нами: освободит или поработит.

Джулиан Ассанж – главный редактор проекта WikiLeaks, обладатель Новой премии СМИ организации «Международная амнистия» (2009), золотой медали Сиднейского фонда мира (2011), премии «Уокли» за журналистику (2011) и премии Марты Геллхорн (2011). Он был участником рассылки Cypherpunk и создал многочисленные программы, проникнутые философией шифропанка, включая криптографическую систему rubberhose и исходный код для WikiLeaks. Вместе со Сьюлетт Дрейфус он написал историю международного хакерского движения – книгу «Компьютерное подполье».

Что такое шифропанк?

Люди, называющие себя шифропанками, пропагандируют использование криптографии и других подобных методов, надеясь с их помощью добиться общественных и политических перемен [1] . Возникшее в начале 1990-х годов, это движение активнейшим

образом участвовало в «криптовойнах» того времени и последовавшей «весне интернета» 2011 года.

Термин «шифропанк» (*англ.* cypherpunk) – от слов «(криптографический) шифр» и «панк» – был добавлен в Оксфордский словарь английского языка в 2006 году [2] .

Введение: призыв к криптографическому оружию

Эта книга – не манифест. Для манифестов сейчас не время. Эта книга – предостережение.

Наш мир не просто катится к транснациональной антиутопии – он мчится к ней на всех парах. Однако в полной мере данный факт осознают лишь круги, связанные с госбезопасностью. Обычные люди из-за секретности, сложности и масштаба идущих процессов этого не видят. Интернет – величайшее изобретение, которое могло даровать нам свободу, – ныне превращен в наиболее опасный проводник тоталитаризма в истории. Интернет – это угроза всей человеческой цивилизации.

Преобразование интернета случилось незаметно – люди, которые понимают, что именно происходит, сами трудятся над установлением глобального контроля и не заинтересованы в том, чтобы эта информация вышла наружу. Если траектория развития общества не изменится, наша цивилизация через два-три года превратится в постмодернистскую антиутопию, где слежка ведется за всеми и каждым в отдельности, и укрыться от нее не может никто, кроме наиболее опытных и информированных людей. Нельзя исключать, что эпоха глобального контроля уже настала.

О том, как интернет меняет нашу цивилизацию, писали многие мыслители, однако все они оказались неправы. Эти авторы ошиблись, потому что у них не было чувства перспективы – оно появляется только с накоплением непосредственного опыта. Они ошиблись, потому что никогда не сталкивались с врагом.

Всякое миропонимание гибнет при первом столкновении с врагом.

Мы увидели своих врагов.

За последние шесть лет проект WikiLeaks вступил в конфликт почти со всеми влиятельными державами планеты. Новая система слежки открылась нам изнутри – и мы сумели проникнуть в ее тайны. Она открылась нам с точки зрения участника сражения – мы должны были защищать своих людей, свои финансы, свои источники информации. Она открылась нам в глобальном разрезе – мы располагаем людьми, имуществом и информацией почти во всех странах. Она открылась нам во временно́м разрезе – мы боролись с данным феноменом много лет и видели, как контроль усиливается и распространяется, снова и снова. Это агрессивный паразит, который высасывает соки из общества, активно работающего с интернетом. Он захватывает всё новые территории, поражая любые страны, а прежде всего – людей.

Что нам нужно сделать?

Давным-давно в некоем месте, расположенном не здесь и не там, мы, создатели и граждане тогда еще молодого интернета, обсуждали будущее нашего нового мира.

Нам казалось, что он еще теснее свяжет человечество – и изменится сама природа государств, определяемых через способ обмена информацией, экономические ценности и военную мощь.

Нам казалось, что слияние существующих государственных структур и интернета создает предпосылки к изменению природы государства.

Для начала давайте вспомним, что государство – это система, через которую протекает принудительная сила: оно словно бы создает поле, размагничивающее источники свободы. Группировки внутри страны могут биться друг с другом за электорат, создавая видимость демократии, но фундамент любого государства – систематическое применение насилия (и противостояние ему). Землевладение, собственность, аренда, дивиденды, налогообложение, судебные штрафы, цензура, авторские права и торговые знаки – все это существует благодаря угрозе применения государственного насилия.

Бо́льшую часть времени мы не можем даже вообразить, сколь тонка грань, отделяющая нас от него, – и все мы идем на уступки, чтобы его избежать. Уподобляясь матросам, вдыхающим свежий бриз, мы редко задумываемся о том, что под поверхностью нашего мира кроется тьма, без которой его не было бы.

Что может стать проводником принудительной силы в новом пространстве интернета?

Имеет ли вообще смысл такой вопрос? Как в этом потустороннем пространстве, в царстве вроде бы платоновских идей и информационных потоков может возникнуть само понятие принудительной силы? Силы, способной видоизменять исторические записи, прослушивать телефоны, разделять людей, разрушать сложные структуры и возводить стены – то есть действовать, как армия оккупантов?

Платоновская природа интернета, его идей и информационных потоков окажется иллюзорной, если вспомнить о физической основе всего этого. Фундамент Сети – волоконно-оптические линии связи, проложенные в толще океана, спутники, летающие над нашими головами, компьютерные серверы, размещенные в зданиях различных городов, от Нью-Йорка до Найроби. Как солдат смог зарубить Архимеда простым мечом, так и вооруженные силы способны захватить контроль над главным достижением западной цивилизации и завоевать наше платоновское царство.

Новый мир интернета, отделившийся от старого мира неодушевленных атомов, жаждал независимости. Однако государства и их друзья решили поместить его под колпак, заполучив власть над его физическими носителями. Государство, подобно армии, охраняющей нефтяную скважину, или таможеннику, вымогающему взятки на границе, быстро научилось использовать контроль над физическим пространством для обретения абсолютного контроля над нашим платоновским пространством. Однажды государство разобьет наши мечты о независимости, а затем, усевшись на оптоволоконные кабели и наземные станции систем спутниковой связи, начнет массовый перехват информационных потоков нашего нового мира – самой его сути, успевшей стать основой любых личных, экономических и политических взаимоотношений. Государство вопьется в вены и артерии наших новых сообществ, поглотит любое проявление связей в виде информации или общения, каждый доступный для чтения сайт, любое отправленное письмо, всякую мысль, забитую в Google, после чего сохранит данные – миллиарды перехватов в день, дающих невообразимую власть, – в обширных сверхсекретных информационных хранилищах. Навечно. Государство станет разрабатывать эти копи, эту производную коллективного человеческого разума, используя все более замысловатые алгоритмы поиска и распознавания образов, пополняя свой рудник и все более увеличивая разрыв в правах и возможностях между теми, кто перехватывает информацию, и обществом, которое ее производит. А потом государство воплотит все, чему научилось, в реальном мире: оно станет развязывать войны, нацеливать беспилотные боевые машины, манипулировать комитетами ООН и торговыми соглашениями, а также оказывать услуги обширной сети скованных одной цепью бизнесменов, инсайдеров и коррупционеров.

Но мы нашли средство против государства. Это наша единственная надежда на противодействие тотальной власти. Надежда на то, что храбрость, вдохновение и солидарность помогут нам оказать сопротивление. Мы обнаружили странное свойство физической вселенной, в которой живем.

Вселенная верит в шифрование.

Зашифровать информацию легче, чем расшифровать.

Мы поняли, что сможем использовать это свойство, чтобы создать законы нового мира. Чтобы отделить наше новое платоновское царство от его физических носителей в виде спутников, подводных кабелей – и тех, кому они принадлежат. Укрыть наше пространство за криптографической завесой. Создать новые земли, закрытые для тех, кто контролирует физическую реальность, – ведь для того, чтобы следить за нами, им понадобятся бесконечные ресурсы.

Таким образом мы провозгласим независимость.

Ученые из Манхэттенского проекта поняли, что вселенная позволяет сконструировать атомную бомбу. Это умозаключение не было очевидным. Создание ядерного оружия вполне могло оказаться нереальным. Однако вселенная верит в атомные бомбы и ядерные реакторы. Она благословляет эти феномены так же, как соль, море или звезды.

А еще вселенная, наша физическая вселенная, обладает свойством, позволяющим индивиду или группе зашифровать информацию – надежно, автоматически, даже не сознавая того, – таким образом, что все ресурсы и вся политическая воля сильнейшей сверхдержавы на Земле не помогут ее расшифровать. Сеть соединяющих нас шифровальных каналов создаст области, свободные от принудительной силы внешнего государства. Свободные от массового перехвата. Свободные от контроля.

Так люди смогут противопоставить воле полностью мобилизованной сверхдержавы собственную волю – и победить. Шифрование – это воплощение физических законов, ему не страшны угрозы государств даже в условиях антиутопии с ее транснациональной слежкой за всеми и каждым.

Мир вовсе не обязан функционировать именно так. Однако по каким-то причинам вселенная благоволит шифрованию.

Криптография – это крайнее выражение ненасильственного прямого действия.

Государство, располагающее ядерным оружием, может подвергнуть неограниченному принуждению миллионы людей, однако даже в этом случае оно окажется не в состоянии сломить волю индивидов, желающих утаить от него свои секреты и использующих сильную криптографию.

Сильная криптография способна противостоять любому насилию. Нет такой формы принуждения, которая могла бы решить математическую задачу.

Но в силах ли мы превратить это странное свойство мира в краеугольный камень в фундаменте освобождения и независимости человечества в платоновском царстве интернета? И может ли случиться так, что по мере слияния социума и интернета эта свобода распространится и на физическую реальность, тем самым трансформировав само понятие государства?

Как мы понимаем, государства – это системы, которые решают, где и как последовательно применять принудительную силу.

На вопрос, может ли принудительная сила просочиться в интернет из физического мира, отвечают криптография и идеалы шифропанков.

По мере слияния государств с интернетом будущее нашей цивилизации становится будущим интернета, так что нам требуется пересмотреть соотношение сил.

Если мы этого не сделаем, глобальность интернета превратит само человечество в гигантскую сеть массовой слежки и контроля.

Мы должны дать сигнал тревоги. Эта книга – крик дозорного в ночи.

20 марта 2012 года, пребывая в Соединенном Королевстве под домашним арестом в ожидании экстрадиции, я встретился с тремя друзьями, такими же, как я, дозорными, в надежде на то, что, если мы заорем в один голос, наши крики пробудят город. Мы обязаны рассказать обо всем, что узнали, – пока у тебя, читатель, еще есть шанс разобраться в происходящем и сделать то, что ты должен сделать.

Пришло время взяться за оружие нашего нового мира, время сражаться за себя и за тех, кого мы любим.

Наша задача – укрепить свободу там, где мы можем это сделать, где не можем – замедлить наступление антиутопии и, наконец, ускорить ее саморазрушение, если нам не останется ничего другого.

Джулиан Ассанж, Лондон, октябрь 2012 года

Участники обсуждения

ДЖУЛИАН АССАНЖ – главный редактор и вдохновитель WikiLeaks [3] . Джулиан с самого начала был участником рассылки Cypherpunk («Шифропанк») и остается одним из

самых видных представителей философии этого движения в мире. Его работа с проектом WikiLeaks наполнила традиционный лозунг шифропанков «приватность для слабых, прозрачность для сильных» политическим содержанием. Хотя Джулиана больше знают как активного борца за свободное волеизъявление, требующего, чтобы власть и ее институты были прозрачны и подотчетны народу, он также остро критикует вторжение государства и корпораций в частную сферу индивидуума. Джулиан – автор многочисленных проектов программного обеспечения с шифропанковской философией, среди которых – первый сканер портов TCP/IP strobe.c, файловая система отрицаемого шифрования rubberhose и оригинальный код для проекта WikiLeaks [4] . В юности Джулиан изучал безопасность ранних компьютерных сетей – в те времена различные виды хакинга еще не были уголовно наказуемым преступлением. В 1990-е Джулиан стал в Австралии общественным активистом и организовал там компанию – провайдер интернета, а также написал в соавторстве со Сьюлетт Дрейфус книгу «Компьютерное подполье» – историю международного хакерского движения. По ее мотивам был снят фильм «Подполье: история Джулиана Ассанжа» [5] .

ДЖЕЙКОБ АППЕЛЬБАУМ – основатель Noisebridge, хакспейса [6] в Сан-Франциско, член компьютерного клуба Berlin Chaos и разработчик программного обеспечения [7] . Джейкоб пропагандирует и развивает проект Tor, онлайновую анонимную систему, которая позволяет противостоять слежке и обходить сетевую цензуру [8] . Последние десять лет Джейкоб помогает активистам, защищающим права человека и окружающую среду. В частности, он опубликовал результаты передовых исследований, касающихся безопасности, приватности и анонимности во многих областях – от компьютерной криминалистики до медицинского применения марихуаны. Джейкоб верит в то, что у каждого есть право на чтение без ограничений и право на свободу высказываний без исключений. В 2010 году, когда Джулиан Ассанж не смог произнести речь в Нью-Йорке, Джейкоб сделал это за него. С тех пор он, его друзья и родственники подвергаются агрессии со стороны правительства Соединенных Штатов, в том числе допросам в аэропортах, агрессивным обыскам с угрозами и намеками на неизбежное изнасилование в тюрьме и конфискации оборудования; на слежение за онлайн-сервисами Джейкоба выдаются секретные ордера. Впрочем, он ничуть не запуган этими мерами, он продолжает добиваться победы юридическими способами и остается ярым сторонником свободного волеизъявления, а также видным защитником WikiLeaks.

ЭНДИ МЮЛЛЕР-МАГУН давно состоит в немецком компьютерном клубе Chaos, он бывший член совета директоров и пресс-секретарь клуба [9] . Он является одним из основателей EDRi (European Digital Rights, Европейского движения за цифровые права), общественной организации, отстаивающей права человека в цифровую эпоху [10] . В 2000 году интернет-пользователи ЕС избрали Энди европейским директором ICANN (Internet Corporation for Assigned Names and Numbers, Интернет-корпорация доменных имен и адресов), организации, которая несет ответственность за международную политику в сфере доменных имен и IP-адресов [11] . Как специалист в области инфотехнологической и прочей слежки, Энди проводит журналистские расследования на сайте buggedplanet.info в Project Wiki [12] . Работая с криптографическими технологиями, он вместе с коллегами создал компанию Cryptophone, которая предлагает корпоративным клиентам защищенные от прослушивания системы голосовой коммуникации и проводит стратегические консультации в контексте сетевой архитектуры [13] .

ЖЕРЕМИ ЦИММЕРМАН – один из основателей и представитель гражданской правозащитной группы La Quadrature du Net («Квадратура Сети»), наиболее известной европейской организации, отстаивающей права на онлайновую анонимность и распространяющей информацию о попытках регулирования Сети и ущемлении сетевых свобод [14] . Жереми создает инструменты, которые позволяют всем желающим включиться в публичные обсуждения и попытаться изменить порядок вещей. В основном он участвует в войнах за копирайт, спорах по поводу сетевой нейтральности и других проблемах регуляции, от решения которых зависит будущее свободного интернета. Не так давно группа La

Quadrature du Net добилась исторического успеха в европейской политике, проведя кампанию против Международного соглашения по борьбе с контрафактной продукцией (ACTA) в Европейском парламенте. Вскоре после участия в обсуждении, которое легло в основу данной книги, Жереми, уезжавший из США, был задержан двумя офицерами ФБР и допрошен на тему WikiLeaks.

Примечание редактора

Для того чтобы книга о шифропанках стала более понятной рядовому читателю, каждый участник дискуссии получил возможность существенно расширить и прояснить свои аргументы, а также снабдить их сносками. Отредактированная рукопись в целом отражает динамику изначального разговора.

О попытках преследования проекта WikiLeaks и связанных с ним людей

Участники последующего обсуждения неоднократно ссылаются на недавние события из истории проекта WikiLeaks и его попытки опубликовать те или иные документы. Поскольку эти отсылки могут быть непонятны читателям, не знакомым с историей WikiLeaks, краткая информация о нем приведена ниже.

Миссия проекта WikiLeaks – получать инсайдерскую информацию, размещать ее в открытом доступе и в дальнейшем защищать от неизбежных юридических и политических атак. Влиятельные государства и организации постоянно пытаются запретить деятельность WikiLeaks, однако проект, публикующий то, что никто больше публиковать не станет, изначально обладает защитой от подобных нападений.

В 2010 году WikiLeaks осуществил самую известную на сегодня акцию, разоблачив злоупотребления дипломатической секретностью в армии и правительстве США. Эти публикации известны под названиями «Сопутствующее убийство», «Логи войны» и «Кабельгейт» [15] . В ответ правительство США и его союзники предприняли слаженную и длящуюся по сей день атаку с целью уничтожения WikiLeaks.

Большое жюри по WikiLeaks

Прямым следствием публикаций этого проекта стало инициированное властями США и начатое сразу несколькими учреждениями уголовное преследование Джулиана Ассанжа и работников WikiLeaks, а также его спонсоров и предполагаемых сообщников. Созванное в Александрии, штат Виргиния, Большое жюри должно было при поддержке ФБР и Министерства юстиции США решить, возможно ли выдвинуть против Джулиана Ассанжа и других ряд обвинений, в том числе и в сговоре согласно закону о шпионаже (Espionage Act) 1917 года. Американские чиновники заявили, что ситуация «не имеет прецедентов по масштабу и по сути». Большое жюри работает без судей и адвокатов. После того как расследование началось, члены Конгресса США предложили использовать закон о шпионаже в качестве средства для запугивания журналистов, «сознательно публикующих ставшую доступной вследствие утечки информацию», и сделать такой подход обычным для юридической системы США [16] .

На момент выхода этой книги расследование деятельности WikiLeaks продолжается [17] . Некоторые люди были юридически принуждены к даче показаний. На судебных заседаниях по делу Брэдли Мэннинга, солдата, обвиненного в передаче информации WikiLeaks, выяснилось, что дело, в которое ФБР подшивает данные о расследовании WikiLeaks, насчитывает 42 100 страниц, из них около 8000 посвящены этому человеку. Брэдли Мэннинга держали в заключении без суда более 880 дней. Специальный докладчик ООН по пыткам Хуан Мендес официально заявил, что власти обращаются с Брэдли Мэннингом жестоко и бесчеловечно и подобное обращение может быть приравнено к пыткам [18] .

Призывы к расправе над Джулианом Ассанжем и объявление о создании оперативной группы по WikiLeaks

Расследование Большого жюри – не единственное направление атаки на проект WikiLeaks. В декабре 2010 года после «Кабельгейта» различные американские политики стали призывать к внесудебной расправе над Джулианом Ассанжем, в том числе с помощью удара беспилотного летательного аппарата (дрона). Сенаторы США клеймили WikiLeaks как «террористическую организацию» и называли Ассанжа «хай-тек-террористом» и «агентом противника», участвующим в «кибервойне» [19] .

Накануне «Кабельгейта» и публикации материалов, связанных с войной в Ираке, в Пентагоне была создана оперативная группа по WikiLeaks (WikiLeaks Task Force, она же WTF) численностью в 120 человек. Целью ей поставили «проведение операций» против данного проекта. Было публично объявлено о создании в ФБР, ЦРУ и Госдепартаменте США аналогичных оперативных групп – все они работают до сих пор [20] .

Прямая цензура

В беспрецедентной попытке подвергнуть СМИ цензуре власти США стали давить на провайдеров, требуя от них отказаться от предоставления услуг сайту WikiLeaks.org. 1 декабря 2010 года Amazon удалил WikiLeaks из своей системы хранения данных, а 2 декабря служба DNS объявила, что домен WikiLeaks.org уничтожен. Однако после этого WikiLeaks не исчез благодаря эффекту «массового зеркалирования»: тысячи сторонников проекта копировали сайт и выкладывали в интернет свои версии, распространяя IP-адреса через социальные сети [21] .

Администрация Обамы объявила федеральным служащим, что выложенные в рамках проекта WikiLeaks материалы остаются секретными – даже несмотря на то, что их опубликовали ведущие СМИ планеты, включая газеты New York Times и Guardian. Федеральных служащих известили о том, что чтение этих материалов на WikiLeaks.org или в New York Times будет приравнено к нарушению режима секретности [22] . Правительственные учреждения, такие как Библиотека Конгресса, Министерство торговли и армия США, заблокировали доступ к материалам WikiLeaks в своих сетях. Блокировка распространялась не только на государственный сектор. Чиновники из правительства США известили высшие учебные заведения, что студентам, которые надеются поступить на госслужбу, стоит воздержаться от использования в своих работах опубликованных WikiLeaks материалов и не читать их в интернете.

Финансовая цензура: банковская блокада

WikiLeaks существует на пожертвования поддерживающих его людей. В декабре 2010 года ключевые банковские и финансовые учреждения, включая VISA, MasterCard, PayPal и Bank of America, поддались неофициальному давлению США и начали отказывать WikiLeaks в предоставлении финансовых услуг. Они блокировали денежные переводы и пожертвования, сделанные через основные кредитные карты. Все эти учреждения зарегистрированы в Америке, однако их доля на мировом финансовом рынке столь велика, что в возможности переслать деньги WikiLeaks и тем самым поддержать его публикации было отказано как гражданам США, так и людям по всему миру.

«Банковская блокада», как назвали ее СМИ, осуществляется без судебных или административных постановлений и на момент публикации данной книги не прекращена. WikiLeaks подал иски в суды различных стран с целью прорвать блокаду и одержал несколько предварительных побед; судебные процессы продолжаются до сих пор. Вследствие блокады WikiLeaks не получает дохода, между тем расходы проекта возросли, и почти два года он использует резервные фонды.

Происходящее демонстрирует, что у властей есть возможность контролировать финансовые операции третьих лиц. Это прямое покушение на экономическую свободу

человека. Более того, блокада, угрожающая существованию проекта WikiLeaks, являет собой пример новой, весьма опасной формы глобальной экономической цензуры [23] .

У ряда людей, предположительно связанных с проектом WikiLeaks, возникли загадочные проблемы с банками – от ошибок в реквизитах до полного закрытия счетов.

Притеснение Джейкоба Аппельбаума и Жереми Циммермана

17 июля 2010 года Джулиан Ассанж должен был участвовать в конференции хакеров HOPE в Нью-Йорке. Он отменил выступление, и за него речь произнес Джейкоб Аппельбаум. После этого правоохранительные органы начали травлю Аппельбаума и его близких. Джейкоба часто задерживали, обыскивали, ему не давали связаться с адвокатом и допрашивали при пересечении границы всякий раз, когда он въезжал в Соединенные Штаты или выезжал из них. Его технику изымали, права нарушали, угрожая при этом еще бóльшими проблемами. Аппельбаума задерживали и преследовали больше десятка правоохранительных учреждений США – от иммиграционной и таможенной полиции, подчиняющейся Министерству национальной безопасности, до сухопутных войск. Во время задержаний на Аппельбаума оказывали давление – вплоть до того, что не разрешали пользоваться туалетом. При этом ему не предъявляли никаких обвинений, представители властей так ни разу и не объяснили, по какой причине Джейкоба Аппельбаума подвергают травле [24] .

В середине июня 2011 года Жереми Циммерман, собирающийся подняться на борт самолета в вашингтонском аэропорту «Даллес», был задержан двумя людьми, представившимися агентами ФБР. Они начали задавать вопросы, касающиеся WikiLeaks, угрожая при этом арестом и тюремным заключением.

Аппельбаум и Циммерман – лишь двое из длинного списка друзей, помощников и предполагаемых соратников Джулиана Ассанжа, которых травили и за которыми следили американские власти. В этот список также входят и юристы, и выполнявшие свои профессиональные обязанности журналисты.

Изъятие электронных записей без ордера и «дело о судебном ордере Twitter»

14 декабря 2010 года компания Twitter получила «ордер административного суда». Министерство юстиции США требовало от компании поделиться сведениями, которые могли иметь отношение к расследованию деятельности WikiLeaks. Бумага из суда представляла собой «ордер 2703 (d)» с отсылкой к закону о сохраненной информации (Stored Communications Act). Согласно ему, правительство США имеет право добиваться раскрытия записей приватных электронных разговоров без выданного судьей ордера на обыск. По сути, американские власти обходят четвертую поправку к конституции, защищающую граждан от несанкционированных обысков и изъятий.

Судебный ордер требовал выдать названия учетных записей, логи сообщений, адреса, телефоны, реквизиты банковских счетов и номера кредитных карт людей, предположительно связанных с WikiLeaks, включая Джейкоба Аппельбаума, исландского парламентария Биргитту Йонсдоттир, голландского бизнесмена и пионера интернета Ропа Гонгрейпа, а также всю информацию по аккаунту собственно WikiLeaks. Ордер запрещал компании сообщать кому-либо о полученных требованиях. Однако Twitter смог успешно оспорить этот запрет в суде и отвоевал право информировать заинтересованных лиц о том, что власти требуют выдачи их данных.

26 января 2011 года, получив от компании Twitter известие о судебном ордере, Аппельбаум, Йонсдоттир и Гонгрейп, чьи интересы представляли адвокатское бюро Keker and Van Nest, Американский союз защиты гражданских свобод и Фонд электронных рубежей, подали через представителей ходатайство об отмене ордера. Дело получило огласку как «дело о судебном ордере Twitter» [25] . Адвокат Аппельбаума предъявил также ходатайство с требованием обнародовать остающиеся засекреченными протоколы судебных

заседаний, на которых власти пытались получить конфиденциальные данные Аппельбаума от Twitter и других компаний. 11 марта 2011 года мировой судья отклонил оба ходатайства. Истцы обжаловали это решение.

9 октября 2011 года газета Wall Street Journal сообщила, что калифорнийский провайдер электронной почты Sonic.net также получил ордер с требованием выдать сведения о Джейкобе Аппельбауме. Компания оспорила ордер в суде и проиграла, однако получила разрешение предать огласке тот факт, что ее вынудили раскрыть информацию об Аппельбауме. По сведениям Wall Street Journal, аналогичный ордер получила и компания Google, однако был ли он оспорен в суде, газета не сообщила [26] .

10 ноября 2011 года федеральный судья отклонил иски Аппельбаума, Йонсдоттир и Гонгрейпа и обязал Twitter предоставить Министерству юстиции затребованные им сведения [27] . 20 января 2012 года истцы обжаловали решение судьи, оспорив отказ раскрыть информацию об ордерах, которые получили другие компании [28] . На момент выхода этой книги дело еще не было завершено.

Усиление коммуникации против усиления слежки

ДЖУЛИАН: В начале 1990-х, когда запрет криптографии на государственном уровне породил движение шифропанков, многие верили в могущество интернета, который должен был гарантировать всем нам свободную и неподцензурную – по сравнению с обычными СМИ – коммуникацию. Однако шифропанки всегда понимали, что у свободы Сети есть обратная сторона: возможность следить за любым обменом информацией во всей полноте. Сегодня усиленной коммуникации противопоставлена усиленная слежка. Под «усиленной коммуникацией» подразумевается наличие у вас дополнительных степеней свободы по сравнению с теми, кто пытается контролировать чужие идеи; усиление слежки означат обратное.

Сегодня слежка куда более заметна, нежели в те времена, когда поток информации просматривали только американцы, британцы, русские и власти некоторых других стран вроде Швейцарии и Франции. Теперь за Сетью внимательно наблюдают все, практически каждое государство, слежка приобрела массовый характер, она коммерциализируется. Сегодня она становится тотальной: люди рассказывают в интернете обо всех своих политических пристрастиях, о семейных и дружеских связях. Таким образом, усилилась не только слежка за общением людей, существовавшая и ранее, – расширилась сама коммуникация. Причем увеличился как ее объем, так и число типов коммуникации. Новые типы, ранее бывшие приватными, ныне перехватываются в массовом порядке.

Идет битва между силой сведений, собранных информаторами и теневыми структурами, которые постепенно образуются, расширяют связи друг с другом и с частным сектором, и возросшей мощью обычных людей и интернета, ставшего для человечества привычным средством связи.

Я хотел бы поговорить о том, как нам следует рассказывать о наших идеях. Передо мной стоит большая проблема: как человек, не понаслышке знакомый с государственной слежкой и понимающий, как далеко транснациональная индустрия безопасности зашла за последние двадцать лет, я слишком хорошо обо всем этом осведомлен и потому не могу посмотреть на ситуацию глазами обывателя. Однако теперь мой мир – мир всех и каждого: все мы выложили в интернет суть нашей жизни. Мы обязаны как-то рассказывать о том, что нам известно, пока мы можем это делать.

ЭНДИ: Я предлагаю посмотреть на ситуацию не с точки зрения обычного гражданина, а с точки зрения человека, облеченного властью. Не так давно я побывал в Вашингтоне на одной странной конференции и увидел парней с беджами немецкого посольства. Я подошел к ним и сказал: «Ух ты, вы из посольства Германии», – а они сказали: «Ну, не совсем из посольства, мы на деле из-под Мюнхена». Выяснилось, что они представляют внешнюю разведку, и на вечернем фуршете я у них поинтересовался: «Так в чем же суть секретности?» Они ответили так: «Главное – замедлить процессы, чтобы лучше их контролировать». В этом

и заключается их агентурная работа: они замедляют процесс, чтобы люди не поняли, что происходит. Объявить что-то секретным – значит ограничить круг тех, кто обладает знаниями и может на это воздействовать. Если посмотреть на Глобальную сеть с точки зрения власть имущих, последние двадцать лет – страшные годы. Власти воспринимают интернет как болезнь, которая затрудняет их возможность влиять на происходящее и ограничивать знания людей и их способность воздействовать на реальные процессы. Взять хотя бы Саудовскую Аравию, где по какому-то историческому совпадению религиозные вожди и владельцы большей части страны – это одни и те же люди: их заинтересованность в переменах равна нулю. Где-то от нуля до минус пяти, может быть. Они воспринимают интернет как болезнь и спрашивают консультантов: «Есть у вас лекарство от этой штуки? Если интернетная зараза появится в нашей стране, нам нужен иммунитет». Ответ – тотальная слежка. Консультанты говорят: «Нам нужен полный контроль над этой штукой, нам нужны фильтры, нам необходимо знать обо всем, что делается в Сети». Вот что происходило в последние двадцать лет. Власти вкладывались в слежку как могли – они страшились, что интернет станет им помехой.

ДЖУЛИАН: И все-таки вопреки тотальной слежке миллионы людей благодаря массовой коммуникации могут быстро прийти к согласию. Если у нас получится очень быстро перейти из обычного состояния в новое состояние согласия масс, государству, даже способному наблюдать за процессом, не хватит времени, чтобы дать эффективный ответ. С другой стороны, вспомним о том, что в 2008 году в Каире прошла акция протеста, организованная через Facebook. Она застала правительство Мубарака врасплох, и в итоге протестующих выследили через тот же Facebook [29] . В 2011 году в «руководстве революционера», одном из важнейших документов тех египетских событий, самая первая страница призывала «не использовать Twitter или Facebook», чтобы распространять это руководство – и на последней странице стояло то же самое предостережение [30] . Тем не менее множество египтян использовали и Twitter, и Facebook. Эти люди выжили лишь потому, что революция получилась успешной. Если бы она провалилась, все они оказались бы в очень, очень тяжелом положении. Не стоит забывать и о том, что президент Мубарак уже на ранней стадии отрезал Египет от Сети. Помогло революции отключение интернета или навредило – это еще вопрос. Некоторые считают, что помогло – люди стали выходить на улицу, чтобы узнать новости, а когда ты на улице – ты на улице. Когда перестают работать мобильник и интернет, поневоле заволнуешься.

Революция должна быть успешной, ей нужна критическая масса участников, она должна случиться стремительно и победить – в противном случае инфраструктуру, позволившую людям быстро прийти к согласию, используют, чтобы выследить и изолировать тех, кто все это организовал.

Так обстояли дела в Египте, а Египет – да, союзник США, но не часть англоязычного разведывательного альянса, куда входят США, Великобритания, Австралия, Новая Зеландия и Канада. Давайте представим себе, что египетская революция начинается в Америке. Что произошло бы с сетями Facebook и Twitter? Государство взяло бы их под контроль. И если бы революция потерпела поражение, ЦРУ и ФБР стали бы извлекать из социальных сетей сведения о главных зачинщиках, как это происходит сейчас.

ЖЕРЕМИ: Слежку трудно отделить от контроля. Нам нужно говорить и про слежку, и про контроль. Это больше моя тема – контроль над интернетом со стороны правительств или корпораций.

ДЖЕЙКОБ: Думаю, не надо объяснять, что цензура – побочный продукт любой слежки вообще, будь то самоцензура или настоящая техническая цензура, и мне кажется, именно это важно донести до обычных людей, не углубляясь в технические дебри. Скажем, если б мы прокладывали дороги так, как строим интернет, на каждой стояли бы камеры слежения и микрофоны, доступ к которым имела бы только полиция – или люди, успешно притворяющиеся полицией.

ДЖУЛИАН: Джейк, в Великобритании дела так и обстоят.

ДЖЕЙКОБ: Когда компания строит дорогу, от нее не требуют оснастить каждый квадратный сантиметр высококлассными приборами слежения, передающими данные некоему тайному обществу. Если обычным людям объяснить, что именно так мы строим дороги в интернете и потом призываем ими пользоваться, люди поймут аналогию и осознают: контролировать дорогу не всегда будут те, кто ее создавал.

ЭНДИ: А кое-кто и дорог-то не строит. Он разбивает в интернете сад и предлагает всем раздеться. Да, я про Facebook! Бизнес, который приносит людям радость, раскрывая сведения о них всем подряд.

ДЖЕЙКОБ: Именно. В ГДР информаторов вознаграждали за то, что они работали на Штази – орган госбезопасности, – и точно так же их теперь вознаграждают за наличие аккаунта в Facebook. Только Facebook платит не деньгами, а социальным кредитом – соцсеть позволяет тебе переспать с соседом. Тут важно говорить именно о человеческом аспекте, потому что дело не в технике как таковой, а в контроле посредством слежки. Местами это совершеннейший паноптикон [31] .

ДЖУЛИАН: Меня занимает философия технологии. Под технологией я понимаю не какой-то прибор, а, скажем, согласие большинства в правлении или структуру парламента – то есть системное взаимодействие. Например, я полагаю, что феодальные системы породила мельничная технология. Как только благодаря громадным инвестициям мельницы оказываются централизованы, их чисто физически становится легко контролировать – и естественным образом появляются феодальные отношения. В ходе истории мы, видимо, учились создавать все более сложные технологии. Некоторые из них совместимы с демократией, и доступ к ним может быть обеспечен всем и каждому. Но бóльшая часть технологий из-за своей сложности порождает в итоге весьма сплоченные организации вроде корпорации Intel. Не исключено, что любая технология по своей природе проходит через периоды открытия, централизации и демократизации, когда знание о ней передается следующему, более образованному поколению. Но мне сдается, что основное свойство технологии – это сосредоточение контроля над ней в руках тех, кому принадлежат необходимые данной технологии физические ресурсы. Показательный пример тут – производство полупроводников. Для него нужен абсолютно чистый воздух, нужен завод, на котором тысячи работников обязаны носить специальные головные уборы, чтобы ни один кусочек кожи, ни один волосок не помешали многошаговому и чрезвычайно сложному процессу. Компания, создающая полупроводники, обладает миллионами часов научных наработок. Если это популярный продукт – а полупроводники именно таковы, на них держится весь интернет, – значит, освобождение интернета завязано на производство полупроводников. Оно же, в свою очередь, зависит от способности тех, кто физически контролирует завод, находить дешевое сырье.

Следовательно, основа революции высокотехнологичных коммуникаций – и основа свободы, которой мы благодаря этим коммуникациям способны обладать, – неолиберальная, транснациональная, глобализированная рыночная экономика современности. На деле интернет – верхушка айсберга. Высота, которую, если мы говорим о достижениях технологии, современная экономика может взять. Интернет зиждется на очень сложных торговых связях между производителями оптоволоконного кабеля, производителями полупроводников, горнодобывающими компаниями, которые извлекают из-под земли сырье, а также здесь не обойтись без финансовой смазки, которая делает возможной торговлю, без судов, стоящих на страже законов о частной собственности, и т. д. В реальности интернет – это вершина пирамиды всей неолиберальной системы.

ЭНДИ: Что касается технологии, после того как Иоганн Гутенберг изобрел печатный станок, его время от времени запрещали в разных частях Германии, именно потому книгопечатание и распространялось: его запрещали в одной местности, оно перемещалось в другую юрисдикцию [32] . Я не изучал эту историю в деталях, но знаю, что печатников преследовала католическая церковь, поскольку те нарушали ее монополию на изготовление книг, и когда у них появлялись проблемы с законом, они переезжали туда, где

книгопечатание было разрешено. Запрет по-своему помогал распространять печатные станки. С Сетью, думаю, все происходило чуть по-другому. У нас появились машины, которые можно было применять как средство производства, – даже Commodore 64, хотя большинство использовало его для других целей.

ДЖУЛИАН: На каждом маленьком компьютере можно запускать собственное программное обеспечение.

ЭНДИ: Именно. А еще при помощи компьютера можно распространять идеи. Но, с другой стороны – и это философский аргумент, – в начале 1990-х, когда интернет вышел на глобальный уровень, один из основателей базирующегося в США Фонда электронных рубежей Джон Гилмор заметил: «Сеть интерпретирует цензуру как нечто вредное и обходит ее стороной» [33] . Как мы знаем сегодня, это была техническая трактовка пополам с оптимистическим взглядом на перспективы интернета, своего рода попытка принять желаемое за действительное – и одновременно самоисполняющееся пророчество.

ДЖУЛИАН: Но это было верно для Юзнета, который появился около тридцати лет назад и представляет собой, если угодно, множество связанных друг с другом электронных почтовых ящиков. Чтобы понять, что такое Юзнет, вообразите, что нет разницы между людьми и серверами и у каждого есть свой юзнетовский сервер. Вы пишете что-то и передаете файл одному или двум людям. Те (автоматически) проверяют, не получали ли они ваше послание раньше. Если нет, они принимают его и рассылают всем, с кем у них есть связь, и т. д. В результате послание дойдет до каждого, и у всех будет по копии. Если некто начнет подвергать файлы цензуре, его попросту проигнорируют, на Юзнет это не повлияет. Послание дойдет до всех, кто не является цензором. Гилмор говорил о Юзнете, а не об интернете. И он не имел в виду сайты.

ЭНДИ: Это технически верное замечание, но интерпретация слов Гилмора и их долгосрочное воздействие породили людей, которые осознавали себя как интернет. Они говорили: «Ладно, цензура есть, но мы ее обойдем», – а политик, не разбиравшийся в технологии, думал: «Черт, эта новая штука ограничивает наш контроль над информационной сферой». Я думаю, Гилмор, один из провидцев шифропанка, сделал великое дело: он вдохновил криптоанархистский взгляд на мир, когда у тебя есть своя версия анонимной коммуникации и ты не боишься, что за тобой будут следить.

ЖЕРЕМИ: По-моему, различные технологии распространяются по-разному – чтобы понять, как работает мельница или печатный станок, надо их увидеть, а сейчас мы все чаще встраиваем систему контроля в саму технологию. Контроль – это часть технологии. В большинстве случаев мы не можем даже открыть современный компьютер, чтобы узнать, из каких компонентов он состоит. И все компоненты спрятаны в маленькие футляры, так что мы не в состоянии понять, что именно они делают.

ЭНДИ: Из-за их сложности?

ЖЕРЕМИ: Из-за сложности и еще потому, что создатели технологии не хотят, чтобы кто-то разобрался в том, как она работает. Ведь речь идет об оригинальной технологии [34] . Кори Доктороу описал это в статье «Будущая гражданская война за компьютеры общего назначения» [35] . Если компьютер универсален, вы можете делать с ним что захотите. Обрабатывать любую информацию на входе, превращать ее во что угодно на выходе. И мы создаем все больше и больше устройств, являющихся компьютерами общего назначения, но работают они только как GPS-навигаторы, или как телефоны, или как MP3-плееры. Мы создаем все больше устройств со встроенной системой контроля, которая запрещает пользователю делать какие-то вещи.

ДЖУЛИАН: Встроенный контроль не позволяет понять, как работает устройство, и переделать его, чтобы оно работало не так, как задумано производителем, а когда устройство подключено к Сети, все становится еще хуже.

ЖЕРЕМИ: Именно, потому что одной из его функций может быть слежка за пользователем и его данными. Вот почему в свободном обществе такое значение имеет свободное ПО.

ЭНДИ: Я абсолютно согласен с тем, что нам нужны машины общего назначения. Но сегодня утром, когда я пытался вылететь сюда из Берлина, лайнер не смог подняться – я столкнулся с таким впервые. Самолет отъехал в сторону, и командир экипажа сказал: «Дамы и господа, наши электрические системы отказали, так что мы решили остановить самолет и перезапустить системы». Я сидел и думал: «Черт, звучит как перезагрузка Windows: клавиши Control + Alt + Delete – вдруг заработает!» И я не слишком огорчился бы, если бы на самолете установили узкоспециальное устройство, которое управляет только самолетом – и делает это очень хорошо. Когда я лечу в самолете, я не хочу, чтобы пилотов отвлек «Тетрис», или вирус Stuxnet, или что-то еще [36] .

ЖЕРЕМИ: Самолет сам по себе не обрабатывает твои личные данные, он не контролирует твою жизнь.

ЭНДИ: Ну, когда самолет летит, он очень даже контролирует мою жизнь.

ДЖЕЙКОБ: Довод Кори, я думаю, можно обобщить так: у нас больше нет машин, самолетов, слуховых аппаратов – у нас есть компьютеры на четырех колесах, компьютеры с крыльями и компьютеры, которые усиливают слух. И вопрос не в том, узкоспециальные они или нет, вопрос звучит по-другому: можем ли мы проверить, делают они именно то, что, как утверждается, они должны делать, или нет, и можем ли мы понять, насколько хорошо они функционируют? Люди сплошь и рядом пытаются доказать, что у них есть право упрятать информацию под замок и держать ее в секрете, поэтому они либо усложняют компьютеры, либо ставят юридические препоны, не позволяющие понять, как машины устроены. Тут есть опасность для общества, потому что, как нам известно, люди не всегда действуют в интересах общества, и мы также знаем, что люди ошибаются – не злонамеренно, – так что убирать информацию под замок очень опасно по ряду причин, в том числе и потому, что никто из нас не идеален. Это факт. Возможность получить доступ к чертежам системы, от которой зависит наша жизнь, – одна из причин, из-за чего такое значение имеет свободное ПО, но потому же нас должно волновать и аппаратное обеспечение, «железо». Оно позволяет делать надежные инвестиции, улучшать используемые системы и проверять, работают ли эти системы так, как должны. Безотносительно свободы: устройство этих систем важно знать еще и потому, что если оно нам не известно, то мы склонны полагаться на власть – на тех, кто либо понимает, как системы работают, либо может их контролировать, даже если незнаком с принципами их функционирования. Вот почему сейчас столько говорят про кибервойну: люди, которые вроде как отвечают за войны, заговорили о технологии так, будто понимают, как она работает. Они часто рассуждают о кибернетической войне, и никто из них – вообще никто – не рассуждает о кибернетическом укреплении мира или о миротворчестве. Они вечно говорят о войне – это их бизнес, и они пытаются взять под контроль технологию и законодательство, чтобы добиться своих целей. Если мы не будем контролировать нашу технологию, эти люди захотят использовать ее в собственных интересах, в частности для ведения войн. Так могут появиться на свет всякие страшные штуки – думаю, именно так был создан червь Stuxnet. С другой стороны, пока Америка воюет, разумные люди говорят, что контроль над технологией способен предотвратить войну. Может, это и хороший довод для государства, которое не атакует постоянно другие страны, но вряд ли он применим к стране, вовлеченной одновременно в несколько военных операций.

Милитаризация киберпространства

ДЖУЛИАН: Я наблюдаю сейчас за милитаризацией киберпространства – точнее, за его оккупацией. Когда вы общаетесь с кем-то через интернет или по сотовой связи, которая сегодня срослась с интернетом, вашу коммуникацию перехватывает военная разведка. Это все равно что жить с танком в спальне. Когда вы шлете SMS жене, между вами стоит солдат. Если говорить о коммуникации, мы все живем по законам военного времени, просто танков не видим – но они есть. До такой степени Сеть, которая должна была стать гражданским пространством, превратилась в пространство милитаризованное. Но интернет – это наш

космос, все мы используем его для общения друг с другом и с членами наших семей. Коммуникация, составляющая ядро частной жизни, перешла в интернет. Так что на деле наша частная жизнь попала в военную зону. Как если бы солдат притаился под нашей кроватью. Милитаризуется уже сама гражданская жизнь.

ДЖЕЙКОБ: Не так давно мне пришло приглашение из исследовательской лаборатории безопасности и секретности Вашингтонского университета с просьбой потренировать команды этой лаборатории – она хотела принять участие в соревнованиях по киберзащите студентов Тихоокеанского региона. В последний момент меня попросили их консультировать. Мы много тренировались, чтобы поучаствовать в кибервойне, в которой SPAWAR, гражданская организация в составе ВМС США – она проводит пентесты, занимается агрессивным и оборонительным хакингом, – играла роль «красной команды» [37] . Она атакует всех прочих игроков, и задача твоей команды – защитить компьютерную систему, которую тебе дают в начале игры, причем ты заранее ничего об этой системе не знаешь. Ты понятия не имеешь, какую систему тебе придется защищать, вначале не ясно даже, как начисляются очки, и тебе остается только лезть вон из кожи и надеяться на победу.

ДЖУЛИАН: Ты уверен, что вы действительно играли? Может, это была совсем не игра!

ДЖЕЙКОБ: Нет, тебе дают несколько компьютеров – и ты должен их защищать, а «красная команда» ломает твою защиту и перехватывает контроль над системой. Что-то вроде детской версии «Захвата флага» на настоящей хакерской конференции. Очень любопытное соревнование – у этих парней полно «отмычек», и они сами пишут свои программы [38] .

ДЖУЛИАН: И какой в этом смысл – с точки зрения ВМС США?

ДЖЕЙКОБ: В данном случае они спонсируют игру, потому что хотят найти потенциальных киберсолдат. Я принес тебе блокнот с логотипом ЦРУ – эта организация занималась на игре вербовкой. Там присутствовал парень по имени Чарли – Чарли из ЦРУ, – он объяснял, что, если ты хочешь устроиться в ЦРУ, это отличная возможность найти работу в реальном мире. Там были представители SPAWAR и Microsoft, они тоже вербовали людей. Идея в том, чтобы натаскать всех игроков, все команды, лучшие из них сразятся на чемпионате страны и «защитят государство» – и в качестве киберсолдат смогут потом иметь дело не только с кибероборонойо, но и с кибератаками. Мы набрали на игре что-то около 4000 баллов, в сумме столько же, сколько второе, третье и четвертое места. На деле мы сыграли лучше их всех, вместе взятых.

ДЖУЛИАН: Ну да, ну да…

ДЖЕЙКОБ: Я тут ни при чем – не думаю, что я такой уж хороший тренер, мой лозунг звучал: «Темнее всего перед тем, как приходит полная тьма», – просто ребята были настоящие гении. Игра получилась любопытная, насквозь военная. Допустим, тебе говорят: «Эй, мы хотим услышать ваш боевой клич!» А ты такой: «Простите, что?..» Нас об этом спросили на обеде, в перерыве между сражениями. На игре только и говорили, что об атакующих системах, о войне, кибервойне, величии военного образа мысли. И вот что интересно: если не считать команду, с которой я работал, в игре участвовало множество людей, что сражались, но не по «Искусству войны», а скорее как на турнире «Кубок сисадмина», обороняя свои системы любыми средствами, и это было омерзительно [39] . Я с ужасом смотрел на людей с военным опытом, которые думали по-военному, но не обучали свои команды стратегии, а громогласно призывали их защищать системы – или же атаковать системы, – и для них это было самое настоящее поле боя, они сочились патриотическим пафосом. Они не пытались развивать творческий подход или поощрить независимый анализ – нет, они требовали от других работать, подобно винтикам, и исполнять приказы во имя народного блага. Я такого никогда раньше не видел. Меня от них тошнило, и почти все мои ребята с трудом переваривали таких людей, они не могли воспринимать их всерьез.

ДЖУЛИАН: Как ты думаешь, может быть, это стандарт для учений ВМС США, который теперь пытаются применить в других областях? Стандарт, установленный

решением – международным стратегическим решением – киберкомандования Соединенных Штатов?

ЭНДИ: Похоже на детские тренировочные лагеря нацистов.

ДЖЕЙКОБ: Sie können das sagen weil du bist Deutsche [40] . Нет, не похоже. BMC участвует в этой игре постольку, поскольку ее финансирует правительство США. Им нужен был тренер, они нашли меня, и я согласился – мне понравилась моя команда, студенты последнего курса. На деле происходит вот что: власти США убеждают людей биться за родину – и пытаются внушить им патриотические чувства. Это была чрезвычайно странная игра: с одной стороны, неплохо знать, как обезопасить систему, и понимать, как работает инфраструктура, от которой зависят наши жизни; с другой – власти не пытались убедить участников во всем этом разобраться, они хотели пробудить в них патриотический пыл, чтобы люди, выполняя подобную работу, были счастливы.

ЭНДИ: Как ни жаль, заинтересованность Соединенных Штатов в безопасности систем очень ограниченна – им нужны уязвимые системы, чтобы можно было захватить над ними контроль. Сегодня криптозащита контролируется не так жестко, как предлагали США около 1998 года, когда отвечавший за международную коммерцию замминистра торговли Дэвид Аарон ездил по миру и ратовал за то, чтобы дать правительству доступ к зашифрованным паролям любого пользователя [41] . Однако криптография все равно считается так называемой технологией двойного применения, и во многих странах ее экспорт в качестве продукта для конечного потребителя ограничен законом, а на мировом уровне данный вопрос регулируют Вассенарские соглашения [42] . В контексте объявления каких-то стран и их действий «злом» это, может, и верное решение, но налицо двойные стандарты – скажем, экспорт технологии телекоммуникационной слежки ограничен в куда меньшей степени [43] .

ДЖУЛИАН: Энди, ты много лет работал над созданием криптографических телефонов. О каких видах массовой слежки можно говорить применительно к средствам связи? Каков последний технологический тренд в области «оптовой» слежки и правительственной разведывательной индустрии?

ЭНДИ: Массовое накопление информации. Иначе говоря, власти сохраняют всю телекоммуникацию, все голосовые звонки, весь инфопоток сообщений, любые групповые рассылки SMS, а также данные по интернет-соединениям, в ряде ситуаций ограниченные по крайней мере электронными письмами. Если сравнить военный бюджет с расходами на кибервойну, окажется, что обычное вооружение стоит кучу денег, так что киберсолдаты или массовая слежка чрезвычайно дешевы по сравнению, скажем, с одним самолетом. Один-единственный истребитель стоит…

ДЖУЛИАН: Около ста миллионов.

ЭНДИ: А хранение информации дешевеет с каждым днем. Компьютерный клуб Chaos подсчитал, что хранение с приличным качеством звука всех телефонных разговоров по Германии за год обойдется примерно в 30 миллионов евро, включая административные расходы, а само по себе хранение стоит около 8 миллионов [44] .

ДЖУЛИАН: Есть еще компании вроде южноафриканской VASTech, продающие подобные услуги за 10 миллионов в год [45] . «Мы перехватим все ваши звонки и сохраним их для вас». За последние два года подход изменился: раньше перехватывался весь инфопоток из одной страны в другую, потом власть выбирала конкретных индивидов, за которыми хотела следить, и прослушивала их коммуникацию, а теперь перехватывается и сохраняется вообще все – и навечно.

ЭНДИ: Если говорить в общих чертах, ситуация развивалась следующим образом. Раньше гражданина прослушивали, если он занимал дипломатический пост, работал в какой-то компании, подозревался в чем-то или контактировал с людьми, которые делали что-то не то, – и тогда за человеком начинали следить. Сегодня считается, что эффективнее поступать так: «Мы сначала сохраним всю информацию, а потом ее рассортируем». Власти сохраняют инфопоток на долгосрочную перспективу, и деятельность всей индустрии можно разделить на «тактический» и «стратегический» подходы. Тактический сводится вот к чему:

«Прямо сейчас, во время собрания, нужно нашпиговать помещение “жучками”, заслать внутрь агента с микрофоном, в начиненной электроникой одежде, развернуть из автомобиля системы слежения GSM (Global System for Mobile communications, Глобальная система мобильной коммуникации), чтобы перехватывать разговоры сразу, не обращаясь к оператору сотовой связи, не получая полицейский ордер на обыск или другие бумажки, без каких-либо юридических процедур». Стратегический подход подразумевает, что мы делаем все то же самое по умолчанию, записываем все подряд и позднее сортируем материалы при помощи аналитических систем.

ДЖУЛИАН: То есть стратегический перехват – это сохранение всего того, что передает спутник связи, и того, что идет по оптоволоконному кабелю.

ЭНДИ: Да, потому что никогда не знаешь, кого и в чем будешь подозревать.

ДЖЕЙКОБ: В Соединенных Штатах рассматривалось дело Агентства национальной безопасности (АНБ) и компании AT&T – второе дело, «Хептинг против AT&T». В Фолсоме, штат Калифорния, Марк Клейн, бывший технический работник телекоммуникационного гиганта AT&T, сообщил, что АНБ сохраняло всю информацию, которую могло получить от AT&T. Они забирали ее оптом – сетевое общение и телефонные звонки, – а значит, всякий раз, когда я звонил по телефону или подключался к Сети в Сан-Франциско в период, о котором говорил Марк Клейн, АНБ получало всю информацию. Оно действовало на территории США против американских граждан [46] . Я более чем уверен в том, что АНБ использовало перехваченную информацию в расследованиях, которые власти проводили, чтобы доказать вину тех или иных людей, и здесь есть множество интересных нюансов, связанных с конституционными правами, – ведь хранить эту информацию они собираются вечно.

ЖЕРЕМИ: Еще есть пример системы Eagle, которую французская компания Amesys продала ливийскому диктатору Каддафи, и в коммерческом договоре значилось: «Механизм перехвата информации в масштабах страны». По сути это была большая коробка: устанавливаешь ее где-либо – и прослушиваешь разговоры всех своих подданных [47] .

ДЖУЛИАН: Десять лет назад тотальная слежка казалась фантастикой, в нее верили только параноики, но сегодня стоимость массового перехвата снизилась до того, что даже страны вроде Ливии со сравнительно небольшими ресурсами могут позволить себе приобретать французскую технологию. Большинство стран мира уже перехватывают все инфопотоки. Следующий прорыв случится, когда власть научится понимать перехваченную и сохраненную информацию и эффективно на нее реагировать. Сегодня во многих странах идет стратегический перехват всего инфопотока внутри государства, а также инфопотока из страны вовне, но что касается последующих действий – автоматической блокировки банковского счета и развертывания полицейской операции, обособления каких-то одних групп и освобождения от ответственности других, – до этого еще не дошло. Siemens продает платформу для разведки с автоматическим реагированием. То есть когда цель А появляется в стольких-то метрах от цели Б – а это можно определить по перехваченным данным сотовых телефонов – и цель А получает электронное письмо с неким ключевым словом, производится такое-то действие. Вот что нас ждет.

Борьба с тотальной слежкой по законам человеческим

ЖЕРЕМИ: Факт, что сегодня технология позволяет полностью отслеживать всяческую коммуникацию. Но у данной монеты есть и другая сторона, а именно – что мы можем сделать с этим. Надо признать, что упомянутая тобой тактическая слежка в ряде случаев применяется вполне законно: следователям, которые занимаются плохими парнями, сообществами плохих парней и т. д., использование таких средств может быть при необходимости разрешено под надзором суда. Вопрос в том, где проходит граница между судебным надзором и контролем граждан над применением подобных технологий. Это политический вопрос. Когда возникают такие вопросы, политиков, которые не понимают, о каких технологиях идет речь, просят всего лишь подписать бумагу. Я думаю, что мы,

граждане, должны не просто объяснять – в том числе политикам, – как это вообще функционирует, но и вступать в политические дебаты по вопросам использования таких технологий. Я знаю, что в Германии возникло массовое движение против сохранения обобщенной информации, в результате чего конституционный суд отменил соответствующий закон [48] . В ЕС продолжают спорить о пересмотре Директивы о сохранении информации [49] .

ЭНДИ: Ты говоришь о теории демократического государства, которому, конечно, нужно выявлять тут и там плохих парней и прослушивать их телефонные разговоры на основании судебного решения – плюс вести надзор за тем, чтобы прослушка осуществлялась по правилам. Беда в том, что власти должны исполнять законы. Если власти этого не делают, зачем они вообще нужны? Особенно необходимо исполнять законы в части стратегического подхода. А демократические страны Европы оптом закупают аппаратуру, которая позволяет им перехватывать инфопоток, действуя за рамками закона. Судебное решение им не нужно, они просто включают машину и прослушивают тебя – и такую технологию никак не проконтролируешь.

ДЖУЛИАН: Правильно ли будет сказать, что с массовой государственной слежкой можно бороться двумя способами: по законам физики и по человеческим законам? Первый способ – создавать устройства, которые предотвращают перехват. Второй – ввести демократический контроль, то есть принимать законы, запрещающие прослушку без ордера и т. д., и пытаться регулировать слежку на практике. Однако стратегический перехват так просто не одолеешь, его невозможно целенаправленно ограничить законами. Стратегический перехват означает, что вся информация сохраняется вне зависимости от того, виновен человек или нет. Мы должны помнить, что такая слежка ведется именно сильными мира сего. Политики никогда не пойдут на разоблачение государственной слежки. Между тем технология сама по себе столь сложна, а ее использование столь засекречено, что никакой демократический надзор тут не поможет.

ЭНДИ: Еще можно следить за собственным парламентом.

ДЖУЛИАН: При этом всегда можно оправдать слежку – сославшись на мафию, на иностранную разведку, – чтобы народ согласился с созданием такой системы.

ДЖЕЙКОБ: Четыре всадника Инфокалипсиса: детская порнография, терроризм, отмывание денег и война с некоторыми наркотиками.

ДЖУЛИАН: И если такая сложная и секретная на уровне проекта система уже создана, разве возможно контролировать ее политическими средствами? Я думаю, если убрать за скобки очень маленькие страны вроде Исландии, законы и политики не в состоянии взять массовый перехват под контроль – разве что в государстве произойдет революция. Законы тут бессильны. Слишком дешево и просто обойти политиков и следить за людьми без их ведома. В 2008 году шведский парламент принял закон о перехвате информации, так называемый FRA-lagen, по которому шведская разведка, занимающаяся криптоанализом, или FRA, может законно перехватывать любую информацию в любом количестве внутри страны и переправлять ее в Соединенные Штаты – с некоторыми оговорками [50] . Но если уж созданы система перехвата и организация, секретно шпионящая за людьми, о каких оговорках может идти речь? Выполнить требования закона нереально. И действительно, появились судебные дела, доказывающие, что FRA не раз нарушала закон. Многие страны следят за гражданами вообще без всяких законов. И это очень крупное везение, если, как в Швеции, власти решают защитить от преследования самих себя и меняют законодательство. Это, кстати, типичная реакция – когда речь идет о массовой слежке, закон принимается лишь для того, чтобы прикрыть задницу самих следящих. Что касается технологии, она очень сложна; например, когда в Австралии и Великобритании обсуждался закон, который позволил бы перехватывать все метаданные, большинство не понимало, чем именно они ценны и что вообще значит само это слово [51] . Перехват метаданных подразумевает создание системы, которая физически перехватывает всю информацию и потом отбрасывает все, кроме метаданных. Но такой системе нельзя доверять. Понять, что именно она

перехватывает и сохраняет, можно одним способом – привлекая очень опытных инженеров, которые обладают правом войти в систему и посмотреть, что именно она делает, а политики не склонны давать кому-то такое право. Проблема становится все менее разрешимой, потому что сложность и секретность – это гремучая смесь. Система непрозрачна из-за сложности. И непрозрачна из-за секретности. В нее встроена бесконтрольность. Таково свойство системы. Она опасна по определению.

ЖЕРЕМИ: Я не говорю, что политический подход работает. Я говорю о том, как в теории функционирует демократическое государство – и действительно, даже внутри такого теоретического государства имеются спецслужбы, которым позволено то, что запрещено обычным полицейским и следователям. И даже если мы должным образом ограничим законами обычных следователей, те, кто использует технологии слежки, никуда не исчезнут. На самом деле вопрос заключается вот в чем: должны ли мы, вместо того чтобы контролировать использование технологий, взять под контроль торговлю и владение ими?

ДЖУЛИАН: Речь идет об аппаратуре для массовой слежки, которая перехватывает инфопотоки половины страны или города.

ЖЕРЕМИ: Именно. Это как с ядерным оружием: вы не можете просто взять и продать ракету, и хотя некоторые страны желают создать свое ядерное оружие, у них возникают проблемы. Когда мы говорим о системах вооружения, регулирование идет на уровне технологии, а не ее использования. Я думаю, дискутировать надо о том, должны ли технологии массовой слежки расцениваться как военные.

ДЖЕЙКОБ: Да и нет. Когда это оружие – а в странах вроде Сирии или Ливии оборудование для слежки превращается в оружие, – его применяют специфически, чтобы выявить политических оппонентов. Французская компания Amesys прослушивала британцев, используя технику, применять которую законы Франции запрещают, и успешно продавала свои услуги [52] .

ЭНДИ: Во Франции они на такое не пошли бы, да?

ДЖЕЙКОБ: Ну, Amesys поймали за руку, когда The Spy Files опубликовали ее внутренние документы [53] . Рассуждая о данной технологии как об оружии, мы должны помнить, что это не грузовик. Тот, кто продает ее какой-то стране, предоставляет ей грузовик, механика и команду снайперов, которые ездят в кузове, выбирают людей по какому-то признаку и убивают их.

ДЖУЛИАН: Скорее это целая армия грузовиков.

ЭНДИ: Любопытно, как регулируется использование криптографии. Есть Вассенарские соглашения, они применяются на международном уровне – то есть вы не можете экспортировать шифровальные технологии, которые помогают обезопасить покупателя от слежки, в страны, объявленные плохими или – по каким-то причинам – проблемными. Но если вы продаете оборудование для слежки, ограничений нет. Никаких запретов на экспорт. Причина, я полагаю, проста: даже у демократических правительств есть свой интерес, и он состоит в том, чтобы осуществлять контроль. Даже торгуя с плохими странами и поставляя им оборудование для слежки, чтобы они делали ужасные вещи, вы выигрываете, потому что узнаёте, кого именно власти этой страны прослушивают, чего боятся, кто в стране возглавляет оппозицию, кто организует политические мероприятия и т. д. Значит, вы в силах предсказать грядущие события, понять, кого вам следует финансировать, и т. д. Я вижу тут очень грязную игру, которая идет между государствами, и возможна она потому, что продажа технологий для слежки законом никак не регулируется.

ДЖУЛИАН: Я бы остановился на аналогии между массовой слежкой и оружием массового уничтожения. Законы физики позволили создать атомную бомбу, и с ее появлением изменилась геополитика, изменилась жизнь множества людей, хоть и по-разному – кто-то, наверное, стал жить лучше, кто-то ощутил себя на краю полного апокалипсиса. Появились соглашения по контролю, которые пока что – если не считать Японии – спасали нас от ядерных ударов. При этом факт применения и неприменения ядерного оружия очевиден. За последние десять лет массовая слежка очень сильно

усложнилась и подешевела: мы живем в эпоху, когда население удваивается каждые двадцать пять лет, между тем мощность слежки удваивается каждые полтора года. Кривая роста слежки круче кривой роста населения. Слежки не избежать. Сегодня за 10 миллионов долларов можно купить аппаратуру, способную непрерывно сохранять перехваченные инфопотоки страны средних размеров. Должна ли наша реакция быть эквивалентной? Демократия и свобода по всему миру оказались под очень серьезной угрозой, на нее нельзя не реагировать, точно так же как нельзя не реагировать на угрозу атомной войны – и нельзя не контролировать ядерное оружие, пока мы способны это делать.

ЭНДИ: В Ливии я видел, как демократически настроенные повстанцы ворвались на станции слежения, забрали записи, доказали, что западные компании помогали режиму Каддафи подавлять политические акции, а потом новое правительство прибрало станции слежения к рукам и теперь снова эксплуатирует их на полную мощность [54] . Я согласен, что контроль над технологией – идея хорошая, но вместе с тем я скептически отношусь к противопоставлению интересов граждан и властей. Я бы даже не говорил о правительствах, потому что властью обладает тот, у кого есть возможность прослушивать все телефонные разговоры. То же самое с ценами на бирже – с чисто экономической точки зрения вы заработаете кучу денег, если знаете, что именно происходит.

ДЖУЛИАН: В странах, где есть законы, определяющие задачи основных агентств электронной разведки – таких как АНБ в Америке, ЦПС (Центр правительственной связи) в Великобритании, УРО (Управление радиотехнической обороны) в Австралии, – их изменили, добавив к задачам экономическую разведку. Скажем, когда Австралия и США вступают в борьбу за поставки пшеницы, они шпионят за всеми, кто вовлечен в эту сделку. Так повелось с давних пор, уже лет десять о такой слежке говорят в открытую, – и понятно, что подобного не избежать. Началось все с торговли оружием: компании вроде Lockheed Martin, Raytheon и Northrup заключали сделки на поставку вооружений – и они же разрабатывали системы массового перехвата информации, потому что были близки к властям. Торговцы оружием получали помощь от друзей и покрывали перехват информации о сделках в интересах национальной безопасности. Сейчас такие перехваты касаются всего, что способно обогатить страну, то есть практически любой сферы жизни.

ДЖЕЙКОБ: Хорошая аналогия: в декабре 2011 года на коммуникационном конгрессе Chaos говорили о том, что технология массовой слежки, особенно тактическая, но и стратегическая тоже, напоминает мины [55] . Очень мощная штука. То, что подобный сценарий вероятен, не означает, что мы неизбежно пойдем именно по этому пути, тем более пройдем его до конца, когда следить будут за всеми и каждым. Правда, против нас действуют экономические факторы. Кто-то объяснял мне, что в Норвегии телефонная система функционировала так: некий счетчик крутился быстрее или медленнее в зависимости от того, как далеко вы находились в момент дозвона. Закон запрещал норвежской телефонной компании хранить информацию или вести учет метаданных по вашим звонкам, скажем, фиксировать номер, с которого вы звонили, – это был отголосок Второй мировой войны, когда норвежцы беспокоились о приватности. Так что вполне можно создать технологию, которая защищает приватность и при этом работает в условиях рыночной экономики, принося прибыль. Но, например, бой за технологию GSM мы проиграли. И дело даже не в том, что операторы выставляют счета конкретным клиентам, дело в архитектуре программного обеспечения: система в настоящий момент выстроена так, что не скрывает ни местонахождение говорящего, ни то, что он говорит.

ДЖУЛИАН: Мобильный телефон – это следящее устройство, по которому можно еще и звонить.

ДЖЕЙКОБ: Точно. Когда мы говорим, что за кем-то в стране третьего мира следят, что это означает на практике? Что телефонные системы, которые соединяют страну с остальным миром, превращаются в шпионское оборудование, когда кто-то решает использовать собранную ими информацию.

ЭНДИ: Я видел, как некоторые африканские страны получали всю сетевую

инфраструктуру, включая оптоволоконный кабель и магистральные коммутаторы, в подарок от китайцев.

ДЖЕЙКОБ: Подарок от ZTE или кого-то в этом роде? [56]

ЭНДИ: Да, и, само собой, китайцев интересует информация, так что им не нужно платить деньгами – они берут плату информацией, это новая валюта.

Слежка за частным сектором

ЖЕРЕМИ: Финансируемая властями слежка – и правда огромная проблема, бросающая вызов структуре всех демократий и их функционированию, однако есть еще частная слежка и – в потенциале – массовое накопление данных частными лицами. Взгляните на Google. Если вы – обычный пользователь сервисов Google, эта компания знает, с кем вы общаетесь, с кем знакомы, что вы ищете, ей потенциально известны ваша сексуальная ориентация, ваши религиозные и философские убеждения.

ЭНДИ: Google знает о вас больше, чем вы сами.

ЖЕРЕМИ: Больше, чем знает ваша мама, и, возможно, больше, чем вы сами. Google знает, когда вы в сети, а когда – нет.

ЭНДИ: Вы помните, что искали в интернете два года, три дня и четыре часа назад? Вы этого не помните, а Google помнит.

ЖЕРЕМИ: На деле именно по этим причинам я стараюсь Google не использовать.

ДЖЕЙКОБ: Это лозунг «Убей свой телевизор» для XXI века [57] . Эффективный протест – если не считать того, что «эффект сети» сводит ваш протест к нулю [58] . Убей свой телевизор, парень.

ЖЕРЕМИ: Ну, это не протест, это скорее мой личный взгляд на вещи.

ЭНДИ: Я видел прекрасные фильмы о людях, которые выбрасывали телевизоры с третьих этажей своих домов.

ЖЕРЕМИ: Вопрос не только в слежке, финансируемой властями, вопрос еще и в приватности, в том, как используют информацию третьи лица, в том, что мы знаем о применении информации. Я не пользуюсь социальной сетью Facebook и знаю о ней не так много. Но сегодня мы видим в Facebook людей, которые счастливы делиться любыми сведениями о себе, – и можно ли обвинить человека в том, что он не видит границу между общественным и личным? Несколько лет назад, до эпохи цифровых технологий, публичные люди работали в шоу-бизнесе, или это были политики, или журналисты, а сейчас потенциал публичной жизни есть у каждого, достаточно нажать кнопку и опубликовать информацию о себе в Сети. «Опубликовать» – значит «сделать что-то публичным», предоставить всему миру доступ к этой информации, – и, конечно, когда подростки выкладывают фотографии, на которых они пьяны и т. д., они могут не понимать, что фотография будет доступна всему миру и, возможно, очень-очень долго. Facebook делает деньги на том, что размывает границу между частной жизнью, кругом друзей и публичностью. Это происходит, даже если ты выкладываешь информацию, которая предназначена только для твоих друзей и близких. Что бы ты ни думал о степени публичности выложенной информации, когда ты выкладываешь данные на Facebook, ты сперва даешь их сети и уже потом – каким-то другим ее пользователям.

ДЖУЛИАН: Даже граница между правительством и частным бизнесом размыта. Посмотрите на то, как расширился рынок военных контрактов на Западе за последние десять лет. Раньше АНБ, крупнейшее шпионское агентство в мире, работало с десятью основными подрядчиками. Два года назад число этих подрядчиков выросло до тысячи. Граница между правительством и частным сектором исчезает на глазах.

ЖЕРЕМИ: И есть подозрение, что разведывательные агентства США имеют доступ ко всей информации, сохраненной Google.

ДЖУЛИАН: Конечно, имеют.

ЖЕРЕМИ: И ко всем данным Facebook, так что в каком-то смысле Facebook и Google являются филиалами этих агентств.

ДЖУЛИАН: Джейк, ты в курсе насчет судебного ордера Google? Получал ли Google ордер с требованием поделиться информацией, связанной с твоим аккаунтом? Калифорнийский доменный регистратор dynadot, зарегистрировавший сайт wikileaks.org, получил ордер насчет WikiLeaks. Он касался продолжающегося секретного расследования деятельности WikiLeaks Большим жюри, суд потребовал от dynadot финансовые документы, логины и т. д. – и регистратор все им выдал [59] .

ДЖЕЙКОБ: Газета The Wall Street Journal писала о том, что Twitter, Google и Sonic.net, сервисы, которые я использую или использовал в прошлом, получили каждый по извещению 2703 (d) – это такая необычная секретная форма судебного ордера [60] .

ДЖУЛИАН: Она выдается по патриотическому закону?

ДЖЕЙКОБ: Нет. По сути, ордер ссылался на закон о сохраненной информации. Согласно The Wall Street Journal, каждый из этих трех сервисов говорит, что власти требовали у него метаданные, утверждая, что у них есть право получить их без ордера. Продолжается судебный процесс, по итогам которого будет принято решение, есть ли у властей право хранить свою тактику в секрете и от общественности, и от судебной системы. Я читаю The Wall Street Journal и узнал обо всем этом оттуда.

ДЖУЛИАН: Итак, Google прогнулся перед правительством США, когда Большое жюри, расследующее дело WikiLeaks, запросило твои данные через ордер – и не простой ордер, а специальный шпионский. Еще раньше, в 2011 году, прошла новость о том, что Twitter получил несколько таких ордеров от того же Большого жюри, но стал добиваться через суд права сообщить пользователям о том, что данные об их аккаунтах затребованы по ордеру, – то есть настоял на отмене запрета на разглашение. У меня нет аккаунта в Twitter, так что мои данные они не получили, но наши с Брэдли Мэннингом имена стояли во всех ордерах – Большое жюри искало информацию именно о нас. Джейк, у тебя был аккаунт в Twitter, а значит, Twitter вручили ордер и насчет тебя тоже. И Google получил такой ордер, но не стал бороться за право разгласить его содержание [61] .

ДЖЕЙКОБ: Судя по всему, так и было. Я прочел обо всем этом в The Wall Street Journal. Возможно, у меня нет права говорить о произошедшем иначе, чем в связи с The Wall Street Journal.

ДЖУЛИАН: Из-за подписки о неразглашении? Ее же объявили неконституционной, разве нет?

ДЖЕЙКОБ: Не факт. Что касается дела Twitter, я могу сказать, что мы предложили не выдавать данные властям, потому что ущерб будет невосполним – получив эти данные, правительство станет хранить их вечно. Но суд решил, что мы не правы. Нам сказали: «Нет, ваше предложение отклонено, Twitter обязан выдать данные». Мы подали апелляцию и оспорили, в частности, секретность назначения апелляции к слушанию – и об этом я говорить не вправе, – однако на данный момент суд решил, что в интернете вы не можете ждать сохранения приватности, если добровольно предоставляете информацию третьей стороне, между тем в Сети каждый пользователь – третья сторона.

ДЖУЛИАН: Даже если компания вроде Facebook или Twitter говорит, что будет хранить информацию в тайне.

ДЖЕЙКОБ: Именно. Опять же граница между государством и бизнесом размывается. Может быть, это самое важное в нашем разговоре – сказать, что АНБ и Google являются партнерами по обороне США в секторе кибербезопасности.

ЭНДИ: Что бы «кибербезопасность» в данном контексте ни означала. Это широкое понятие.

ДЖЕЙКОБ: Они пытаются до минимума сузить сферу применения закона о свободе информации, чтобы хранить все в тайне. Кроме того, власти США заявляют, что у них есть право выдавать административный ордер, более суровый, чем ордер на обыск, потому что третья сторона обязуется не сообщать тебе об этом ордере, и у тебя нет права протестовать – в дело вовлечена третья сторона, у которой нет конституционного права защищать твои данные.

ДЖУЛИАН: Третья сторона – это Twitter, или Facebook, или твой интернет-провайдер.

ДЖЕЙКОБ: Да кто угодно. Мне сказали, что те же правила применяются, когда речь идет о приватности банковских данных или о телефонном разговоре. Ты добровольно сообщаешь свой номер телефонной компании, когда звонишь с него. Ты же это знал, да? Используя телефон, набирая чей-то номер, ты все равно что говоришь себе: «Я знаю, что разговор не будет приватным». С компьютером связь еще менее очевидна. Люди не понимают, как работает интернет, – как работают телефонные сети, они тоже не знают, – но суды все время подтверждали отсутствие приватности, и в нашем деле с Twitter, о котором я, увы, не могу говорить, потому что в действительности живу в несвободной стране, суд постановил, по сути, то же самое [62] . Полное безумие – понимать, что мы делимся с этими компаниями всеми нашими личными данными, а компании потом фактически приватизирует тайная полиция. Если говорить о Facebook, у нас есть теперь демократическая слежка. Вместо того чтобы платить людям, как делало Штази в ГДР, мы воспеваем социальные сети как субкультуру – там ведь трахаются. И заодно доносят на друзей: «Ах, эти двое обручились»; «Ух ты, они расстались»; «Ох, я знаю, кому мне надо позвонить».

ЭНДИ: Есть люди, которые сумели прижать Facebook и получить всю сохраненную информацию о себе, ссылаясь на европейский закон о защите данных, и самый маленький файл весил 350 мегабайт, а самый большой – около 800 мегабайт [63] . Что любопытно, по этому закону Facebook вынужден был обнародовать структуру своей базы данных. Всякий раз, когда вы входите в систему, она сохраняет всю информацию о вас – каждый ваш клик – и запоминает, как долго вы остаетесь на той или иной странице, так что Facebook может решить, нравится она вам, не нравится и т. д. Как оказалось, ключевым идентификатором в структуре базы данных Facebook является слово target – «мишень». Они называют людей не «подписчиками», не «юзерами», а targets, мишенями, на что вы можете сказать: «О’кей, это маркетинговый термин…»

ДЖУЛИАН: И он используется внутри системы.

ЭНДИ: Да, но это может быть мишень и в военном смысле – или в том, в котором говорят о мишенях в разведке. Как именно используется информация – зависит от обстоятельств.

ДЖУЛИАН: Да. Это-то и страшно.

ЭНДИ: Ты разложил все по полочкам. Раньше мы говорили, что пользователь Facebook на деле – не клиент. В реальности он – продукт, а настоящий клиент – рекламодатели. Это наименее параноидальное, самое безобидное описание того, чем занимается данная социальная сеть. Проблема в том, что нельзя винить компанию в подчинении законам конкретной страны. Соблюдать законы – нормально, не соблюдать – преступно. Так что ты не можешь сказать: «Эй, они соблюдают закон!» Разве это обвинение?

ДЖЕЙКОБ: Тут есть кое-что, с чем я должен поспорить. Если ты создаешь систему, сохраняющую все данные о человеке, и при этом знаешь, что живешь в стране, законы которой могут заставить тебя выдать информацию власти, вероятно, тебе не стоит создавать такую систему. И есть разница между приватностью, вытекающей из политики компании, и приватностью, встроенной в систему изначально. Если люди для тебя – мишени, и ты живешь в стране, власти которой склонны смотреть на мир через прицел… Согласись, размести Facebook серверы в Ливии времен Каддафи или в Сирии при Ассаде, это оказалось бы жутчайшей халатностью. Тем не менее ни одна повестка национальной безопасности за последние год или два не связана с терроризмом. Их было около 250 тысяч, они касались чего угодно, но только не терроризма [64] . Компании знают, что происходит, и у них есть серьезные этические обязательства, вытекающие из простого факта: они создали свои системы и построили бизнес на том, что фактически продают пользователей. Это все даже не связано с технологией. Никакой технологии – чистая экономика. Компании решили, что важнее сотрудничать с властями, продавать своих клиентов, нарушать их приватность и быть частью системы контроля – чтобы потом тебе заплатили за то, что ты причастен к слежке, причастен к контролю, – чем противостоять власти, и теперь они – часть системы контроля.

Они стали соучастниками и несут за это ответственность.

ЭНДИ: Этические обязательства – не главный коммерческий довод сегодня, верно?

Борьба с тотальной слежкой по законам физики

ЖЕРЕМИ: Самое время задать вопрос: где тут выход – как для индивидуального пользователя, так и для общества в целом? Существуют технические решения – скажем, децентрализованные сервисы, когда каждый хранит свою информацию у себя, или шифрование данных, когда каждый доверяет близким провайдерам, помогающим ему с шифрованием, и т. д. Есть политические решения, их мы обсудили. Я не уверен, что в данный момент мы можем решить, какой из двух подходов лучше. Мне кажется, мы должны реализовывать их параллельно. Нам нужно бесплатное программное обеспечение, которое любой желающий способен понять и модифицировать, и все могут удостовериться в том, что программа делает то, что должна делать. Я думаю, бесплатное ПО – одна из основ свободного онлайн-общества, оно позволяет всегда контролировать машину и не дает машине контролировать тебя. Нам нужна сильная криптография, чтобы информацию, предназначенную только для нас, не смог прочесть никто другой. Нам нужны средства коммуникации вроде Tor или криптофонов, позволяющие общаться только с теми, с кем мы хотим. Однако власти и отдельные компании всегда могут оказаться сильнее нас, «ботанов», и нашей способности разрабатывать и распространять эти технологии. При создании технологий нам способны помочь законы и средства, которыми располагают граждане, чтобы можно было установить контроль над технологией – пусть и не всегда в реальном времени – и наказывать тех, кто использует ее неэтично, нарушая приватность граждан.

ДЖУЛИАН: Я позволю себе определить то, что вижу, как разницу между американской и европейской перспективами шифропанка. Вторая поправка к Конституции США дает право на ношение оружия. Я только что смотрел ролик о праве носить оружие, который мой друг снял в США, и там над оружейным магазином висит плакат: «Демократия заряжена и на предохранителе». Это гарантия того, что в стране не установится тоталитарный режим, – американцы вооружены, и, если их доведут до ручки, они просто вынут оружие и силой вернут себе контроль над страной. Насколько этот довод серьезен в наши дни – интересный вопрос, ведь за последние тридцать лет появились самые разные виды оружия. Оглянувшись, можно сказать, что на деле тайные криптографические коды, не позволяющие властям за нами следить, были своего рода боеприпасами. В 1990-е годы мы вели большую войну, пытаясь сделать криптографию доступной всем и каждому, и по большому счету мы эту войну выиграли [65] .

ДЖЕЙКОБ: На Западе.

ДЖУЛИАН: На Западе мы ее выиграли, и наша победа – в каждом браузере, хотя сегодня итоги той войны власти пытаются переиграть множеством способов [66] . Важно то, что мы не можем доверять правительству и считать, что его слова не расходятся с делом, потому мы должны располагать базовыми криптографическими средствами, находящимися полностью под нашим контролем; для нас это своего рода оружие, и если шифр хорош, властям, как бы они ни пытались, не удастся взломать код и раскрыть нашу коммуникацию.

ДЖЕЙКОБ: Практически любая власть сегодня базируется на насилии или же на угрозе насилия. Криптография хороша тем, что никакой уровень насилия не поможет решить математическую проблему.

ДЖУЛИАН: Именно так.

ДЖЕЙКОБ: Тут есть важный момент. Это все не значит, что тебя не подвергнут пыткам или что власти не нашпигуют твой дом «жучками», не осуществят какую-либо диверсию. Но если правительство наткнется на зашифрованное сообщение, какой бы властью оно ни обладало, математическую проблему ему решить не удастся. Боюсь, эта мысль совершенно неочевидна для людей без технического бэкграунда – и нужно донести ее до них. Если бы мы могли решить все математические проблемы, это оказалась бы другая история, и, конечно, власть была бы способна взломать любой шифр.

ДЖУЛИАН: Но это такой же факт, как то, что мы можем конструировать атомные бомбы, – точно так же мы можем создавать математические проблемы, которые не решит самое влиятельное государство. Я думаю, именно этот момент так привлекает калифорнийских либертарианцев и прочих людей, верящих в идею «демократии – заряженной и на предохранителе», потому что тут налицо весьма интеллектуальный подход – пара человек, вооруженных криптографией, против всей мощи самого сильного государства в мире. Итак, у вселенной есть свойство, которое защищает приватность, – некоторые шифровальные алгоритмы правительству вообще не по зубам. Другие очень сложно взломать даже АНБ. Мы знаем об этом, потому что АНБ рекомендуют использовать данные алгоритмы для коммуникации внутри армии США, и если к ним можно было бы подобрать какой-то ключ, русские или китайцы давно бы уже справились – и последствия для человека, решившего рекомендовать небезопасный шифр, были бы ужасны. Так что сегодня шифры достаточно хороши, и мы можем быть в них уверены. К сожалению, нам никак нельзя положиться на машины, где используются шифры, и это проблема. Но к массовому перехвату информации она не ведет; скорее к целевой слежке за компьютерами отдельных людей. Если ты не эксперт по безопасности, защитить компьютер тебе будет очень сложно. Однако криптография может решить проблему массового перехвата данных, а именно она представляет угрозу мировой цивилизации. Индивидуальный перехват информации – не катастрофа.

Тем не менее, я думаю, мы имеем дело с безумно мощной экономической и политической силой, как и сказал Жереми, и, вероятнее всего, в итоге естественная эффективность технологий слежения победит, а значит, мы постепенно придем к глобальному тоталитарному обществу, в котором под наблюдением находится каждый, – под «тоталитаризмом» я имею в виду всеобщую слежку, – и, видимо, последними свободными людьми в этом обществе останутся те, кто знает, как обороняться при помощи криптографии. А еще там будут люди, живущие за пределами Сети, неолуддиты, обитатели пещер, ну или традиционные дикие племена, за которыми нет мощи современной экономики, а значит, их способность действовать крайне ограниченна. Конечно, можно просто держаться подальше от интернета, но тогда ты никак не сумеешь повлиять на ситуацию. Ты сам себя исключишь из числа людей, обладающих каким-либо влиянием. То же с сотовыми телефонами: можно отказаться от их использования, но тогда твое влияние уменьшится. Это путь назад.

ЖЕРЕМИ: Если посмотреть с точки зрения рыночной перспективы, я убежден, что есть рынок для приватности, который по большому счету никто не изучал; вероятно, у бизнеса появится экономический стимул разрабатывать устройства, дающие пользователю индивидуальную возможность контролировать свои данные и свою коммуникацию. Вероятно, здесь кроется один из способов решения проблемы. Я не уверен, что этого будет достаточно, но не исключено, что разработки уже идут, просто мы о них не знаем.

ДЖУЛИАН: Криптография проникает повсюду. Ее используют все ключевые организации, превращаясь в сетевые города-государства. Все коммуникационные потоки в интернете – быстрый международный перевод денежных средств, инфопотоки транснациональных компаний, сообщение между филиалами какой-либо организации – идут по незащищенным каналам связи. Это как организм, лишенный кожи. Корпорации и страны сливаются друг с другом, каждая сеть мирового значения соревнуется с другими, а их коммуникационные потоки уязвимы для оппортунистов, стран-конкурентов и т. д. Потому над интернетом созданы новые, виртуальные частные сети, и их приватность гарантирована криптографией. Благодаря тому что на криптографию есть спрос, ее не запретили совсем. Возьмите телефон Blackberry, в который встроена шифровальная система, используемая в сети Blackberry. Управляющая этой сетью канадская фирма Research In Motion может декодировать инфотрафик обычных пользователей, и у нее есть по меньшей мере два дата-центра – в Канаде и Великобритании, – так что англо-американский альянс разведок может добраться до всей коммуникации Blackberry. Однако большие корпорации

используют криптографию, чтобы обезопасить себя. Западные правительства мирились с этим, пока криптография не вышла за пределы бизнеса и ее не начали использовать частные лица. Тогда власти стали реагировать так же враждебно, как реагировало на криптографию правительство Мубарака в Египте [67] .

Я думаю, единственный эффективный способ обороны от грядущей антиутопии с ее тотальной слежкой – защищать свою приватность самому, потому что те, кто может перехватить любую информацию, никак не мотивированы сдерживать себя. Я тут вспомнил об одной исторической аналогии, а именно о том, как человечество осознало, что нужно мыть руки. Понадобилось создать и популяризовать микробную теорию инфекции, чтобы пробудить в людях паранойю по поводу невидимых существ, которые распространяют заразу и незаметны невооруженным глазом. Точно так же мы не видим массового перехвата информации. Как только люди поняли что-то про микробов, производители мыла создали продукты, и потребители стали их покупать, чтобы уменьшить чувство неуверенности. Надо внушить страх, чтобы люди осознали проблему, после чего появится спрос на ее решение. В другой части уравнения тоже не все благополучно: нас уверяют, что программы безопасны и используют криптографию, а они на поверку часто оказываются фальшивками, потому что криптография – сложная штука, а сложность хорошо маскирует обман [68] .

Обо всем этом людям нужно поразмыслить. Вопрос только один: каким из двух путей потечет их мысль? Они могут думать: «Нужно быть осторожным, не говорить лишнего, я должен приспосабливаться», – все время, в любой ситуации. Или же они могут думать: «Мне нужно понять, как работают компоненты этой технологии, и инсталлировать программы, которые меня защитят, чтобы я мог свободно выражать свои мысли и общаться с друзьями и близкими». Если люди не сделают этого второго шага, у нас воцарится универсальная политкорректность – даже общаясь с лучшими друзьями, мы будем подвергать свою речь самоцензуре, и уж точно мы не станем соваться в политику.

Интернет и политика

ЖЕРЕМИ: Любопытно, что влиять на ситуацию могут хакеры – в первоначальном значении слова, а не в уголовном. Хакер – это энтузиаст технологии, тот, кому нравится понимать, как технология устроена, не становиться ее рабом, а делать ее эффективнее. Когда вам было пять или семь лет, вы наверняка брали отвертку и пытались открыть приборы, чтобы понять, что и зачем у них внутри. Именно так ведут себя хакеры – и они создали интернет по множеству причин, в том числе потому, что это было весело, и они развили его и подарили всем остальным. Потом компании вроде Google и Facebook ухватились за возможность создавать бизнес-модели, в основе которых лежит захват личных данных пользователя. И все равно у хакеров есть нечто вроде влияния. Сегодня мне главным образом интересно наблюдать за тем, как хакеры набирают силу даже на политической арене. В США появились SOPA и PIPA – агрессивные законопроекты в области копирайта, по сути – попытка дать Голливуду власть приказать любому интернет-провайдеру ограничить доступ к любому сайту и ввести цензуру в интернете [69] .

ДЖУЛИАН: И еще право на банковскую блокаду вроде той, от которой страдает проект WikiLeaks [70] .

ЖЕРЕМИ: Точно. То, что сделали с WikiLeaks банковские компании, – это теперь обычный метод борьбы с плохими сетевыми пиратами, которые убивают Голливуд и все такое прочее. Но мы видели, какая волна гражданского возмущения поднялась в интернете – и не только в США; если бы против SOPA и PIPA вышли только американские граждане, этого оказалось бы слишком мало. Нет, протестовал весь мир, а хакеры были в авангарде и предоставляли средства, позволяющие участвовать в общественной дискуссии и обычным людям.

ДЖУЛИАН: Хакеры помогали проводить кампанию протеста.

ЖЕРЕМИ: Кажется, на Tumblr – или на каком-то другом сайте? – на домашней странице можно было ввести номер телефона, после чего тебе звонили и соединяли тебя с

Конгрессом. Ты говорил с кем-то и высказывал свою точку зрения: «Эти законы – чушь собачья».

ДЖЕЙКОБ: Интернет защищали посредством интернета.

ЖЕРЕМИ: Я думаю, что мы, хакеры, несем ответственность за систему, которую создали и передали миру, и сейчас мы видим, как эффективно ответственность можно превращать в действия, если делать что-то сообща. Сегодня в ЕС идут споры по поводу ACTA. Это международное соглашение, по сути – черновик SOPA и PIPA [71] . Я только что был в Европарламенте, где мы, индивиды, бородатые вонючие индивиды, диктовали наши условия одному парламентскому комитету. Мы указывали им на пункты в регламенте Европарламента, о которых члены комитета, судя по всему, слышали в первый раз, и говорили, что именно нужно делать, и на голосовании мы победили – 21 голос против 5, так что британский докладчик был разбит наголову. Крохотный процедурный шаг на пути к победе над ACTA, этим чудовищным глобальным соглашением, которое создали за нашими спинами, чтобы обмануть саму демократию. Но мы, граждане, способны одолеть монстра – легко, с интернет-сервисами, рассылками, Wikipedia, чатами IRC и т. д., – и я уверен, что мы видим зарю новой эры и отрочество интернета: общество использует его, чтобы изменить что-то по-крупному. Чрезвычайно важно, чтобы мы, хакеры, обладающие техническими знаниями, направляли обычных людей и говорили им: «Вы должны использовать технологию, которая дает контроль над вашими личными данными вам, а не Facebook или Google», – и чтобы люди ладили с технологиями, ну или могли поладить. Такая вот крупица оптимизма.

ДЖУЛИАН: Джейк, если говорить о политической радикализации молодежи в интернете, – последние два года ты ездил по миру, рассказывал о проекте Tor, говорил с людьми, которые хотят анонимности, хотят сохранить личные данные в тайне от властей, и ты наверняка видел, как молодежь в самых разных странах становится более радикальной. Этому феномену стоит придавать значение?

ДЖЕЙКОБ: Конечно. Это очень заметный феномен. Классический пример, который сразу пришел мне в голову, – Тунис. Я поехал туда, когда пал режим Бен Али, и мы говорили о проекте Tor в аудитории информатики, там были люди из университета, подкованные в технологии. Одна девушка подняла руку и спросила: «Как следует поступить с плохими людьми?» И выпалила списком имена четырех всадников Инфокалипсиса – отмывание денег, наркотики, терроризм, детская порнография. «Как быть с плохими людьми?» Этих четырех всадников вспоминают всегда, их призрак используют для борьбы с сохраняющей приватность технологией, потому что мы, конечно, обязаны сражаться с теми, кто занимается такими жуткими вещами. Я спросил: «Кто из вас был на сайте Ammar 404?» – это прозвище цензурного ведомства, которое режим Бен Али создал накануне революции, чтобы перекрывать доступ к интернету. Все, кто находился в аудитории, исключая девушку, задавшую вопрос, но включая профессора, подняли руки. Тогда я сказал девушке: «Посмотрите на этих людей. Они – такие же студенты, как вы. Неужели вы полагаете, что для борьбы с названными вами явлениями требовалось подавлять их свободу?» А она сказала: «На самом деле я тоже должна поднять руку». Я пересказал тот разговор вкратце, но суть в том, что, если объяснить контекст, люди понимают, о чем на самом деле идет речь. Контекст все меняет. Люди прозревают все время и по всему миру, но, как правило, поздно, они задним числом осознают, что могли бы использовать технологию, задним числом понимают: «Значит, дело не только в плохих людях, иначе получается, что я тоже буду плохим человеком, если скажу о власти что-то такое, что ей не понравится». В этот момент люди утрачивают иллюзии.

Впрочем, говорить, что этот процесс идет последние пару лет, неверно. Прости, Джулиан, но именно ты сыграл большую роль в радикализации моего поколения. Если посчитать, я – представитель уже третьего поколения шифропанков. Благодаря файловой системе rubberhose, которую создали вы с Ральфом Вайнманном, я стал работать над криптосистемами. Я создал криптографическую файловую систему M.A.I.D. в ответ на

действия британских правоохранительных органов – в Великобритании криптография запрещена, и власти имеют право затребовать любой твой пароль [72] . В свое время Джулиан создал rubberhose, потому что деспотические режимы пытали людей, требуя пароль, а rubberhose позволяет выдать один из паролей и не погибнуть. Моя криптосистема M.A.I.D. создавалась для правовой структуры, в которой обвиняемые имеют право молчать, но способны доказать, если их заставят это сделать, что говорят правду, без нарушения конфиденциальности. Увидев систему Джулиана, я понял, что технологию можно использовать, чтобы позволить обычным людям изменить мир. Если углубиться в историю, как не вспомнить старую рассылку Cyherpunk, одним из основателей которой был Тим Мэй, и посты Джулиана в этой рассылке – вот что сделало целое поколение более радикальным. Люди осознали, что они не раздроблены, как раньше, что у них есть время написать программы, которые помогут миллионам [73] .

Не все последствия мы предвидели – скажем, создатели Google изначально не планировали делать свое детище величайшим механизмом слежки всех времен. Но на деле они создали именно его – и как только люди это понимают, власти начинают рассылать повестки национальной безопасности, да?

ЖЕРЕМИ: Я думаю, ты сказал сейчас три очень важные вещи.

ДЖЕЙКОБ: Всего три?

ЖЕРЕМИ: Среди прочего.

ЭНДИ: О’кей, я добавлю четвертую, ладно?

ДЖЕЙКОБ: Ты пока не знаешь даже, о чем речь.

ЖЕРЕМИ: Я вижу три темы, которые связаны друг с другом. Я не утверждаю, что их надо рассматривать по отдельности. Первая тема – это авторитарные режимы и власть, которой обладают такие режимы в эпоху цифровых технологий. В случае с режимом Бен Али – то же самое касается сегодня многих других государств – власть может диктовать людям, что им позволительно знать и с кем уместно общаться. Это ужасно, этому нужно противостоять, что и позволяет интернет – свободный интернет. Вторая тема – создание сервисов и более эффективной технологии, обходящих цензуру, но главное – создание сервисов как части инфраструктуры, которая поможет нам избавляться от диктаторов. И третья тема – политические байки, упомянутые тобой в связи со всадниками Инфокалипсиса, все те предлоги, какими политики каждый день потчуют СМИ: «Мы же не хотим погибнуть от рук террористов? Значит, нам нужен патриотический закон», или: «Любители детской порнографии повсюду», или: «В интернете полно педонацистов, поэтому нам нужна цензура».

ДЖЕЙКОБ: Педонацистов?

ЖЕРЕМИ: Да, педонацистов – доменное имя pedonazi.com уже выкуплено. «Творческие люди вымрут, никто не станет снимать кино, поэтому нужно дать Голливуду право на цензуру интернета» – и т. д. Я думаю, что Глобальная сеть может оказаться и антидотом от политических баек. Они играют на эмоциях и еще на недолгой жизни СМИ – информация появляется и исчезает через двадцать четыре часа, ее замещает новая информация. В интернете мы создаем, как я его называю, интернетное время. Большой интернет никогда ни о чем не забывает, и мы можем собирать досье годами, день за днем, мы можем их детализировать и анализировать. Именно это мы делали последние три года с ACTA. Опять же образцом для нас послужил проект WikiLeaks – первая версия ACTA была выложена на WikiLeaks в 2008 году [74] .

ДЖУЛИАН: Да, это мы ее раскопали.

ЖЕРЕМИ: И еще две версии мы выложили сами. За три года появилось пять версий текста, и мы можем взять их и проработать абзац за абзацем, строчка за строчкой и сказать, что вот эти слова чреваты тем-то, этот пункт вставлен по требованию лобби, мы можем призвать экспертов в области права и технологии и понять, чего на деле добиваются политики, когда говорят: «Ах, соглашение ACTA необходимо нам, чтобы спасти культуру и уберечь детей от фальшивых лекарств», – и тому подобную чушь. Мы создадим свою

политическую версию документа в интернет-времени, и в ее основе будут точный анализ и кропотливая работа множества людей.

ДЖУЛИАН: Именно так, и, я думаю, твой взгляд на АСТА сегодня преобладает.

ЖЕРЕМИ: Будем надеяться.

ДЖУЛИАН: Краткий исторический обзор: за политическими кулисами так называемое соглашение по борьбе с контрафактной продукцией, порожденное американской копирайт-индустрией, цитируется во множестве двусторонних соглашений, посредством которых власти пытались на международном уровне создать новую систему координат в области обнародования информации: что законно предавать огласке, а что нет, и какие механизмы запрещают выкладывать те или иные сведения. АСТА стандартизирует более жесткую версию американской системы DMCA (Digital Millennium Copyright Act, закон об авторском праве в цифровую эпоху), при которой вы, получив письмо с требованием убрать информацию из интернета, обязаны подчиниться, и вам дается две недели на то, чтобы привести контраргументы и т. д., но, так как работать с контраргументами провайдерам накладно, они убирают информацию сразу, перекладывая борьбу на плечи автора или того, кто информацию загрузил. В Америке применение закона DMCA имело разрушительные последствия – из интернета было удалено великое множество самой разной информации. Сайентологи злоупотребили этим законом и убрали с сайта YouTube буквально тысячи видеозаписей [75] . Предположим, что нам все удастся и Европарламент проголосует против АСТА, по крайней мере на этот раз. Но основные задачи АСТА все равно будут выполнены – мы устроили демократические дебаты, АСТА демонизирована в глазах общественности, мы победили на уровне мировоззрения, однако за кулисами по-прежнему заключаются тайные двусторонние соглашения, и они ведут к тому же результату, потому что власти плюют на демократию. Скажем, проект WikiLeaks заполучил и опубликовал новое соглашение о свободной торговле между ЕС и Индией, и в этом документе есть огромные куски АСТА [76] . То же с рядом других соглашений и правовых актов. Мы отрубили АСТА голову, а ее тело распалось на мелкие кусочки – и они расползлись по миру в форме всех этих двусторонних соглашений. На поверхности мы достигли демократической победы, но в глубине все осталось таким, как было. Я говорю к тому, что не верю в политический или правовой путь решения проблемы; с другой стороны, расслабляться на этом фронте нельзя, иначе наши враги станут продвигаться еще быстрее. Важно ловить их с поличным на чем угодно, как мы поймали их с АСТА. Тогда они будут замедляться. Но и победа в парламенте не прекратит движение в глубине.

ДЖЕЙКОБ: Думаю, к этому нужно добавить, что Роджен Динглдин – один из создателей проекта Tor и мой, я бы сказал, учитель, благодаря которому я многое понял про то, как обходить цензуру и сохранять анонимность в онлайне, – говорит, что, например, файерволы не просто технически успешны (а если ты хочешь создать технологию, которая борется с файерволами, тебе нужно знать, как они устроены) – они успешны еще и социально. Люди, воюющие с АСТА, не были бы способны на это без технологии, но на деле имеет значение не техжаргон, важно, что технология позволяет взаимодействовать обычным людям. Важно только то, что люди начинают по-другому смотреть на мир и менять его, пока у них есть такая возможность, и самое главное тут – человеческий фактор. WikiLeaks опубликовал документы, способствующие этому процессу, делиться информацией – важно, но ключевой аспект – люди, которые воспринимают важную информацию и распространяют ее. Нам ведь скажут, что многие из нас живут в демократических странах, что мы свободны, что власть согласует с нами свои решения. И если каждый поймет, что именно происходит, и мы обнаружим, что под данным решением власти не подписывались, очень нелегко будет просто взять и принять законы вроде АСТА – без согласия народа.

ЖЕРЕМИ: Неправильные политические решения должны обходиться тем, кто их принимает, все дороже, и мы все вместе можем гарантировать, что так и будет благодаря свободному интернету, пока он у нас есть.

ДЖЕЙКОБ: Все это делается и без Сети – свободные общества существовали и в

доинтернетную эпоху, просто с экономической точки зрения свобода тогда обходилась дороже, и бороться с угрозами свободе было где-то сложнее. Вот почему так важны движение peer-to-peer и пиринговая сеть [77] .

ЭНДИ: Четвертая важная вещь вот какая: архитектурное решение децентрализованной системы – это то главное, что мы должны дать людям. А сегодня мы имеем централизованную облачную компьютерную инфраструктуру [78] .

ДЖУЛИАН: Мы имеем полностью централизованный Facebook. Полностью централизованный Twitter. Полностью централизованный Google. Все это – в США и под контролем тех, кому принадлежит и принудительная сила. Вот цензура и появилась после того, как благодаря WikiLeaks случился «Кабельгейт» – и Amazon тут же удалил нас со своих серверов [79] .

ЭНДИ: А облачная инфраструктура стимулирует бизнес, предлагая более дешевую обработку информации в так называемых международных дата-центрах, которые контролируются американскими корпорациями, и в итоге информация перетекает в юрисдикцию США – от поставщиков платежных услуг и не только.

ДЖУЛИАН: Если говорить о переходе к облачным вычислениям, меня очень беспокоит следующая тенденция. В одном месте скапливается громадное количество серверов – так эффективнее стандартизировать контроль над средой, стандартизировать систему платежей. Это конкурентоспособная стратегия: дешевле держать все серверы в одном месте, чем распределять их по миру. Интернет-коммуникация, если убрать за скобки потоковое видео, происходит по большей части между двумя серверами, и дешевле разместить их как можно ближе друг к другу. В итоге мы имеем огромные ульи серверов. Скажем, для Google размещать его серверы рядом с крупными поставщиками контента – или наоборот – вполне логично: Google индексирует их страницы, делая их доступными для поиска. В США есть массивные здания, которые под завязку набиты серверами множества различных компаний. Именно в них АНБ размещает пункты массового перехвата информации. Интернет мог бы существовать и без централизации, технология это позволяет, просто централизованная система более эффективна. В условиях экономической конкуренции такие системы побеждают.

ЭНДИ: Все это важно понимать в разрезе архитектуры системы – централизованную инфраструктуру проще контролировать, в ней легче злоупотребить властью, – но, кроме прочего, централизованная розничная торговля ведет к банкротству мини-супермаркета на углу.

ДЖУЛИАН: И в итоге появляется фантастически огромная транснациональная компания типа Safeway.

ЭНДИ: Именно, это тот же самый процесс, что и в торговле. Вот почему чрезвычайно важно поддерживать децентрализованную инфраструктуру. Когда я работал в организации ICANN, которая создает доменные имена и регулирует связанные с ними вопросы, я узнал кое-что интересное от Винса Серфа, человека, создавшего по меньшей мере часть протокола TCP/IP – фундаментального коммуникационного протокола интернета. Винс часто говорил: «Знаешь, с властями хорошо то, что нет какой-то одной власти – их всегда много». Среди правительств есть те, которые хотят децентрализовать власть, а внутри правительств есть разные воюющие группировки. В итоге именно это и спасет нас от Старшего Брата – тех, кто хочет стать Старшим Братом, слишком много, и они неизбежно передерутся между собой.

ДЖУЛИАН: Энди, я с тобой не согласен. Да, когда-то у нас были национальные элиты, конкурировавшие друг с другом, но сегодня они объединяются – и отрываются от своих народов.

ЭНДИ: Они объединяются, тут ты прав, – и я не уверен, что их внутренние распри спасут наши задницы, – но у нас появляется шанс сохранить самих себя. Мы не должны отказываться от нашей инфраструктуры, и если мы хотим противостоять государству тотальной слежки, единому Старшему Брату, нам необходимо изучить его, понять, на самом ли деле это конгломерат больших стран, которые говорят: «Объединившись, мы наберем еще

больше очков!» Мы должны понимать, в чем наша роль, – а она в том, чтобы сохранять децентрализацию, придерживаться собственной инфраструктуры, не полагаться на облачные системы и прочую чушь, гнуть свою линию.

ДЖУЛИАН: Но мы можем столкнуться с господством технологии. Если правда, что легче использовать Twitter, чем создать собственный аналог; если правда, что легче применять Facebook, чем Diaspora или другую альтернативу; если правда, что облачные вычисления дешевле, – тогда эти технологии и сервисы будут господствовать [80] . Недостаточно сказать, что мы создадим свои локальные аналоги, – они попросту окажутся неконкурентоспособны, их станет использовать меньшинство. Недостаточно сказать, что мы должны создать Facebook для бедных, и ждать, что в нашу сеть валом повалят пользователи. Нам нужен более эффективный план.

ЭНДИ: Самое время снова вспомнить о католической церкви – наступают времена, когда книги опять оказались у единственного продавца, и раз Amazon пытается захватить контроль над всей цепочкой поставок электронных книг, мы должны сохранять наши печатные и издательские мощности. Кому-то покажется, что я преувеличиваю, однако мы видели, на что способны эти компании, если они или правительственные учреждения, от которых они зависят и в юрисдикции которых находятся, не желают чего-либо допустить. Я думаю, следующий шаг очевиден: нам нужны свои деньги – и если кому-то не по нраву финансовая поддержка проектов вроде WikiLeaks, у нас должна быть возможность финансировать их, не полагаясь на центральную инфраструктуру, в которой власть творит что угодно.

ЖЕРЕМИ: Я хотел бы согласиться с Энди. Думаю, архитектура системы – это главное, за что мы боремся. Смысл в том, что на нас лежит ответственность, и мы должны донести ее до людей – именно мы, хакеры, специалисты по технике, каждый день создающие интернет и играющие с ним, понимаем, что происходит. Возможно, так нам удастся завоевать сердца и умы нового поколения. Вот почему такое значение имеют войны за копирайт – с появлением пиринговых сетей, начиная с Napster в 1999 году, человечество осознало, что когда люди делятся файлами…

ДЖУЛИАН: Да ты преступник.

ЖЕРЕМИ: Нет, мы создаем культуру лучше прежней.

ДЖУЛИАН: Нет, ты преступник.

ЖЕРЕМИ: Это вопрос мировоззрения, но если ты создаешь для себя культуру лучше прежней, в итоге все будут использовать Napster [81] .

ЭНДИ: Вся история человечества, история культуры – история копирования идей, их преобразования и дальнейшего развития, и если ты называешь это воровством, значит, ты один из тех циников.

ЖЕРЕМИ: Именно, именно! Культурой нужно делиться.

ДЖУЛИАН: Ну, на Западе в 1950-х появилась индустриальная культура. Наша культура превратилась в индустриальный продукт.

ЖЕРЕМИ: Мы сейчас кормим тролля – Джулиан играет адвоката дьявола и делает это дьявольски хорошо.

ДЖЕЙКОБ: Я никого не подкалываю. Это все очевидная чушь.

ЖЕРЕМИ: Да, чушь. Для политиков это «воровство», но не стоит забывать, что все те, кто пользовался Napster в 1999 году, стали фанатами музыки, они ходят на концерты, они бесплатно рекламируют исполнителей: «Ты должен послушать эту группу, ты обязан сходить на концерт!» – и т. д. У людей появился практически пример того, как пиринговая технология децентрализует архитектуру системы. На самом деле Napster был тогда несколько централизован, но он все равно пропагандировал идею децентрализованной архитектуры. Все увидели, как она в реальном времени приносит пользу обществу, и поняли, что делиться культурой так же необходимо, как делиться знаниями. Когда мы обсуждаем, как обойти цензуру, как бороться с политическими байками, чтобы создать демократическую систему лучше прежней и более совершенное общество, мы обсуждаем, по сути, как

делиться знаниями. У нас есть примеры того, как децентрализованные сервисы и расшаривание информации улучшают мир, а контрпример тут приводят адвокаты дьявола, сейчас такого адвоката играет Джулиан. Это когда индустрия приходит и говорит: «Ах, всюду воровство, и оно убьет культуру, убьет актеров, убьет Голливуд, убьет кино, убьет котят и вообще всех на свете». Индустрия побеждала в прошлом, но сейчас мы близки к тому, чтобы одолеть ACTA. И я снова должен не согласиться с адвокатом дьявола в исполнении Джулиана. ACTA – это величайший в истории пример искажения демократии: индустрия плюет в лицо парламенту и международным институциям, плюет в лицо общественному мнению, пробирается в наш дом через черный ход и ставит нас в неприемлемые условия. Если удастся вышвырнуть индустрию вон, мы создадим прецедент – и получим возможность продвигать позитивную программу действий: «ACTA не прошла, а теперь давайте сделаем что-нибудь хорошее в интересах общества». Мы работаем над этим, и отдельные депутаты Европарламента понимают, что, когда люди делятся информацией, когда они расшаривают файлы без выгоды для себя, их нельзя сажать в тюрьму, нельзя наказывать.

Думаю, если нам удастся победить в ЕС, мы сможем доказать остальным странам, что делиться знаниями, делиться информацией – значит улучшать мир, что культуру нужно продвигать, а не воевать с ней и что любая попытка – парламента, диктатора, корпорации – запретить делиться информацией и знаниями в децентрализованной системе должна быть пресечена. Точка. Я думаю, мы подтолкнем мир в правильную сторону.

ДЖУЛИАН: Что насчет дебатов вокруг PIPA и SOPA в США? Это предложенные Конгрессом законы, которые позволят американской индустрии накладывать финансовое эмбарго и блокировать интернет.

ДЖЕЙКОБ: Цель этих законопроектов – атака на WikiLeaks и все проекты, которые с ним связаны или идут по его стопам.

ДЖУЛИАН: В Конгрессе особо отмечалось, что банковская блокада – это эффективное средство борьбы с нами [82] .

ЖЕРЕМИ: И они хотели вручить это средство борьбы Голливуду.

ДЖУЛИАН: Мы организовали масштабную сетевую кампанию против этих законов, и в конце концов к нам присоединились Google, Wikipedia и многие другие проекты. Но я не стал радоваться, мол, теперь все хорошо, раз мы выиграли эту битву. Я чертовски перепугался, потому что Google вдруг ощутил себя не просто дистрибьютором информации, а политическим игроком – и наслаждался огромной, невероятной властью над Конгрессом.

ЖЕРЕМИ: Google был лишь малой частью коалиции против SOPA и PIPA.

ДЖЕЙКОБ: Да, и мало того – Tumblr, кажется, внес больший вклад, чем Google.

ЭНДИ: Tumblr, Wikipedia и великое множество отдельных людей, совершавших поступки, о которых вы, может, никогда и не слышали, – все они внесли в борьбу свой вклад. Тысячи параллельных действий, все в одном направлении, и это опять же децентрализованное политическое движение. Мы все увидели, как функционирует децентрализованное политическое движение. Google был, наверное, самым крупным его участником – и одним из самых заметных.

ДЖУЛИАН: Ну, Конгресс заметил именно его.

ДЖЕЙКОБ: Я вернусь к тому, что сказал Жереми, – по сути, он продвигает идею политического вождизма. Не думаю, что ты это имел в виду, но получилось у тебя именно оно, и тут я хотел бы тебя остановить. Пиринговое движение против любого вождизма в принципе. Идея состоит в том, что мы все равны [83] и можем делиться информацией, создавать разные сервисы и обеспечивать различную функциональность. Однажды Росс Андерсон сказал мне: «Когда я полвека назад присоединился к пиринговому движению…» – мощное вступление, правда? Он объяснил мне, что хотел одного: чтобы за открытием печатного станка не последовало его «закрытие». Когда мы начали централизовать сервисы, централизовать контроль над информационными системами, мы на деле начали «закрывать» печатный станок в том смысле, что теперь Британская энциклопедия уже не издается на

бумаге, только на CD, и если у тебя нет компьютера общего назначения, читающего CD, у тебя нет доступа к знаниям. В случае с Британской энциклопедией это не важно – у нас есть Wikipedia и много чего еще. Однако я не думаю, что общество готово отказаться от печатного станка.

ЭНДИ: Я не уверен, что Wikipedia так уж хороша в качестве источника информации. Я не доверяю ни единой ее странице, кроме тех, которые переписал сам.

ДЖЕЙКОБ: Британская энциклопедия ничем от Wikipedia не отличается. Это всего лишь один источник из многих, его информация может подтвердиться или не подтвердиться. Я имел в виду другое: мы не должны продвигать идею политического вождизма – это очень опасно.

ДЖУЛИАН: Погоди-ка. А почему? Я в каком-то смысле вождь. В чем проблема с вождями?

ЖЕРЕМИ: Я говорю не о вождях, я говорю лишь, что у нас есть новые средства борьбы. Мы тут говорили о печатном станке. Еще один передовой мыслитель, мой приятель Бенжамен Байяр, вероятно, не очень известный за пределами Франции, сказал: «Печатный станок научил нас читать; интернет научил нас писать» [84] . Это совершенно новое явление – небывалая возможность писать и выражать свои мысли для каждого из нас.

ЭНДИ: Да, но с каждым днем все важнее фильтровать информацию.

ЖЕРЕМИ: Конечно, потому что говорят все – и многие несут чушь. Как сказал бы вам ученый и активист Ларри Лессиг – думаю, с ним согласятся многие преподаватели, – мы учим людей писать, а когда студенты сдают работы, девяносто девять с чем-то процентов из них – полная ахинея, но все равно мы учим людей писать [85] . Само собой, люди несут чушь в интернете – это естественно. Однако чем чаще вам приходится высказываться на публике, тем продуманнее ваша речь – и тем больше вы готовы участвовать в непростых дискуссиях. А явления, которые мы обсуждаем, связаны со сложной технологией, и нам нужно разделить ее на компоненты, чтобы понять и спокойно всё обсудить. Речь вовсе не о политическом вождизме, а о том, чтобы посредством политической системы развить в людях новую способность выражать свои мысли, делиться ими, участвовать в расшаривании знаний, и для этого вовсе не обязательно принадлежать к политической партии, работать в СМИ или в любой другой централизованной структуре, без которой в прошлом самовыражение было невозможно.

Интернет и экономика

ДЖУЛИАН: Вспомним о трех основных свободах. Когда я брал интервью у главы партии «Хезболла» Хассана Насраллы…

ДЖЕЙКОБ: Где носит этот чертов дрон? Что там летит в небе, а?..

ДЖУЛИАН: Кстати, Насралла находится под своего рода домашним арестом, он не может выйти из тайного убежища.

ДЖЕЙКОБ: Я не уверен, что вас уместно сравнивать. Пожалуйста, не сравнивай себя с ним…

ДЖУЛИАН: Встает вопрос: есть ли в «Хезболле» элементы государства – стала ли она, по сути, отдельной страной? В телеграммах посольства США есть упоминания о том, что «Хезболла» создала собственную оптоволоконную сеть на юге Ливана [86] . У «Хезболлы» имеются три главных элемента государства: она контролирует армию на определенной территории, она обладает коммуникационной инфраструктурой и контролем над ней, и еще у «Хезболлы» есть финансовая инфраструктура – и контроль над ней. Эти три элемента – три основные свободы. Свобода передвижения, физическая свобода передвижения – возможность перемещаться из одного места в другое без прикрывающей тебя армии. Свобода мысли и свобода коммуникации, которая является неотъемлемой частью свободы мысли: если публичное самовыражение чревато опасными последствиями, единственный способ гарантировать право на коммуникацию – конфиденциальное общение. Наконец, свобода экономических отношений, а она, как и свобода коммуникации, немыслима без

приватности. Давайте поговорим об этих трех принципах, которые обсуждались шифропанками с 1990-х годов. В частности, обсудим попытки обеспечить весьма значимую третью свободу – свободу экономических отношений.

ЖЕРЕМИ: Но почему только три принципа? В моей европейской Хартии фундаментальных прав их больше.

ДЖУЛИАН: Приватность становится приоритетом либо в социальном аспекте, когда она необходима, чтобы свободно общаться и свободно думать о чем-либо, либо в экономическом. Наверняка есть много разных видов свобод, но эти три свободы – фундамент, на котором держится все остальное.

ЖЕРЕМИ: Но существует юридическое определение фундаментальной свободы.

ДЖУЛИАН: Я прочел Хартию ЕС – и скажу тебе, что это полная ерунда, не имеющая никакого отношения к консенсусу.

ЖЕРЕМИ: Да, соглашусь, к тому же лоббисты сумели пропихнуть в нее интеллектуальную собственность.

ДЖУЛИАН: И всякие другие совершенно безумные вещи.

ЭНДИ: Полагаю, мы сойдемся на том, что валютная система – экономическая инфраструктура для обмена валют – в настоящий момент терпит крах. И тот, у кого есть аккаунт на eBay, с этим сразу согласится – то, что делают Paypal, Visa и MasterCard, фактически не оставляет нам выбора, кроме как пойти на условия монополиста. В одном из сообщений WikiLeaks имелся любопытный факт: российские власти пытались договориться с Visa и MasterCard, чтобы платежи граждан РФ обрабатывались на территории России, и Visa с MasterCard отказались работать на этих условиях [87] .

ДЖУЛИАН: Да, совместной мощи посольства США и компании Visa хватило, чтобы не дать обрабатывать платежи по банковским картам внутри своих границ даже России.

ЭНДИ: Иначе говоря, платежи граждан РФ в российских магазинах обрабатываются через дата-центры в Америке. А значит, власти США могут если не контролировать их, то по крайней мере считывать.

ДЖУЛИАН: Да, и когда Путин идет купить себе банку кока-колы, через полминуты об этом узнают в Вашингтоне.

ЭНДИ: И это, конечно, крайне неудобная ситуация, независимо от того, нравятся мне США или нет. Очень опасно складировать все данные о платежах в одном месте: возникает соблазн использовать эту информацию.

ДЖЕЙКОБ: Шифропанки уяснили фундаментальное правило: архитектура инфосистемы обусловливает политическую ситуацию, и централизованная архитектура, даже если ее контролируют лучшие люди в мире, привлекает мерзавцев, которые, злоупотребляя властью, творят то, что создатели системы никогда не сделали бы. Деньги толкают людей на многое.

ДЖУЛИАН: Как и нефтяные скважины в Саудовской Аравии – проклятие нефти.

ДЖЕЙКОБ: Куда ни глянь, увидишь одно и то же, особенно это касается финансовой системы: даже самые прекрасные намерения ни черта не значат. Важна только архитектура системы. Если мы говорим о коммуникации – архитектура интернета. Так называемые системы законного перехвата информации – эти слова на деле означают, что за вами шпионят…

ДЖУЛИАН: Законный перехват информации – эвфемизм.

ДЖЕЙКОБ: Именно, как «законное убийство».

ЭНДИ: Или «законная пытка».

ДЖЕЙКОБ: Вы же слышали о законных ударах беспилотников по американским гражданам по приказу президента Обамы? Когда он убил в Йемене 16-летнего сына Анвара аль-Авлаки, это было законное убийство, ну или целевое уничтожение, если говорить их словами [88] . Так называемый законный перехват информации – то же самое: достаточно добавить слово «законный», чтобы вдруг оказалось, что, когда в дело замешано государство, все вполне законно. На самом деле такие вещи становятся возможными из-за структуры

государства, структуры законов и структуры технологии, и еще из-за структуры финансовой системы. Шифропанки хотели создать системы, позволяющие общаться действительно свободно, без вмешательства третьих лиц. То же с «валютами Чома», то есть электронными деньгами, созданными по спецификациям Дэвида Чома, придумавшего eCash (полностью анонимную электронную валюту), хотя мне могут возразить, что эти системы централизованы больше, чем следует. Идея в том, чтобы создать анонимные валюты в противовес Visa/MasterCard, отслеживаемой валюте. Хотя валюты Чома связаны с единым центром, они используют криптографические протоколы, придуманные, чтобы гарантировать анонимность сделки [89] .

ДЖУЛИАН: По сути, это электронная наличка, но, скажем так, без серийного номера на банкноте.

ДЖЕЙКОБ: Или с серийным номером, который дает вам понять, что перед вами настоящие деньги, но не позволяет узнать, что Джулиан заплатил Энди и какую именно сумму.

ЖЕРЕМИ: Наличные деньги для цифрового мира.

ДЖУЛИАН: Создание электронной валюты очень важно именно потому, что контроль над платежными средствами – это один из трех элементов государства, как я и сказал применительно к «Хезболле». Если лишить государство монополии на средства экономического взаимодействия, оно утратит один из трех важнейших признаков государственности. Если государство действует как мафия, как крышующий вас рэкетир, оно трясет из вас деньги любыми доступными способами. Контроль над денежными потоками важен не только потому, что позволяет властям повышать доходы, но и потому, что государство может контролировать, что именно люди делают, – стимулировать их заниматься чем-то и, наоборот, полностью запрещать какую-то деятельность, или организацию, или взаимодействие между организациями. Так, например, если взять экстраординарную финансовую блокаду WikiLeaks, не свободный рынок решил изолировать наш проект – это правительственное распоряжение превратило ряд финансовых игроков в королей и не позволило вмешаться другим участникам рынка. На экономическую свободу посягнула элитная группа, которая может влиять как на регуляцию, так и на принципы работы банков [90] .

ЭНДИ: Как ни печально, эта проблема виртуальной реальности до сих пор не решена. Две кредитные организации, обе с электронной инфраструктурой, размещенной в Америке, – то есть информация в этой инфраструктуре находится в юрисдикции США, – контролируют большинство платежей по кредитным картам. Компании вроде Paypal, также находящиеся в юрисдикции США, проводят в жизнь американскую политику, будь то блокирование закупок кубинских сигар у немецких онлайн-дистрибьюторов или блокада платежей WikiLeaks в неамериканских юрисдикциях. А значит, у властей Соединенных Штатов есть доступ к информации и возможность контролировать платежи в планетарном масштабе. Американские граждане, пожалуй, скажут, что это лучшая демократия, какую только можно купить за деньги, но для европейских граждан она не имеет никакой ценности.

ДЖУЛИАН: В нашем обычном мире у нас есть свобода передвижения – до определенной степени, иногда совсем крохотной.

ДЖЕЙКОБ: Ты уверен, Джулиан? Сдается мне, твоя свобода передвижения – это классический пример того, насколько мы свободны на самом деле.

ДЖУЛИАН: Великобритания заявила, что намерена ставить в мое положение по сто тысяч человек в год [91] . Думаю, это в какой-то мере сопутствующий ущерб.

ДЖЕЙКОБ: Вот потому отцы-основатели моей страны стреляли в британцев. Мы стреляли в них не без причины. И эта причина не исчезла! Тирания не исчезла.

ЖЕРЕМИ: Еще немного – и мы перейдем на личности.

ЭНДИ: Твоя страна, США, в настоящее время приватизирует тюрьмы и заключает договоры, которые гарантируют частным компаниям, управляющим бывшими федеральными тюрьмами, их 90-процентное наполнение [92] . Как это понимать?

Капитализм дошел до полного абсурда.

ДЖУЛИАН: В американских тюрьмах сейчас больше людей, чем было сидельцев в СССР.

ДЖЕЙКОБ: Тут логическая ошибка: я возражаю против чего-то неправильного, а вы делаете вывод, будто я защищаю что-то столь же неправильное. Я не говорю, что Соединенные Штаты совершенны. Я думаю, что США – великая страна во множестве аспектов, и особенно в том, что касается идеалов отцов-основателей.

ДЖУЛИАН: Идеалы отцов-основателей за последние десять лет явно подзабылись.

ДЖЕЙКОБ: Стоит помнить о том, что идеалы отцов-основателей – во многом мифология, и нам не следует делать кумиров из этих людей. Так что да, ты прав. Мое замечание о британской тирании и ситуации, в которой оказался Джулиан, касалось только того, что подобное – часть культуры. Тут действует общество, его реакция имеет решающее значение, и технология почти не в силах что-либо исправить. А финансы – самая опасная тема из всех. Вот почему человек, придумавший другую электронную валюту, биткоин (Bitcoin), пожелал остаться неизвестным. Никто не хочет оказаться создателем первой успешной электронной валюты [93] .

ДЖУЛИАН: В Америке парни, придумавшие e-gold, в итоге пошли под суд [94] .

ДЖЕЙКОБ: Меня просто бесит эта история.

ДЖУЛИАН: Я хотел бы вернуться к трем фундаментальным свободам: свободе коммуникации, свободе передвижения и свободе экономических отношений. Если мы посмотрим на переход нашего глобального общества в интернет, после него со свободой личного передвижения практически ничего не произошло. Свобода коммуникации в некоторых отношениях фантастически расширилась – сегодня мы можем общаться с огромным числом людей, – но и одновременно фантастически сузилась: конфиденциальности больше нет, наша коммуникация вполне способна оказаться под наблюдением – да за ней и следят, сохраняя всю информацию, которая в итоге может быть использована против нас. Прежняя свобода элементарного взаимодействия с людьми на физическом уровне утрачена.

ЭНДИ: Приватность достижима, но она стоит дорого.

ДЖУЛИАН: Нашим экономическим отношениям нанесен такой же ущерб. Когда мы заключаем обычную коммерческую сделку, кто об этом знает? Люди, которые видели, как вы шли на рынок. Кому известны подробности вашей экономической жизни теперь? Когда вы покупаете что-то у соседа, в традиционном рыночном обществе детали сделки можно сохранить в тайне, но если вы платите соседу картой Visa, кто узнаёт о вашей сделке?

ДЖЕЙКОБ: Весь мир.

ДЖУЛИАН: Весь мир узнаёт. Ведущие западные державы обмениваются информацией, все они знают о вашей сделке и будут хранить эти данные вечно.

ЭНДИ: Джулиан, ты все верно говоришь, но я не уверен, что можно провести границу между свободой коммуникации и свободой экономических отношений. Сегодня Сеть – инфраструктура для социальных, экономических, культурных, политических, вообще любых отношений.

ДЖЕЙКОБ: Включая свободу передвижения.

ЭНДИ: Какова бы ни была структура коммуникации, деньги – это всего лишь биты информации. Вариант использования Сети. И если экономическая система базируется на электронной инфраструктуре, по конфигурации последней можно судить о том, как движутся денежные потоки, как они контролируются, как централизуются и т. д. Пусть в самом начале интернет и не задумывался как инфраструктура для всего вообще, но экономическая логика диктует свое: «Дешевле делать то-то и то-то в Сети». Лет десять-двадцать тому назад банки и эмитенты кредитных карточек использовали банкоматы ATM с интерфейсом X.25, по сути, это были отдельные сети, а сегодня все перешли на протокол TCP/IP, потому что так дешевле [95] . Архитектура технологии стала ключом ко всему, она влияет на все прочее, и именно ее нам нужно переделать. Если мы хотим, чтобы

наши платежи обрабатывались децентрализованно, нам нужно владеть инфраструктурой.

ДЖЕЙКОБ: У нас есть биткоин – электронная валюта.

ЭНДИ: Не подверженная инфляции.

ДЖЕЙКОБ: Она функционирует децентрализованно, то есть вместо Федерального резерва множество людей по всему миру коллективно решают, каково положение дел и сколько стоят их деньги.

ДЖУЛИАН: И есть компьютерные программы, благодаря которым система работает.

ДЖЕЙКОБ: Давайте я объясню без специальных терминов. Биткоин – это электронная валюта, которая является скорее товаром, чем денежной единицей, и люди сами решают, сколько евро стоит один биткоин. В каком-то смысле это аналог золота, и так называемый майнинг [96] биткоинов тоже чего-то стоит: ты используешь свой компьютер, чтобы найти биткоин, и стоимость его связана со сложностью вычислительных мощностей. Если без технических терминов – я могу послать валюту Джулиану, а Джулиан подтвердит ее получение, при этом у Энди никак не выйдет ни вмешаться в процесс, ни аннулировать сделку. Тут возникают свои сложности – на самом деле биткоин не является анонимной валютой, и это, по-моему, очень скверно.

ДЖУЛИАН: Биткоин – интересный гибрид: держатели счетов абсолютно анонимны, ты можешь создать аккаунт, когда захочешь, но при этом транзакции биткоиновой экономики полностью открыты. Такая открытость нужна, чтобы все согласились, что транзакция произошла и на счету отправителя теперь меньше денег, а на счету получателя – больше. Это один из немногих способов поддерживать систему распределенной валюты без центрального сервера, который был бы привлекательной мишенью для принудительного контроля. В случае с биткоинами новаторскими являются система распределения и алгоритмы, делающие ее возможной, когда ты не доверяешь любой отдельно взятой части, если угодно, биткоиновой банковской сети. Само доверие децентрализовано. И реализуется работа системы не через законы, или какую-то иную правовую регуляцию, или аудит, а через криптографическую сложность вычислений, которую каждая часть сети должна преодолеть, чтобы доказать, что она не лжет. То есть честный «банкинг» биткоинов встроен в архитектуру системы. Вычислительные мощности переводятся в стоимость электричества для каждой ветви биткоинового банка, и мошенников можно наказать штрафами, привязанными к ценам на электричество. В этих ценах стоимость операций, которые необходимы для совершения мошенничества, будет превышать затраты на электроэнергию, что лишает эти действия экономической выгоды. Данные концепции раньше не изучались не потому, что были слишком инновационны (на бумаге они были описаны двадцать лет назад), а потому что биткоин добился почти полного равновесия системы и добавил одну весьма новаторскую идею – как именно доказать истинное глобальное одобрение транзакций в биткоиновой экономике, даже если многие банки жульничали и основать такой банк мог кто угодно. Разумеется, как и за все прочие валюты, за биткоины нужно платить – работой или другими денежными единицами, для чего существуют группы валютного обмена. Есть и еще ряд ограничений. Скажем, 10-минутная задержка – примерно столько вам нужно потратить на вычисления между отправкой валюты и подтверждением глобального одобрения сделки, получаемым другой стороной. Биткоины функционируют практически как бумажные деньги – и украсть их могут точно так же. У биткоинов есть все преимущества налички: получив их, вы твердо знаете, что вам заплатили, что чек не аннулируют, что банк не отменит сделку задним числом. Принудительные силы ничего не могут с вами сделать. С другой стороны, наличные деньги нужно тщательно охранять. Это, я полагаю, самая большая проблема. Однако добавить дополнительные уровни защиты, придумать сервис депонирования, чтобы можно было хранить биткоины в сервисе, созданном специально, чтобы на них никто не позарился, и застраховать их от кражи – все это достаточно легко сделать.

ДЖЕЙКОБ: Любопытно: если бы создатели биткоинов требовали от людей использовать Tor, чтобы те создавали не счета, а криптографические идентификаторы, и все пользователи биткоинов перешли бы на Tor, никто не смог бы определить, из какой точки вы

производите оплату, даже если у вас имелись бы долговременные идентификаторы, позволяющие опознать вас как личность, осуществляющую те или иные сделки.

ЖЕРЕМИ: Не углубляясь в технические дебри, мы можем сойтись на том, что у биткоинов, несмотря на прекрасную задумку, есть свои недостатки. В эту систему встроена дефляция – деньги из нее уходят. В долгосрочном плане она нефункциональна, однако лежащие в основе биткоинов идеи можно доразвить. Сейчас работает версия, кажется, 0.7 или 0.8.

ДЖЕЙКОБ: Идеи Дэвида Чома получили вторую жизнь [97] .

ЭНДИ: Я бы сказал, что биткоин – это самая успешная попытка создать цифровую валюту за последние десять лет.

ДЖУЛИАН: Они подобрались совсем близко к решению. Я думаю, биткоин не исчезнет. Это эффективная валюта; вы можете открыть счет за десять секунд, а перевод денег обойдется вам в стоимость интернет-соединения и потребления электричества за несколько минут. Биткоины более чем конкурентоспособны по сравнению с почти любым другим видом денежных переводов. Полагаю, биткоины будут очень успешны. Вспомните, что случилось, когда летом 2011 года пресса обрушилась на систему после нескольких случаев мошенничества – и обменный курс упал до трех долларов США за биткоин [98] . Постепенно стоимость валюты выросла до 12 долларов. Она не скакала вверх-вниз, а росла медленно, и кривая роста заставляет предположить, что биткоины пользовались существенным спросом. Подозреваю, что по большей части он был обусловлен торговлей небольшими партиями наркотиков, заказами марихуаны по почте и т. д. [99] Биткоин как валюта обходится очень дешево. Ее используют многие провайдеры, особенно там, где есть проблемы с оплатой кредитками, скажем, в бывшем СССР. Если система продолжит расширяться, она подвергнется атаке властей. Сами биткоины уничтожить не удастся, криптография отражает любые простые атаки принудительной силы, а вот надавить на обменные сервисы, конвертирующие биткоины в другую валюту и наоборот, будет куда проще. С другой стороны, эти сервисы могут находиться в любой точке земного шара, и в каком-то количестве юрисдикций они продержатся, а когда закроют последний, черный рынок станет менять биткоины по своему курсу. Я думаю, им пойдет на пользу, если провайдеры начнут принимать их в качестве оплаты за все маленькие игры, покупаемые на Facebook и не только. Это эффективное платежное средство, так что индустрия, которая будет его использовать, создаст свое лобби, и биткоины не запретят. Примерно по такому же сценарию не запрещают криптографию. Поначалу с ней боролись на том основании, что это-де торговля оружием, но как только криптографию начали использовать в браузерах и банковских системах, сразу появилось достаточно мощное лобби, благодаря которому криптографию не запретили, – хотя я допускаю, что власти готовятся к контратаке.

ДЖЕЙКОБ: Проблема в том, что мечта о конфиденциальности в сфере финансов недостижима. Надо честно это признать. Неверно думать, что экономическая логика в условиях интернета отличается от обычной. Когда я приехал сюда и стал покупать британские фунты, у меня потребовали номер карточки социального обеспечения, а в США по нему сразу можно определить, кто я такой, я сообщил свое имя, я связал его с банковским счетом, я отдал свои деньги. Серийные номера моих банкнот были записаны и переданы вместе с прочей информацией федеральному правительству. То же происходит в интернете. В Америке иностранную валюту достать сложнее – мы просто очень далеко от других стран. Исторически движение валюты контролируется – и далеко не только в Сети. Как я понимаю, банкоматы записывают серийные номера купюр, после чего поток данных подвергается анализу, чтобы проследить, на что деньги тратились и как использовались. Посмотрите на эти системы, посмотрите на интернет. Вы увидите, что после ухода человечества в Сеть положение с конфиденциальностью не улучшилось – наоборот, она как была мечтой, так и осталась. В этом смысле, я думаю, очень важно знать, что происходило в мире до интернета, чтобы понимать, что ждет нас впереди. А происходило и происходит вот что: если у вас есть куча денег, вы доплачиваете за конфиденциальность, а если у вас нет кучи денег, скорее

всего, никакой приватности вам не светит. В интернете все еще хуже. Биткоины – шаг в верном направлении: если скомбинировать их с анонимным каналом коммуникации, скажем, с Tor, можно посылать биткоины проекту WikiLeaks через Tor, и со стороны будет видно только, что пользователь Tor послал биткоины, а WikiLeaks их получил. Это вполне возможно – и в некоторых отношениях биткоины куда лучше налички.

ДЖУЛИАН: Мы обсуждаем приватность коммуникации и право на публикацию чего-либо. Эту концепцию очень легко понять – у нее долгая история, – и, скажем, журналисты обожают о ней говорить, потому что защищают свои интересы. Но давайте сравним ценность этой концепции с ценностью приватности и свободы экономических отношений. Всякий раз, когда ЦРУ отслеживает некую сделку, оно знает, что такой-то человек из такого-то места перевел деньги такому-то человеку в такое-то место, и оно оценивает важность этой сделки. Если экономические отношения обусловливают структуру общества, разве их свобода или приватность на деле не более важна, чем свобода слова?

ДЖЕЙКОБ: Они по своей природе взаимосвязаны. Думаю, это и есть разница между американским и европейским шифропанком – большинство американских шифропанков со мной согласятся. В обществе, где есть свободный рынок, ты вкладываешь деньги в то, во что веришь.

ДЖУЛИАН: Ты вкладываешь деньги в то, что дает тебе власть.

ДЖЕЙКОБ: Именно так. Я не говорю, что это правильно, это практически праворадикальное отношение к миру и, наверное, вовсе не то, чего мы хотим. Мы скорее за социально ограниченный капитализм.

ДЖУЛИАН: Посмотрим на ситуацию с точки зрения разведки. Пусть бюджет вашего разведуправления – 10 миллионов долларов. Вы можете либо читать электронные письма, либо отслеживать коммерческие сделки. Что вы предпочтете?

ЭНДИ: Сегодня тебе скажут: «Мы заставим платежные компании и банки использовать интернет, убив одним выстрелом двух зайцев». Именно это и было проделано. Беда в том, что изменить что-то напрямую нельзя. Можно использовать сервисы вроде Tor, чтобы защитить коммуникацию, можно шифровать телефонные звонки или электронные письма. С финансами дело обстоит сложнее, у нас есть законы об отмывании денег и прочее, и нам все время говорят, что наркобароны и террористы злоупотребляют инфраструктурой, чтобы делать очень плохие вещи.

ДЖЕЙКОБ: Всадники Инфокалипсиса.

ЭНДИ: Мне бы хотелось большей прозрачности в отношении занимающихся слежкой компаний, а также госрасходов на эти цели. Вопрос в том, что именно мы приобретем, если обеспечим полную анонимность одной только денежной системы. Что на деле произойдет? Думаю, тут и там появятся места, позволяющие расслабиться и сказать: «Знаете, я могу громко заявить о чем-то, могу пойти в парламент, а могу просто взять и подкупить несколько политиков».

ЖЕРЕМИ: Ты сейчас про США, да?

ДЖЕЙКОБ: Это не анонимность.

ЭНДИ: Я не уверен, что так будет только в США. Мы в Германии вообще не называем это коррупцией, мы говорим, что есть фонды, приобретающие картины, которые пишут жены политиков, так что я говорю, например, о торговле произведениями искусства. Для этого есть разные благозвучные названия. Может, во Франции говорят о партиях дружбы, а где-то еще – о съеме проституток.

ЖЕРЕМИ: Америка – особая статья, там политическая система и бизнес связаны очень жестко. Ларри Лессиг рассказывал, что после десяти лет изучения вопросов копирайта он отказался от попыток навести в этой области порядок (на деле не отказался), потому что осознал: проблема не в том, что политики не понимают, как надо поступать с копирайтом, проблема в том, что они связаны с индустрией, диктующей им свою гадкую политику [100] . Вот где корень всех зол.

ДЖУЛИАН: Жереми, а ты уверен, что это проблема? Может, это позитивное качество

хорошо работающей индустрии…

ЭНДИ: Кажется, адвокат дьявола вылакал мой виски.

ДЖЕЙКОБ: Посмотрим, сможет ли он закончить предложение, не лопнув от смеха. Тролльте же нас, о мастер тролль.

ДЖУЛИАН: Хорошо работающая индустрия, производящая богатство для общества, использует доходы в том числе для того, чтобы гарантировать себе дальнейшее развитие, и избавляется от непродуманных законопроектов, появившихся на свет благодаря рекламной шумихе и политическому мифотворчеству. Лучший способ сделать это – подкупить конгрессмена, то есть взять плоды производства и пустить их на то, чтобы изменить закон, угрожающий росту индустрии.

ДЖЕЙКОБ: Стойте – я приму этот удар. Ты готов? Готов? Вот прямо сейчас – ты готов? Нет.

ДЖУЛИАН: Что скажешь?

ДЖЕЙКОБ: Ты не прав по нескольким причинам, и одна из них – мощный контур отрицательной обратной связи. Например, если не ошибаюсь, в штате Калифорния одним из крупнейших спонсоров политических кампаний является профсоюз тюремных охранников, и он лоббирует более строгие законы не потому, что этим людям такое по нраву, а потому, что их зарплата зависит от числа заключенных [101] . Профсоюз убеждает политиков создавать новые тюрьмы, сажать больше народу, выносить более жесткие приговоры; что здесь, по сути, происходит? На деле охранники тратят часть зарплаты, которую им дают за хорошую работу – предположительно, – на то, чтобы расширить монополию, дарованную им государством.

ДЖУЛИАН: То есть они тратят свои деньги, переводя доходы из промышленности в индустрию, которая ничего не производит?

ДЖЕЙКОБ: Можно и так сказать.

ДЖУЛИАН: Но, может, это лишь фрагмент большой картины. В любой системе есть злоупотребления, и не исключено, что любители покататься за чужой счет, о которых ты говоришь, – это ничтожное меньшинство, а по большому счету лоббисты, влияющие на Конгресс, стоят на страже интересов промышленности, а она хочет, чтобы законы и дальше позволяли ей развиваться.

ДЖЕЙКОБ: Но это влияние очень легко измерить – достаточно посмотреть, кто содействует говорильне и желает ограничить свободы других людей, создавая ситуацию, где сами демагоги не смогли бы сделать ту карьеру, какую сделали. Когда такие вещи происходят, сразу понимаешь: что-то пошло не так, демагоги просто защищают свое положение, которого добились благодаря той же манипулятивной говорильне, эксплуатации эмоций: «Господи боже, остановите террор, остановите детскую порнографию, остановите отмывание денег, объявим наркотикам войну». Наверняка в другом контексте их речи имеют смысл, обычно какая-то доля правды в демагогии есть – именно поэтому мы и считаем ее недопустимой.

ЭНДИ: Я хотел бы вернуться к копирайту и привести еще один пример – как накалилась ситуация, когда появились автомобили. Фирмы, предлагавшие пассажирам гужевой транспорт, боялись, что техника прикончит их бизнес, и они были правы, но в той ситуации содержалась своя историческая логика. Меня как-то пригласили произнести речь перед немецкой ассоциацией киностудий, и там до меня выступал профессор берлинского университета, который чрезвычайно интеллигентно говорил об эволюции человечества и развитии культуры, – и он сказал среди прочего, что в основе всего лежат копирование идей и их дальнейшая обработка, так же как в основе кинематографа лежат некие темы и их драматургическое выражение. Через сорок минут модератор резко перебил профессора: «О’кей, после того как вы заявили, что нужно легализовать воровство, самое время послушать парня из компьютерного клуба Chaos». И я подумал: «Вау! Какого черта?.. Если я скажу то, что думаю, выйду ли я отсюда живым?» Так что индустрия иногда занимается бизнесом, который не служит эволюции. А это эгоизм – противодействовать эволюции и

делать все, чтобы сохранить свою монополию. Когда появились аудиокассеты, все тоже думали, что студии звукозаписи вымрут. Наоборот, в этой индустрии случился бум. Вопрос в том, какой политики должны придерживаться мы. Как сформулировать ее позитивно?

ДЖУЛИАН: Я вот думаю о том, нельзя ли сделать американскую практику стандартной и формализовать ее, позволив кому угодно покупать голоса в Сенате.

ЖЕРЕМИ: Нет, нет, нет, нет.

ЭНДИ: Предположим, у нас нет денег.

ДЖУЛИАН: Да, и что все прозрачно, и идет открытый аукцион.

ЭНДИ: Но производители вооружения все равно всех побьют.

ДЖУЛИАН: Нет, не думаю. Напротив, я уверен, что военно-промышленный комплекс будет оттеснен – он лучше умеет продвигать проекты за закрытыми дверьми в системе, где не действуют обычные рыночные законы.

ДЖЕЙКОБ: В этой системе есть фундаментальное неравенство.

ЖЕРЕМИ: С либерально-экономической, антимонополистической точки зрения на предложение позволить крупным игрокам формировать политику я отвечу, что в Сети за последние пятнадцать лет инновации развивались снизу вверх, новые концепции возникали ниоткуда, два парня создавали в гараже технологию, которая потом распространялась повсеместно.

ДЖУЛИАН: И это верно почти для любой корпорации – Apple, Google, YouTube, да кого ни возьми.

ЖЕРЕМИ: Кого ни возьми, именно. Любая инновация в интернете становилась внезапно успешной после нескольких месяцев или лет неизвестности, и никто не может сказать, каким будет следующий прорыв, а темп внедрения новых технологий столь велик, что опережает процесс принятия политических решений. И когда вы создаете закон, влияющий на сегодняшний рынок, на соотношение сил между разными компаниями, играющими на нем, когда вы усиливаете тех, кто и так силен, нельзя исключать, что вы переходите дорогу кому-то новому, более эффективному.

ДЖУЛИАН: Рынок нуждается в регуляции, чтобы быть свободным.

ЖЕРЕМИ: Разумеется, необходимо воевать с монополиями, для чего нужна власть бóльшая, нежели власть корпораций, тогда можно наказывать их за плохое поведение, – но я хочу сказать, что политика обязана приспосабливаться к обществу, а не наоборот. С этими войнами за копирайт складывается впечатление, что законодатель хочет заставить все общество измениться в соответствии с рамками, заданными Голливудом, и говорит: «То, что вы делаете в области культуры с вашей новой технологией, аморально, и если вы не прекратите, мы примем законы, которые вынудят вас перестать делать то, что вы считаете правильным». Так хорошая политика не функционирует. Хорошая политика смотрит на мир и приспосабливается к нему, чтобы исправлять неправильное и развивать правильное. Я убежден: если позволить сильнейшим игрокам на рынке формировать политику, мир пойдет совсем другим путем.

ЭНДИ: Я всего лишь стараюсь подвести беседу к позитивному определению хорошей политики. Твоя формулировка на этом этапе, мне кажется, сложновата. Я попытаюсь ее чуть-чуть упростить. Был такой Хейнц фон Фёрстер – крестный отец кибернетики, – когда-то он создал свод правил, одно из них гласит: «Всегда поступай так, чтобы вариантов выбора стало больше» [102] . Это относится к политике, технологии, к чему угодно – всегда делай то, что расширяет, а не сужает твои возможности.

ДЖУЛИАН: К шахматной стратегии это правило относится тоже.

ЭНДИ: Кто-то говорил, что усиление конфиденциальности денежных транзакций чревато негативными последствиями, и тут нужно подумать вот о чем: нынешняя финансовая система живет по особой логике; вопрос в том, как не дать этой системе захватить другие сферы. Ведь она обладает способностью – в отличие от сектора коммуникации – воздействовать на варианты выбора в других сферах и жестко эти варианты ограничивать. Если вы наймете киллера или купите оружие и ввяжетесь в войну с другими

странами, вы сузите спектр возможностей других людей жить и действовать. Чем больше денег я вложу в коммуникацию, тем больше вариантов получат другие. Чем больше я продам оружия…

ДЖЕЙКОБ: Нет… чем больше у тебя возможностей следить за кем-то, тем бóльшим контролем ты обладаешь.

ЭНДИ: И это еще один прекрасный довод в пользу ограничения рынка вооружений, включая телекоммуникационные технологии слежения.

ДЖЕЙКОБ: Понятно, ты хочешь ограничить меня в плане продажи таких технологий – и как ты этого добьешься? Как ты ограничишь мои возможности перераспределять доходы, в том числе через коммуникационные сети? США во время кризиса дотировали корпорации, что оскорбляло множество людей по самым разным причинам, и одна из них заключалась в том, что дотации доказали: богатство – это лишь цепочка битов в компьютерной системе. Более эффективные попрошайки сумели заполучить много битов и оказались на высоте. Тут возникает вопрос: чем ценна система, если ты можешь обвести ее вокруг пальца и получить больше всех битов? А остальных, борющихся за право претендовать на помощь, не признают годными даже на то, чтобы манипулировать их битами [103] .

ЭНДИ: То есть ты считаешь, что нам нужна совершенно другая экономическая система? Ведь сегодня ценность не связана с экономической стоимостью.

ДЖЕЙКОБ: Нет, я считаю, что экономическая стоимость объективна.

ЭНДИ: Ты можешь делать плохие вещи и зарабатывать на этом деньги – и делать хорошие вещи, не получая ни цента.

ДЖЕЙКОБ: Нет, я имел в виду, что экономика неотделима от коммуникации. Я не говорю о том, нужна ли нам другая экономическая система. Я не экономист. Я только хочу сказать, что у коммуникационных систем и у свободы коммуникации есть своя ценность, как есть ценность у свободы бартерного обмена – я обладаю правом дать вам что-то взамен вашего труда, и точно так же у меня есть право объяснить вам свою идею, а у вас есть право сказать, что вы о ней думаете. Мы не можем утверждать, что экономическая система существует в вакууме. Коммуникационная система связана с экономикой напрямую, то и другое – часть общества. Если использовать упрощенное определение и говорить о трех свободах, которые упомянул Джулиан, экономическая свобода очевидным образом оказывается связана со свободой передвижения – вы даже не можете купить билет на самолет, не заплатив за него отслеживаемой валютой, иначе сигнал о вас поступит куда надо. Если прийти в аэропорт и попытаться купить билет на этот же день за наличку, сигнал поступит куда надо.

А это значит, что вас будут дополнительно обыскивать, что вы не сможете лететь без удостоверяющего личность документа, а если вам сильно не повезло и вы заплатили за билет кредитной картой, куда надо пойдет вся информация о вас – от IP-адреса до вашего браузера. По закону о свободе информации я получил сведения о себе у иммиграционной и таможенной полиции, чтобы в будущем сравнить их с более поздними данными. Так вот, в моем досье есть имя Роджера Динглдина, купившего мне билет на самолет в качестве платы за какую-то работу, номер его кредитки, адрес дома, где Роджер находился, когда совершал покупку, название браузера и вся информация о самом билете.

ДЖУЛИАН: И эти данные получило правительство США? Они не просто хранились в процессоре, принадлежащем юридическому лицу?

ДЖЕЙКОБ: Именно. Коммерческая информация была собрана и отослана правительству в компактном виде. Самое безумное здесь то, что мы имеем дело с комбинацией трех свобод, о которых ты говорил. Мое право свободно путешествовать, мое право купить билет на самолет или попросить об этом кого-то, мое право на высказывание – мне нужно было выступить в каком-то месте, ради чего я пошел на компромисс в других сферах. На деле все это отражается на моей способности высказываться, особенно когда позднее я обнаруживаю, что власти собрали и сохранили всю информацию.

Цензура

ДЖУЛИАН: Джейк, ты расскажешь немного о том, как тебя задерживали в аэропортах США и почему это происходило?

ДЖЕЙКОБ: Мне было сказано, что меня задерживают «сами знаете почему».

ДЖУЛИАН: И причину они не назвали?

ЭНДИ: Позвольте, я обобщу? Техническая безопасность и госбезопасность – совершенно разные вещи. Технически ваша система может быть абсолютно надежной – и власти сочтут, что это плохо, потому что, с их точки зрения, безопасность означает, что они могут следить за системой, контролировать ее, взламывать защиту. Дело вовсе не в том, что Джек хотел пробраться в аэропорт, кого-то убить, захватить самолет и т. д. Дело в том, что Джейк может влиять на госбезопасность, путешествуя в другие страны, разговаривая с людьми и распространяя свои идеи. Это самое страшное из того, что может произойти сегодня с властью, – появление человека, идеи которого лучше государственной политики.

ДЖЕЙКОБ: Я очень ценю твои комплименты, но хотел бы отметить, что все куда хуже – власти собирают информацию обо всех и каждом. Это было до того, как я сделал хоть что-то, могущее их заинтересовать; я всего лишь путешествовал, а системы сами благодаря своей конфигурации собирали данные обо мне. Это было до того, как меня задерживали за что-либо, до того, как меня депортировали из Ливана, до того, как американское правительство стало присматриваться к моей персоне.

ЭНДИ: Может, они это предвидели и поняли про тебя все раньше, чем ты сам.

ДЖЕЙКОБ: Конечно, предвидели, и частично потому, что собирали обо мне информацию. Власти всегда отвечали на мои вопросы по-разному. Обычно они дают единственный ответ, и он не меняется: «Потому что у нас есть такое право». На что я говорю: «О’кей, я не оспариваю ваши права – то есть на самом деле оспариваю, но не в данный момент, – я просто хочу знать, почему вы делаете это именно со мной». И они каждый раз говорят мне: «Разве вам не очевидно? Вы работаете над сервисом Tor», – или: «Вы сидите рядом с Джулианом, чего вы хотите?» Меня это изумляет: все люди, которые меня задерживают, – обычно сотрудники пограничко-таможенной службы и иммиграционной и таможенной полиции Соединенных Штатов Америки, – сообщают мне, что у них есть право все это со мной проделывать. Кроме того, они несут чушь вроде: «Помните 11 сентября? Вот потому!» – или: «Потому что мы хотим, чтобы вы ответили на некоторые вопросы, и здесь у вас меньше прав, чем у кого бы то ни было, ну или так мы утверждаем». В таком положении они не разрешают вам звонить адвокату и ходить в уборную, зато дают воду, что-нибудь попить вроде диуретика, чтобы убедить вас, что вы и правда хотите с ними сотрудничать. Они делают это, чтобы надавить на вас, по политическим соображениям. Меня спрашивали, что я думаю о войне в Ираке и о войне в Афганистане. По сути, они на каждом этапе повторяли тактику ФБР во время COINTELPRO (масштабной секретной программы, развернутой между 1956 и 1971 годами). Например, они то и дело настаивали на праве менять мои политические взгляды – и пытались не просто менять их, но и получить особый доступ к тому, что происходит в моей голове. И они конфисковывали мою собственность. Я не имею возможности рассказать обо всем, что со мной происходило, – это темно-серая область, я не уверен, есть ли у меня право говорить о чем-либо. Уверен, что нечто похожее случалось и с другими людьми, но я никогда не слышал, чтобы они делились этим опытом.

Однажды я летал к родным по некоему делу и на обратном пути очутился в аэропорту Пирсон в Торонто. Я возвращался в Сиэтл, где жил в то время, меня остановили, подвергли вторичной проверке, третичной проверке, препроводили в ячейку для задержанных. Меня держали там так долго, что, когда я оказался на свободе, мой самолет улетел. Тут есть одна интересная деталь. Технически помещения предварительного задержания – это территория США на территории Канады, и там действует правило: если ты пропустил рейс или тебе еще долго его ждать, ты должен покинуть помещение. Меня, таким образом, долго держали на территории Америки, а потом выгнали в Канаду. Я полетел на другой конец страны, взял

напрокат машину и пересек границу. Когда я подъехал к границе, меня спросили: «Как долго вы находились на территории Канады?» – и я сказал: «Ну, пять часов плюс задержание в Торонто», – то есть я пробыл в Канаде около восьми часов. Мне сказали: «О'кей, заезжайте, мы вас снова задерживаем». Автомобиль распотрошили, мой компьютер вывернули наизнанку, мой багаж обыскали, а меня самого посадили в камеру. Мне дали сходить в туалет через полчаса – можно сказать, что они были милосердны. Такие штуки называются «исключительный пограничный досмотр» – и власти могут его производить, потому что, говорят они, у них есть такое право, и никто это их право не оспаривает [104] .

ДЖУЛИАН: Понятно. Китайцы, с которыми я общаюсь, говорили мне о великом файерволе Китая [105] . На Западе его воспринимают как цензуру, не позволяющую гражданам КНР узнавать, что об их правительстве говорят западные эксперты, диссиденты, Фалуньгун и Би-би-си, в том числе откровенную пропаганду, – но волнует китайцев на самом деле не цензура. Их волнует другое: цензура в интернете возможна, только когда за интернетом следят. Чтобы проверить, какой именно сайт кто-то посещает, запрещено на этом сайте бывать или разрешено, нужно видеть то, что видит на мониторе пользователь, – а увиденное можно и записать. Вот что китайцев жутко пугает: не сама цензура, а тот факт, что любое прочитанное ими слово отслеживается и записывается. Сказанное касается каждого из нас. Когда люди это понимают, они меняются. Их поведение меняется, и они уже не так решительно жалуются на чиновников.

ДЖЕЙКОБ: Это неправильная реакция на такого рода вещи. Проверки на границах – явление совсем не уникальное, с ним сталкивался каждый американец арабского происхождения после 11 сентября, да и до того. Просто у меня белая кожа и американский паспорт, и я этими привилегиями пользуюсь, и еще я отказываюсь молчать о происходящем: то, что со мной делают, неправильно, власти злоупотребляют полномочиями. И мы обязаны с такими вещами бороться, и в Китае тоже есть смельчаки, которые противостоят произволу властей, например Айзек Мао [106] . Он очень многое сделал для борьбы с этим типом цензуры, и правильная реакция тут – не сдаваться, не уступать давлению лишь потому, что власть заявляет, будто она имеет право на вас давить.

ЖЕРЕМИ: И опять мы вернулись к политике – ты, по сути, говоришь, что людям нужно бороться за свои права, – но люди должны понять, зачем им это надо, и иметь возможность общаться друг с другом, ведь без коммуникации какая борьба? Мне доводилось беседовать с жителями Китая – и я не знаю, занимают ли эти конкретные люди какие-то посты в КНР, или, может, власти специально отбирали их для того, чтобы они съездили за границу и поговорили со мной, – но, когда я спрашивал их о цензуре в Сети, мне часто отвечали: «Это делается на благо народа. Цензура существует, да, и, если бы ее не было, появлялись бы экстремисты, появлялось бы то, что нам не нравится, поэтому правительство принимает меры, чтобы все оставалось хорошо».

ДЖЕЙКОБ: То же самое говорят о торговле органами. Не пропадать же этим органам, верно?

ЖЕРЕМИ: Если приглядеться к китайской цензуре, окажется, что с технической точки зрения это одна из самых передовых цензурных систем в мире.

ДЖЕЙКОБ: В точку.

ЖЕРЕМИ: И я слышал, что в социальной сети «Вэйбо» – это китайский эквивалент Twitter – власти могут фильтровать сообщения по хештегу, чтобы их видели только жители конкретной провинции.

ДЖЕЙКОБ: Важно помнить, что, когда разговор заходит о цензуре в Азии, о тамошних жителях говорят как о «других», будто бы все это касается только Где-То-Там-Стана. А когда ты ищешь что-то в Google в Соединенных Штатах, система сообщает тебе, что часть результатов поиска опущена ввиду требований закона. Между этими явлениями есть разница – и в том, как они реализуются, и, конечно, в социальной реальности, в том, что, почему и даже когда именно опускается, – но по большому счету разница заключается в архитектуре системы. Скажем, американский интернет крайне децентрализован, и его очень сложно

подвергнуть цензуре в китайском стиле.

ДЖУЛИАН: Но огромная часть системы – это Google, а его можно цензурировать. Google просто не показывает огромное множество сайтов, ссылающихся на WikiLeaks.

ДЖЕЙКОБ: Безусловно. И поскольку индекс сам по себе свободен, можно провести дифференциальный анализ.

ДЖУЛИАН: Да, в теории.

ДЖЕЙКОБ: В теории, но и на практике: есть люди, которые работают над распознаванием цензуры такого типа – они сравнивают результаты поиска в разных частях мира. Думаю, важно помнить о том, что цензура и слежка – это не те явления, которые имеют место «в других странах». На Западе люди обожают говорить о том, что «жителям Ирана, Китая и Северной Кореи нужны анонимность и свобода, а у нас тут они и так есть». «Тут» обычно означает «в США». На деле цензура процветает не только при тоталитарных режимах – если ты крупная шишка, никакой режим для тебя не тоталитарный. Мы думаем, что Великобритания – чудесная страна, обычно люди уверены, что Швеция – отличная страна, но, если в любой из этих стран ты поссоришься с властями, ничего хорошего тебя не ждет. Впрочем, Джулиан еще жив, правда? Вот признак того, что Великобритания – свободная страна, верно?

ДЖУЛИАН: Я очень сильно потрудился для того, чтобы сохранить свой нынешний статус. Но, наверное, нам следует поговорить об интернет-цензуре на Западе. Это очень интересная тема. Представьте, что мы перенеслись в 1953 год и заглядываем в Большую советскую энциклопедию – в СССР она распространялась повсеместно и корректировалась по мере того, как сменялись политики. В 1953 году Берия, глава НКВД, советской тайной полиции, скончался [107] и посмертно оказался в политической опале, так что раздел о Берии, где он всячески возвеличивался, по распоряжению властей следовало удалить из энциклопедии. Взамен власти выпустили исправленный вариант статьи, который нужно было вклеить на место исходника во всех экземплярах энциклопедии до единого. И все знали, что раньше статья содержала другой текст. Я рассказываю об этом именно потому, что вклейку нельзя было не заметить, отчего та попытка изменить энциклопедию и вошла в историю. Сегодня в Великобритании Guardian и другие крупнотиражные газеты тайно убирают статьи из сетевых архивов, так что никто об этом и не знает. Ты заходишь на сайт, ищешь материал, скажем, о том, как миллиардера Надми Аучи обвинили в мошенничестве, и видишь слова «Страница не найдена» – и из реестра статей она удалена тоже. Давайте я расскажу, как соприкоснулся с историей Надми Аучи. В 1990 году, когда Ирак вторгся в Кувейт, разразилась первая война в Персидском заливе. В изгнании и после возвращения на родину правительству Кувейта требовались деньги, и оно стало продавать разные активы, включая заводы по переработке нефти за пределами страны. Бизнесмен Надми Аучи, иммигрировавший в Великобританию в начале 1980-х годов из Ирака, где он был крупной шишкой в клике Саддама Хусейна, сыграл в той сделке роль посредника, и впоследствии его обвинили в причастности к хищению 118 миллионов долларов в форме незаконных комиссионных. Это оказалось крупнейшее расследование дела о коррупции в послевоенной Европе. В 2003 году Аучи судили за мошенничество – его дело стало известно как «скандал с компанией Elf Aquitaine». Невзирая на это, Аучи зарегистрировал через люксембургский холдинг более 200 компаний – и еще больше через Панаму. Сегодня он участвует в послевоенных иракских сотовых контрактах и ведет бизнес по всему миру [108] .

Американец Тони Резко, собиравший средства для кампании Барака Обамы, когда тот баллотировался в Сенат, – старый друг Аучи. Миллиардер его финансировал. Как Аучи, так и Резко вели дела с экс-губернатором Иллинойса Родом Благоевичем. Резко и Благоевич были осуждены за коррупцию, Резко в 2008-м, а Благоевич в 2010–2011 годах (после того как ФБР перехватило телефонный разговор, в ходе которого Резко пытался продать бывшее сенатское кресло Обамы). В 2007–2008 годах, когда Обама боролся за то, чтобы стать кандидатом в президенты от Демократической партии, американская пресса принялась изучать его связи. Они навели справки о Резко и выяснили, что он имеет отношение к

покупке дома Барака Обамы. В 2008 году, незадолго до суда, Резко получил от Аучи 3,5 миллиона долларов, о чем не сообщил суду, хотя обязан был сделать это, – за что его и посадили. Американские СМИ обратили внимание на Аучи, а он поручил британской адвокатской конторе Carter-Ruck провести агрессивную кампанию и изъять статьи 2003 года о скандале с Elf Aquitaine и о приговоре, вынесенном во Франции. Эти действия по большому счету были успешными. Аучи обработал британские СМИ и даже американских блогеров – нам известно о дюжине изъятых из Сети статей. Бóльшая их часть, включая материалы в архивах британских газет, испарилась, словно их и не существовало. Нигде нет сообщений типа «текст убран в связи с тем, что его содержание оспорено в законном порядке». Статьи исчезли и из реестров. Мы в WikiLeaks нашли их и опубликовали заново [109] .

ДЖЕЙКОБ: Историю уничтожили.

ДЖУЛИАН: История с Аучи не просто изменена, она перестала существовать. Как говорил Оруэлл: «Тот, кто контролирует настоящее, контролирует прошлое, а тот, кто контролирует прошлое, контролирует будущее». Вот вам пример неотслеживаемого уничтожения истории на Западе, фактически – цензура после публикации. Самоцензура до публикации куда более опасна, но зачастую ее сложно отследить. Мы наблюдали это на примере с «Кабельгейтом»: WikiLeaks работает с разными СМИ по всему миру, и мы видим, кто именно подвергает наши материалы цензуре [110] . Скажем, газета New York Times отредактировала телеграмму, согласно которой миллионы долларов были выделены на то, чтобы через действующие в Ливии нефтяные компании тайно влиять на занимающих видные посты ливийцев. В сообщении даже не указывались названия компаний, но New York Times убрала фразу «связанные с нефтью компании» [111] . Однако самый смак – это когда New York Times взяла сообщение о ядерной программе Северной Кореи на 62 страницах – о том, продавали корейцы ядерные ракеты иранцам или нет, – и вырвала оттуда два абзаца, чтобы доказать, что у Ирана есть ракеты, которыми можно ударить по Европе, в то время как в исходном тексте говорилось совершенно об обратном [112] .

Guardian отредактировала сообщение о том, что Юлия Тимошенко, бывший премьер-министр Украины, возможно, прячет свое состояние в Лондоне [113] . Эта же газета убрала утверждения о том, что казахстанская элита в целом коррумпирована – хотя там не называлось ни одного имени – и что коррупция коснулась как ENI, итальянской энергетической компании, действующей в Казахстане, так и British Gas [114] . В основном Guardian подвергала цензуре сообщения с обвинениями в адрес богатых персон, если только те не входили в список лиц, на которых газета должна нападать [115] . Например, в сообщении о болгарской организованной преступности назывался некий русский, и Guardian выставила его чуть ли не главным антигероем, хотя, кроме него, в сообщении упоминалось очень много организаций и людей [116] . Der Spiegel убрала абзац о канцлере Ангеле Меркель, в котором ни слова не было о правах человека, только о политике [117] . Таких примеров очень много [118] .

ЭНДИ: Наше понимание свободы информации и свободного инфопотока – это в некотором смысле очень радикальная и новая концепция для планеты Земля. Я бы не сказал, что Европа тут сильно отличается от государств в других частях света. Есть страны с демократическим стержнем – это означает, что вы можете читать что угодно, знать что угодно и даже вести юридическую войну против цензурной инфраструктуры, что нереально в Саудовской Аравии или Китае, но это не значит, что в странах с демократическим стержнем цензуры нет вообще.

ДЖУЛИАН: Мой опыт говорит мне, что на Западе цензура куда более изощренна и многослойна – она умышленно пудрит людям мозги и уводит их от понимания того, что происходит на самом деле. Такая сложность нужна, чтобы отрицать существование цензуры в принципе. Ее можно представить в виде пирамиды. Из песка выглядывает только верхушка – но так и задумано. Эта верхушка – дела о клевете, убийства журналистов, видеокамеры, посылающие информацию военным, и т. д. – официально признаваемая цензура. Но это

лишь мельчайший компонент цензуры вообще. Под песком скрыт следующий слой – все те люди, которые не хотят светиться и практикуют самоцензуру, чтобы остаться в тени. Следующий слой – все виды экономических стимулов и покровительства, которые даются взамен согласия писать о тех или иных вещах. Следующий – экономика в чистом виде: ты освещаешь то, о чем говорить экономически выгодно, даже без учета предыдущего слоя. Следующий – предрассудки не слишком образованных читателей: с одной стороны, такими людьми легко манипулировать, всучивая им ложную информацию, с другой – им не расскажешь сложную правду, они ее не поймут. Последний слой – распределение информации: скажем, многие не в состоянии прочесть новость на другом языке. Когда Guardian редактирует сообщения «Кабельгейта», это второй слой.

Существование такой цензуры можно отрицать – либо ее нельзя отследить, либо нет инструкций, которые предписывают замалчивать такую-то информацию. Журналистам редко говорят, мол, не пиши то или не печатай это. Скорее журналист понимает, чего от него ждут, – он знает, в чем именно заинтересованы люди, которых нужно задобрить. Если журналист будет паинькой, его погладят по голове и вознаградят, в противном случае – не погладят и не вознаградят. Все очень просто. Мне нравится вот какое рассуждение: прямолинейная советская цензура, о которой так много кричали на Западе, – ночью люди в армейских сапогах приходят и уводят журналиста из дома – всего лишь сместилась на двенадцать часов. Теперь мы ждем светлого времени суток и средь бела дня отбираем дома у журналистов, когда они попадают в опалу и не в состоянии выплачивать долги. Журналиста уводят из дома, когда дом отбирают. Западное общество специализируется на «отмывании» цензуры и таком структурировании деятельности власть имущих, чтобы любое общественное высказывание, прошедшее через сито, никак не могло повлиять на истинный расклад сил в обществе, где все кому-то что-то должны. Этот расклад скрыт за многослойной сложностью и секретностью.

ЭНДИ: Жереми говорил про педонацистов.

ДЖЕЙКОБ: Опять эти педонацисты.

ЖЕРЕМИ: Два всадника Инфокалипсиса в одном.

ЭНДИ: Педонацисты – отличное обобщение доводов в пользу цензуры в Германии, а частично и в Европе. Германия из-за исторического бэкграунда не желает видеть в Сети риторики ненависти [119] , и, конечно, если правительство говорит, что нужно ввести цензуру в интернете, чтобы победить педофилов, ему позволят делать что угодно. Есть рабочий доклад Европейской комиссии для внутреннего пользования о сохранении информации, и там сказано: «Следует больше говорить о детской порнографии, тогда народ с нами согласится» [120] .

ДЖУЛИАН: Расскажешь об этом чуть подробнее? Если мы хотим очистить интернет от какого-то одного сегмента, скажем, от детской порнографии, то, чтобы оградить от нее пользователей, нам нужно отслеживать деятельность каждого. Нужно создать соответствующую инфраструктуру. Мы должны практиковать массовую слежку и сформировать целую цензурную систему, чтобы убрать из Сети один сегмент.

ЭНДИ: По такой схеме работает весь механизм – например, так называемая система предварительной цензуры в Германии обязывает вас назвать лицо, которое несет юридическую ответственность за все, что вы публикуете. Грубо говоря, если вы публикуете какую-то информацию на бумаге или в интернете и не говорите, кто именно несет ответственность за контент, вы уже нарушили закон. Другими словами, власть перераспределяет ответственность, и, если кто-то нарушает закон, распространяя, например, детскую порнографию или риторику ненависти, всегда можно сказать: «Так, посмотрим, где этот парень живет, арестуем его и уберем дрянь из Сети».

ДЖУЛИАН: То есть мы подвергаем цензуре публикатора, а не читателя.

ЭНДИ: Именно. Логичнее было бы запретить смотреть что-то. Я согласен с тем, что не всякая информация должна находиться в открытом доступе для всех и каждого, – риторику ненависти иногда сопровождают адреса тех или иных людей, что может привести к

ситуациям, которые мне не нравятся.

ДЖУЛИАН: Энди, но это же так по-немецки. Чтобы сделать что-то, чтобы решить, что приемлемо, а что нет, нужен комитет, но сперва назначить членов комитета, а для этого – запустить процесс назначения членов комитета…

ЭНДИ: Да, у нас такой фигни полно. Те же массовые убийства во время Второй мировой войны – нацисты тщательно описывали все, что делали, составляли реестры захваченной собственности. Бюрократическая машина работала вовсю. Можно сказать, что немцы необоснованно убили много людей – истинная правда, – но делали они это как бюрократы. Такова Германия.

ДЖУЛИАН: Когда необходимо решить, что подвергать цензуре, а что нет, нужно сделать две вещи. Во-первых, создать техническую архитектуру, которая в принципе это позволяет. Создать государственную цензурную машину, которая сможет работать эффективно. Во-вторых, для цензуры вам требуются комитет и бюрократия. И этот комитет должен быть по определению тайным – он абсолютно бесполезен, если не является засекреченным и не осуществляет тайного правосудия.

ЭНДИ: Знаете, у нас в Германии есть одно хорошее правило…

ДЖЕЙКОБ: Только одно?

ЭНДИ: Правило такое: если закон нельзя исполнить, он не имеет права на существование. Когда закон не имеет смысла, скажем, если он запрещает ветряные мельницы или что-то в этом роде, немцы говорят: «Ладно, забудем». Нас с вами вдохновляет интернет образца первых лет, когда он только начинал развиваться, – инфопоток был свободен: никто его не ограничивал, не блокировал, не подвергал цензуре, не фильтровал. Распространив наше понимание свободного инфопотока на всю планету – а в каком-то приближении это явление планетарного масштаба, – мы увидим, конечно, что он повлиял на власть, на то, как она проводит в жизнь решения, на цензуру, как предварительную, так и по факту или любую другую. Мы все знаем о возникающих на этой почве конфликтах. Вопрос заключается в том, какова наша концепция власти, ну или будущей послеправительственной организации, ППО, – возможно, одной из первых ППО стал проект WikiLeaks, – потому что я не уверен, что правительства отдельных стран в состоянии решить проблемы этой планеты вроде экологических.

ДЖУЛИАН: Правительства тоже в этом не уверены – неясно, где проходит граница между ними и прочим миром. Правительства размыты. Они расположены в физическом пространстве, а WikiLeaks занимает часть пространства в Сети. Интернет-пространство включено в физическое, однако отношения между ними настолько сложны, что второе не может даже сказать, что первое – это его часть. Вот почему появилось понятие киберпространства, какого-то иного мира, который существует вне нашего, – из-за того, что интернет не связан с физическим миром напрямую, сложен и универсален. Один и тот же файл в интернете можно прочесть в любой точке земного шара как в настоящем, так и в будущем – отсюда универсальность. В этом смысле проект WikiLeaks, занимающий киберпространство и наловчившийся перемещать информацию, невзирая на препятствия в физическом мире, можно назвать организацией из эпохи, в которой государств уже нет, – нас нельзя контролировать географически. Я не хотел бы доводить аналогию до абсурда – все-таки я сижу под домашним арестом. Принудительная сила государства очевидным образом действует на всех людей, где бы они ни находились. Но журналисты любят делать акцент на том, что мы – средство массовой информации, не привязанное ни к одной стране, и они правы, когда подчеркивают последнее обстоятельство. Я всегда говорил: «Как вы думаете, что представляет собой компания Newscorp? Это огромная транснациональная корпорация». Однако Newscorp структурирована таким образом, что на ее ключевые компоненты может влиять власть. Вот почему компании пришлось так нелегко, когда в Великобритании разразился скандал с телефонной прослушкой, вот почему Newscorp пытается присосаться к американскому истеблишменту. Но если ее активы – это в основном информация, организация может стать транснациональной настолько, что уничтожить ее

будет непросто – из-за криптографии. Поэтому нас поместили в финансовую блокаду – прочие наши стороны подавить труднее [121] .

ДЖЕЙКОБ: Давайте взглянем на настоящее оптимистически и вернемся к тому, о чем мы говорили. Ты спрашивал, как меня притесняли, ты спрашивал о цензуре в странах Запада, и я говорил про обамовскую программу точечных убийств, о которой говорят, что она законна, потому что состоялся судебный процесс и убийцы исполняют приговор.

ДЖУЛИАН: Это был тайный судебный процесс.

ДЖЕЙКОБ: Все это можно привязать к Джону Гилмору. Один из его исков касался права анонимно перемещаться по США, и судья в итоге сказал буквально следующее: «Слушайте, нам нужно свериться с секретными правовыми актами. Мы заглянем в эти акты и поймем, можете ли вы делать то, на что вы имеете право, или нет». Они заглянули туда и обнаружили, что Гилмор имеет право перемещаться анонимно – они никак не ограничивали его права. Он так и не узнал, что это за акты, а власти по итогам выигранного им процесса изменили политику управления безопасностью перемещений и Министерства национальной безопасности – оказалось, что права граждан ограничены секретными актами в недостаточной мере [122] .

ДЖУЛИАН: Теперь они ограничены больше прежнего?

ДЖЕЙКОБ: По сути – да, закон стал требовать от тебя еще больше бумаг. Важно заметить, что программа точечных убийств, притеснение людей на границах, цензура в интернете, цензура, которую корпорации осуществляют по требованию властей и по требованию менеджеров самих корпораций, все явления подобного рода – звенья одной цепи. Все они доказывают, что государство присвоило себе слишком много власти в сферах, где мы эти явления наблюдаем. Сконцентрированная в данных сферах власть привлекла людей, которые ею злоупотребляют или хотят еще больше власти. И даже когда ее применение оправданно, мы видим, что мир стал бы лучше, если б не был настолько централизован, если б не шагал к авторитаризму. Запад в этом смысле ничем не отличается от других стран – как оказалось, сидящий над нами царь кибербезопасности не слишком-то отличается от царя, который полвека назад распоряжался в какой-нибудь другой стране силами внутренней безопасности. Мы создаем такие же авторитарные структуры контроля, они привлекают тех, кто хочет ими злоупотребить, и при этом мы пытаемся сделать вид, что на Западе все по-другому. У нас все то же самое, потому что есть единая шкала власти от авторитаризма до либертарианства. Я имею в виду не американскую систему политических партий, я имею в виду, что на этой шкале США очень далеки от СССР, но по многим, очень многим параметрам они куда ближе к СССР, чем Христиания, автономное самоуправление в Копенгагене [123] . И, подозреваю, еще дальше от потенциального утопического мира, который появился бы на Марсе, если б мы основали там новую колонию. Там мы создали бы общество, далекое от тоталитаризма и авторитаризма настолько, насколько возможно. Такого общества у нас нет, и это наше поражение.

ЖЕРЕМИ: Соглашусь: все эти темы связаны между собой. Обсуждая концентрацию власти, мы опять же говорим об архитектуре системы. Обсуждая цензуру в интернете, мы говорим о централизации власти, которая решает, к чему можно иметь доступ, а к чему нельзя, и о том, правомерна ли цензура – правительственная или частных компаний. Вот вам пример: провайдер Orange на несколько недель перекрыл доступ к нашему сайту laquadrature.net. Тот попал в список веб-страниц, на которые не допускались лица моложе 18 лет. Вероятно, мы упомянули детскую порнографию, когда высказались против цензурного законодательства, или, может быть, мы не понравились провайдеру, потому что не одобряем его политику, направленную против сетевой нейтральности, и выступаем за закон, который запретил бы таким, как он, ограничивать сетевую коммуникацию [124] . Нам об этом не скажут. Но здесь мы имеем дело с частным бизнесом, который на уровне сервиса перекрыл доступ к информации в интернете. Я вижу здесь главный риск, и он связан с властью, которую мы даем Orange, или правительству КНР, или кому-то еще.

ДЖЕЙКОБ: Уточнение: когда ты говоришь о частном бизнесе в Великобритании, ты

имеешь в виду, что этому провайдеру принадлежат все коммуникации, оптоволоконные соединения и т. д. – или же что он использует ресурсы государства? Кто выдает ему лицензию на беспроводную передачу? Государство с ним вообще не связано? Есть ли у этого провайдера обязанность заботиться о клиентах?

ЖЕРЕМИ: У таких провайдеров есть лицензии. То ли власть, то ли бизнес меняют архитектуру интернета – вместо единой универсальной сети нам предлагают балканизированное множество маленьких субсетей. Мы все время обсуждаем глобальные проблемы, будь то летящая в тартарары финансовая система, или коррупция, или геополитика, или энергетика, или экология. Сегодня, когда человечество столкнулось с такими проблемами, у нас есть глобальное средство связи, благодаря которому улучшились коммуникация, распространение знаний и участие в политических и демократических процессах. Я подозреваю, что глобальная универсальная Сеть – единственный инструмент, каким мы располагаем, чтобы решить глобальные проблемы, поэтому битва за свободный интернет – наша главная битва, и мы все здесь несем ответственность за ее исход.

ЭНДИ: Я полностью согласен: нам нужно убедить людей в том, что интернет – это универсальная сеть со свободным потоком информации; нам нужно не просто констатировать данный факт, но и обличать компании и провайдеров, которые предлагают нечто, называющееся интернетом, но на деле им не являющееся. Однако мне кажется, что мы не ответили на ключевой вопрос, касающийся фильтрации данных. Я приведу пример проблемы, которую нам необходимо решить. Лет десять назад мы протестовали против так называемых умных фильтров компании Siemens. Это одна из крупнейших телекоммуникационных фирм в Германии, производитель разведывательного ПО. Siemens торговал программами-фильтрами, которые позволяли, например, сделать так, чтобы работники данной фирмы не могли зайти на сайт профсоюза и прочесть о своих трудовых правах. Кроме прочего, эти фильтры блокировали и компьютерный клуб Chaos, что нас очень расстроило. Якобы у нас имелся «преступный контент» или что-то такое. Мы подали на Siemens в суд. А на выставке решили организовать большой митинг протеста и окружить стенды Siemens, чтобы люди шли через нас, как через фильтр. Забавно было то, что мы объявили об акции на нашем сайте, чтобы привлечь максимум народа, а работники Siemens ни черта о ней не знали – они использовали те же программы-фильтры и не могли прочесть предупреждение, хотя мы и не думали его скрывать.

ДЖУЛИАН: Пентагон установил у себя фильтры, не пропускающие любое электронное письмо со словом WikiLeaks. Работающие по делу Брэдли Мэннинга следователи, разумеется, рассылали имейлы о WikiLeaks за пределы Пентагона, но не получили ни одного ответа – система отфильтровала все письма, в которых содержалось это слово [125] . Государство национальной безопасности может сожрать само себя.

ЭНДИ: Что возвращает нас к главному вопросу: существует ли такая штука, как информация с негативным воздействием? Или, с точки зрения общества, нужна ли нам цензура в интернете, потому что она полезна для общества в целом? Даже если мы говорим о детской порнографии, можно сказать: «Погодите, детская порнография высвечивает проблему – насилие над детьми, а чтобы решить проблему, мы должны иметь о ней представление».

ДЖЕЙКОБ: Детская порнография доказывает, что совершено преступление.

ДЖУЛИАН: Нет, она служит поводом для лоббистов.

ЭНДИ: Это, конечно, самый радикальный подход, но если мы говорим о нацистах или о чем-то еще, нам нужно как-то называть то, о чем идет речь. Семейные люди спросят себя: «Разве не лучше для общества отфильтровывать всякую дрянь, чтобы сосредоточиться на чем-то хорошем? Или фильтры ограничивают нашу способность видеть проблемы и решать их?»

ЖЕРЕМИ: Думаю, цензура – это точно не решение. Говоря о детской порнографии, мы не должны даже употреблять слово «порнография» – речь идет о совершении преступления, о насилии над детьми. Нужно найти сервер, отключить его, вычислить людей, загрузивших в

него контент, определить, кто именно создал этот контент, кто совершил насилие над детьми – вот что важнее всего. И если тут замешана преступная группа, коммерческая сеть и т. д., следует арестовать преступников. А мы, когда принимаем законы – у нас во Франции есть закон, дающий МИДу административную власть решать, какие сайты необходимо блокировать, – никак не мотивируем правоохранительные органы находить тех, кто создает преступный контент. Мы говорим: «Ах, давайте закроем всем доступ к плохому контенту», – словно можно решить проблему, закрыв глаза тому, кто на нее смотрит. С этой точки зрения, я думаю, достаточно сказать одно: мы все согласны с тем, что такие фотографии нужно убирать из Сети.

ДЖЕЙКОБ: Извини, но меня всего выворачивает. Весьма огорчительно слышать от тебя подобные доводы. Меня реально тошнит, потому что ты только что сказал: «У меня есть право демонстрировать власть над другими людьми, и я хочу использовать эту власть, чтобы уничтожить историю». Может быть, я в данном случае покажусь экстремистом – как и во многих других случаях, само собой, – но я рискну сказать то, что скажу. Это пример, демонстрирующий, как уничтожение истории оказывает нам медвежью услугу. Благодаря интернету мы поняли, что в обществе бушует эпидемия насилия над детьми. Мы поняли это по детской порнографии – думаю, лучше называть ее эксплуатацией детей; мы увидели доказательства. Прятать их, уничтожать их – я думаю, абсурдно, ведь они позволяют многое понять про общество в целом. Скажем, можно узнать – после того как я закончу это предложение, мне не сделать карьеру в политике, однако против правды не попрешь, – можно узнать, кто именно производит детскую порнографию и кто становится ее жертвой. Игнорировать проблему невозможно. Нужно сделать все, чтобы обнаружить корень зла, то есть тех, кто эксплуатирует детей. По иронии судьбы здесь нам пригодятся технологии слежения: преступник опознаётся по лицу и идентифицируется по метаданным на фотографиях. Уничтожать снимки, создавать правила игры, при которых вот это можно уничтожать, а вон то – нет, создавать организации, осуществляющие цензуру и полицейский надзор, – значит идти по скользкой дорожке, а она, как мы видели, привела нас прямо к копирайту, к другим системам надзора и слежки. Именно потому, что борьба с детской порнографией – дело благородное, нам нельзя искать легких путей. Может, надо пытаться раскрывать преступления и помогать тем, кто стал жертвой, даже если это обойдется нам дорого. Может, нужно не закрывать глаза, а открыто сказать: вот огромная проблема для общества – и она проявляется в интернете особенным образом.

Когда компания Polaroid стала выпускать фотоаппарат Swinger для моментальных фотоснимков, с его помощью тоже совершались такого рода преступления. Но это не значит, что нужно уничтожать технику или следить за ней. Нужно находить и наказывать преступников на основании технически задокументированных улик. Не следует набрасываться на технику и вредить обществу в целом. Если мы говорим об авторах детской порнографии, давайте поговорим и о полиции. Во многих странах правоохранительные органы притесняют людей на регулярной основе. Думаю, в интернете больше злоупотребляющих властью полицейских, чем тех, кто выкладывает детскую порнографию.

ДЖУЛИАН: Почти определенно больше.

ДЖЕЙКОБ: Мы знаем, что в мире есть N полицейских и что X из них нарушали этические требования к профессии, причем по-крупному. Если взглянуть на историю движения «Захвати» (Occupy), мы это увидим. Должны ли мы подвергать Сеть цензуре только потому, что нам известно: да, некоторые полицейские – плохие парни? Должны ли мы вредить полиции и не давать ей делать полезную работу?

ДЖУЛИАН: Есть еще проблема повторной виктимизации, когда сам ребенок – в детском возрасте или когда он уже стал взрослым – или те, кто с ним общается, видят фотографии, на которых запечатлено преступление.

ДЖЕЙКОБ: Пока копы рыщут по Сети, мой удел – повторная виктимизация.

ДЖУЛИАН: Ты мог бы говорить о повторной виктимизации, если бы, например, увидел фотографию, на которой тебя бьет полицейский. Я бы сказал, что важнее защищать

неприкосновенность истории, чтобы в будущем люди точно знали, что происходило в нашу эпоху; повторная виктимизация случается, но вводить из-за этого цензуру, которая уничтожит большие куски истории, – значит расписаться в том, что мы не можем справиться с проблемой, потому что ее не видим. В 1990-е годы я давал связанные с интернетом консультации австралийским полицейским, которые преследовали педофилов, – подразделению по борьбе с сексуальной эксплуатацией детей штата Виктория. Этих копов фильтры в интернете отнюдь не радовали: когда детской порнографии в Сети не видно, исчезает лобби, благодаря которому полиция получает средства на борьбу с педофилией.

ЖЕРЕМИ: Мы все согласны с тем – и это, я думаю, самое важное, – что в конечном итоге следует говорить об индивидуальной ответственности производителей контента, которые создают детскую порнографию и прочее, и именно с этими людьми должна работать полиция.

ДЖЕЙКОБ: Мы не все с этим согласны. Я совсем о другом.

ДЖУЛИАН: Нет, Жереми говорит о производстве контента, а не о его публикации, – тут есть разница.

ДЖЕЙКОБ: Производство контента – это вообще другая тема. Маленькое уточнение: если, например, ты совершишь насилие над ребенком, а Энди сделает фотографию в качестве доказательства, я не думаю, что он будет наказан.

ЖЕРЕМИ: Нет, накажут всех тех, кто участвовал в совершении насилия. В том числе подельников и подстрекателей.

ЭНДИ: Но есть люди, которые совершают насилие над детьми, чтобы его сфотографировать, верно?

ДЖЕЙКОБ: Конечно, есть.

ЭНДИ: Тут можно говорить еще и об экономическом аспекте.

ДЖЕЙКОБ: Полностью соглашусь, и я бы эти вещи различал: контент – историческая запись, доказательство того, что совершено преступление, очень серьезное преступление, и нам нельзя забывать о повторной виктимизации, но главное тут – исходная виктимизация, когда ребенок становится жертвой, и не важно, фотографируют его или нет.

ЖЕРЕМИ: Разумеется. Я именно об этом.

ДЖЕЙКОБ: Есть фотографии, нет фотографий – почти не имеет значения. Если они есть, важно помнить, что конечная цель – остановить и наказать преступника. А это невозможно, если у нас нет доказательства совершения преступления – и стимула для тех, кто умеет раскрывать такие преступления. Я думаю, это чрезвычайно важно, но мы сплошь и рядом забываем, ведь легче всего притвориться, что детской порнографии не существует, остановить ее распространение и сказать, что преступления прекратились. А они не прекратились.

ЭНДИ: Беда в том, что сейчас многие предпочтут легкое решение – ведь прямо смотреть на то, что происходит на самом деле, очень неуютно. Полагаю, у нас есть шанс решить проблему на политическом уровне, потому что мы не предлагаем ее игнорировать или же сделать невидимой. Речь идет в том числе о политике в отношении киберпространства, и тут возникает вопрос, как общество вообще решает такие проблемы. Я сильно сомневаюсь, что есть информация, вредная сама по себе. Вопрос, конечно, в возможности фильтрации контента, и лично я не готов смотреть на любые картинки, выкладываемые в интернет. Среди них есть, на мой взгляд, отвратительные, есть те, которые меня отвлекают, однако то же самое верно и для ближайшего магазина с фильмами – он предлагает выдуманные и гадкие истории. То есть вопрос в том, волен ли я сам решать, что смотреть, какие данные обрабатывать, какие тексты читать. Отсюда мы переходим к программам-фильтрам. Кстати, Вау Холланд, основатель компьютерного клуба Chaos, однажды остроумно заметил: «Фильтры должен ставить конечный пользователь, причем так, чтобы они стояли в его конечном устройстве» [126] .

ДЖУЛИАН: То есть фильтрация – забота того, кто получает информацию.

ЭНДИ: Фильтровать надо здесь. Здесь! (*Показывает на голову.*)

ДЖУЛИАН: В мозгу.

ЭНДИ: В конечном устройстве конечного пользователя, в этой штуке между ушами. Именно здесь должны стоять фильтры, и никакое правительство от имени народа не должно ничего цензурировать. Если ты не хочешь чего-то видеть, никто тебя не заставит, а фильтровать самые разные данные ты сегодня так или иначе обязан.

Приватность для слабых, прозрачность для сильных

ДЖУЛИАН: Энди, я говорил недавно с президентом Туниса и спросил его о том, что станет с архивами разведки, сохранившимися после диктатора Бен Али, – там документы местного, тунисского Штази, – и он сказал, что в них, конечно, есть много интересного, но вообще это проблема, архивы опасны, и он бы от них постепенно избавился. В любом случае он считает, что ради сплоченности Туниса архивы необходимо засекретить, чтобы никто не искал козлов отпущения. Когда власть Штази в ГДР кончилась, ты был совсем юным. Расскажи нам об архивах Штази и о том, что ты думаешь про обнародование секретных материалов.

ЭНДИ: По всей вероятности, разведуправление Германии обладает самыми большими архивами в мире, ну или одними из самых больших. Все документы из восточногерманской Staatssicherheit [127] – инструкции, методички, учебные пособия, внутренние отчеты – в общем и целом рассекречены. «В общем и целом» означает, что не ко всем документам можно легко получить доступ, но многие из них вполне открыты, и правительство создало учреждение, хранящее те бумаги Штази, которые немецкие граждане имеют право изучить.

ДЖУЛИАН: Правительство Германии создало Федеральную комиссию по материалам Штази (Bundesbeauftragte für die Stasi-Unterlagen, BStU), и она предоставляет доступ к большому архиву документов.

ЭНДИ: Да, и журналисты могут подавать так называемые исследовательские запросы, чтобы изучить какие-то материалы. Запрашивать информацию допускается на любую тему. Издано немало книг, а также исследований, раскрывающих особенности действий Штази в разных областях. Думаю, из таких документов можно узнать много полезного. Понятно, что нельзя ожидать от Туниса публикации всех личных дел, которые вело бывшее разведуправление: президент страны – нынешний президент – должен решить, готов ли он делиться информацией о себе, о своих союзниках и т. д. Тайная полиция не считается с приватностью, в твоем деле есть записи о сексуальной жизни, о телефонных звонках, денежных переводах, обо всем том, что ты делал, и вряд ли кто-нибудь захочет все это оглашать.

ДЖУЛИАН: Ты следил, как развивалась ситуация с Амн-аль-Даула, тайной полицией Египта? Тысячи египтян ворвались в ее бюро и разграбили архивы, пока работники Амн-аль-Даула пытались их сжечь, уничтожить, вывезти на мусорную свалку. В итоге многие документы получили огласку и широко разошлись в народе. Можно купить чье-нибудь досье за два доллара на местном рынке и загрузить его в интернет. Никакой катастрофы не произошло.

ЭНДИ: Нет, я всего лишь говорю, что понимаю людей, которые не хотят, чтобы их личные данные были обнародованы. Если бы я жил в государстве, сорок лет копившем обо мне информацию и отмечавшем, когда я посещаю сортир, я бы этого тоже не хотел.

ДЖУЛИАН: Но есть же анализ плюсов и минусов, верно? С моей точки зрения, тот, кто однажды стал «крысой», остается осведомителем навсегда.

ЭНДИ: Все так, но хакерская этика предписывает, грубо говоря, использовать общественную информацию и защищать частную, так что я уверен, что если мы выступаем за приватность – а у нас есть на то очень веские причины, – нам не следует сравнивать плюсы и минусы. Это разные ситуации. Обнародовать такого рода информацию нам нельзя.

ДЖЕЙКОБ: Однако плюсов тут больше, причем во много раз. Вернемся на шаг назад. Ты исходишь из совершенно неверной предпосылки, согласно которой информация является частной, если доступ к ней ограничен, а это не так. Скажем, в моей стране доступ к

засекреченной информации, в том числе к моим личным данным, имеет миллион человек…

ДЖУЛИАН: Четыре миллиона триста тысяч…

ДЖЕЙКОБ: Разве можно называть эти данные личными? Проблема в том, что подобная информация не на сто процентов засекречена от всех людей на планете.

ДЖУЛИАН: Это тайна для бессильных, но не для сильных мира сего.

ЭНДИ: Да, вы правы. Но если мы хотим открыть архивы для всех…

ДЖУЛИАН: В некоторых европейских странах так и сделали.

ЭНДИ: Нет. Я не помню ни одной страны, которая обнародовала бы все досье.

ДЖУЛИАН: Скажем, в Польше архивы открыты в большей степени, нежели в Германии.

ЭНДИ: Возможно. У сделки, на которую пошла Германия, имелась и обратная сторона: бывшие офицеры госбезопасности ГДР стали управлять не только архивами Штази, но и частью так называемой Новой Германии, экс-ГДР. Есть любопытная история о фирме, взявшей подряд на уборку в помещении, где хранятся архивы. Эта фирма выиграла тендер, предложив самые дешевые услуги. А через шесть лет хранящее досье учреждение обнаружило, что фирма, поддерживающая чистоту в здании, организована бывшими работниками Штази.

ЖЕРЕМИ: Я читал сообщение об этом на сайте WikiLeaks. Прекрасная история [128] .

ЭНДИ: WikiLeaks выложил донесение о том деле, так что ты прав: если досье уже собраны и попали в руки плохих людей, говорить о приватности сложно.

ДЖУЛИАН: Давайте перейдем к более общей теме. Благодаря интернету объем доступной информации вырос просто неимоверно. Образовательная функция Сети поражает воображение. С другой стороны, люди говорят о WikiLeaks: «Смотрите, вся частная правительственная информация теперь в открытом доступе, власть не в состоянии хранить секреты». Я утверждаю, что это чушь. Я утверждаю, что WikiLeaks – лишь тень тени. То, что мы выложили в Сеть информацию объемом более миллиона слов, – производная от неимоверного увеличения общего количества секретных материалов. Власти обладают такими огромными объемами закрытых данных, что по сравнению с ними информация, которой кормят общественность, ничтожна, а WikiLeaks – это всего лишь доля процента от государственных тайн. Давайте посмотрим на облеченных властью инсайдеров, которым известны детали любой транзакции любой кредитной карты, и сравним их с людьми, могущими через Google найти тексты и комментарии в чьих-то блогах. Как вам это сравнение?

ЭНДИ: Я бы сказал, что было бы лучше, если б записи о транзакциях оказались обнародованы, – все поняли бы, что любая оплата по кредитной карте оставляет свой след. Есть люди, которые, если рассказать им о всеобщей слежке, сочтут объяснения слишком сложными и абстрактными. Они поймут, в чем дело, только если увидят в Сети записи о самих себе.

ДЖУЛИАН: Или заглянут в свои досье из Facebook – 800 мегабайт информации о каждом пользователе.

ЭНДИ: После падения восточного блока канцлер ФРГ Гельмут Коль решил объединить Германию, и на переговорах по схеме 2+4 американцы поставили свои условия. Они сказали, что хотели бы и дальше контролировать немецкие телекоммуникации, следить за ними, а Коль думал, что это не важно, – он не понимал, что такое слежка за телекоммуникациями. Люди из его команды рассказали мне, что поведение канцлера очень их огорчало и в итоге они распечатали около 8000 страниц расшифровок его телефонных разговоров, записанных Штази, и привезли их в кабинет Коля на двух маленьких тележках. И он сказал: «Что это, черт подери, такое?» А они ответили: «Ваши разговоры по телефону за последние десять лет с разными людьми, включая ваших подружек, вашу жену, вашу секретаршу и т. д.». Тут-то Гельмут Коль и понял, что такое телекоммуникационный перехват. Так что да, досье тайной полиции помогают осознать, чем она занимается. Мы можем ратовать за обнародование всей информации, и, если устроить голосование, я не уверен, что буду против.

ДЖУЛИАН: Я не хочу долго об этом говорить – само собой, пока ты расследуешь преступления мафии, информация должна оставаться секретной. Есть обстоятельства, когда секретность может казаться оправданной. Я не говорю, что она оправданна как политика; я говорю, что политически секретность неизбежна. В ее пользу свидетельствуют политически убедительные аргументы типа «эти парни уже совершили убийство, теперь они замышляют еще одно», и не важно, что мы с вами думаем о легитимности перехвата информации, – так или иначе ее будут перехватывать. Эту политическую схватку не выиграть. Однако у тактической слежки есть преимущество – частично ее можно регулировать, чтобы она вредила наименьшему числу людей. Когда тактическая слежка используется в правоохранительных целях (в противовес разведке), она часто нужна для сбора доказательств. Доказательства в конце концов предъявляются суду, то есть информация обнародуется. Пусть не всегда, но какой-то надзор за такой слежкой есть. Тех, кто ее осуществляет, вызывают в качестве свидетелей, и можно расспросить их о том, как именно они собирали информацию и почему мы должны ей верить. Тут процесс подконтролен. А вот регулирование стратегического перехвата информации абсолютно абсурдно. Это по определению слежка за всеми и каждым, и о каком законе можно говорить, если мы с самого начала перехватываем всю доступную информацию?

ЖЕРЕМИ: Я слушал ваш спор о том, нужно ли обнародовать все собранные кем-то данные, и вспомнил о группе LulzSec, выложившей в Сеть 70 миллионов записей с сайта Sony – данные всех пользователей Sony, – с адресами, имейлами и паролями. Кажется, там были и номера кредитных карточек 70 миллионов человек. Как убежденный правозащитник, я думал: «Вау, что-то здесь не то, если для доказательства своей точки зрения или просто для удовольствия вы выкладываете личные данные». Мне было очень неловко смотреть на имейлы в открытом доступе. Думаю, эти люди забавлялись с компьютерной безопасностью и хотели продемонстрировать, что такая известная и мощная компания, как Sony, не в состоянии хранить чьи-либо личные данные в секрете, и когда 70 миллионов пользователей задают поиск по своим имейлам или именам и натыкаются на эту запись, они сразу задаются вопросом: «Ох, что же я наделал, передав свои данные Sony? Чем я рискую, доверяя личные данные какой-то компании?»

ДЖЕЙКОБ: И стреляют в того, кто принес им эту весть.

Крысы в опере

ДЖУЛИАН: Мы обговорили все пессимистические сценарии, и теперь я хочу обсудить потенциальный сценарий, при котором все будет очень хорошо. Сетевая молодежь становится все более радикальной, а сегодня это бóльшая часть молодежи мира. С другой стороны, мы наблюдаем за отчаянными попытками анонимизации, за борьбой за свободу публикации контента, свободу от цензуры, которую проталкивает широкий спектр госструктур и взаимодействующих с ними частных компаний. Предположим, что ход событий окажется наиболее благоприятным. Что нас тогда ждет?

ДЖЕЙКОБ: Думаю, нам нужно право читать и говорить свободно, без каких бы то ни было исключений, без исключений для любых людей на планете, без исключений вообще, если перефразировать Билла Хикса [129] . Он имел в виду образование, одежду и еду, но к этой формуле можно свести и то, о чем идет речь и у нас: право читать и говорить свободно есть у каждого из нас. Отсюда – право на анонимное высказывание, возможность переводить деньги без вмешательства третьих лиц, возможность свободно путешествовать, возможность исправлять личные данные в информационных системах. Любые инфосистемы должны быть прозрачны и подконтрольны пользователям.

ЭНДИ: Я бы добавил: по мере появления новых способов обработки данных в Сети и с учетом доступности криптографии, сервисов вроде Tor и т. д. объем информации, которую можно запретить, становится все меньше, и власти это понимают. Они осознают, что сегодня действовать втайне получится только на протяжении какого-то времени, что рано или поздно правда выйдет наружу, – и очень хорошо, что они отдают себе отчет. Методы властей

меняются. Они понимают: их действия однажды подвергнутся оценке. Это означает также, что власти будут расширять практику информаторства. Скажем, закон Сарбейнса–Оксли требует от компаний, зарегистрированных на биржах США, создавать инфраструктуры для информаторов, чтобы люди, которые хотят сообщить о преступлениях начальства, имели такую возможность и не подвергались преследованиям со стороны тех, на кого донесли [130] . Хорошо, что власть понимает, что происходит, – в долгосрочном плане это добавит процессу стабильности.

ЖЕРЕМИ: Дополняя Джейка, скажу, что мы должны донести до всех и каждого: свободный, открытый и универсальный интернет – это, вероятно, важнейшее средство решения глобальных проблем, а защита Сети – одна из основных задач, стоящих перед нашим поколением, и когда кто-то где-то – государство ли, частная ли компания – ограничивает право группы людей на доступ к интернету во всей его полноте, страдает в целом интернет. Тем самым ограничивается человечество. Как мы видим, наши коллективные действия увеличивают политическую цену такого рода решений, а значит, все люди со свободным доступом в интернет могут им противостоять. Мы начинаем понимать, что граждане Сети обладают весом при решении политических вопросов, что мы способны заставить наших избранных представителей и наши правительства отчитываться перед нами за неверные решения, влияющие на наши фундаментальные права и на свободную Глобальную сеть. И я уверен, что нам нельзя сидеть сложа руки. Следует и дальше делиться знаниями о том, как бороться за свои права. Совершенствовать наши методы, рассказывать о способах влияния на парламент, разоблачать политиков, вскрывать то, как промышленные лобби воздействуют на процесс принятия решений. Нам следует и дальше создавать сервисы, позволяющие гражданам более эффективно развивать децентрализованную зашифрованную инфраструктуру, и обладать собственной инфраструктурой коммуникации. Нам следует пропагандировать наши идеи, чтобы построить мир лучше прежнего. Мы уже начинаем это делать – и нам не следует останавливаться.

ДЖУЛИАН: Джейк, если прочесть описание проблем интернета, например, в книге Евгения Морозова, окажется, что шифропанки предвещали эти проблемы давным-давно [131] . Мы ни в коем случае не ограничивались нытьем по поводу расцветающей слежки и т. п.; мы знали, что способны, а на деле – должны готовить инструменты для новой демократии. Мы можем создавать их собственным умом, распространять среди других людей и организовывать коллективную оборону. Технология и наука не нейтральны. Некоторые формы технологии дают нам фундаментальные права и свободы, о каких многие мечтали так долго.

ДЖЕЙКОБ: Именно так. Думаю, главное, что мы должны донести до людей, – особенно до подростков 16–18 лет, желающих изменить мир, – это то, что никто из сидящих здесь и вообще никто в мире не рождается с достижениями, о которых потом пишут на могильных плитах. Все мы создаем альтернативы реальности. Каждый из нас в этой комнате создавал такие альтернативы – и любой человек, особенно с интернетом, имеет право делать то же самое в своем контексте. Не то чтобы люди были обязаны преобразовывать мир, но если они хотят – это в их власти. Меняя реальность, они тем самым воздействуют на жизни множества людей, что особенно верно в интернете. Сеть усиливает альтернативы и аккумулирует их.

ДЖУЛИАН: То есть, создав что-то, ты можешь подарить это миллиардам пользователей.

ДЖЕЙКОБ: Участвуя в разработке анонимной сети – вроде того же проекта Tor, – ты помогаешь создавать альтернативу анонимной коммуникации, ранее не существовавшей.

ЖЕРЕМИ: Ты свободно делишься знаниями и создаешь коммуникационные каналы, по которым знания распространяются беспрепятственно. Tor, бесплатная и открытая программа, столь популярна именно потому, что свобода заложена в ней на базовом уровне. Мы создаем заведомо свободные альтернативы, технологии и модели.

ДЖЕЙКОБ: Свободному миру требуется свободное программное обеспечение, а еще

нам нужно свободное и открытое аппаратное обеспечение.

ДЖУЛИАН: Свободное ПО – то есть программы с открытым исходным кодом, позволяющим их переделывать и смотреть, как они работают?

ДЖЕЙКОБ: Именно. Нам нужно ПО, которое открыто в той же мере, в какой при демократии открыты законы, – чтобы каждый мог изучить программу, изменить ее, понять, как она работает, и убедиться: да, она делает именно то, что должна. Свободное программное обеспечение, свободное и открытое аппаратное обеспечение [132] .

ДЖУЛИАН: Как говорили шифропанки, код – это закон.

ЖЕРЕМИ: Это слова Ларри Лессига.

ДЖУЛИАН: В интернете все, что вы делаете, определяется существующими и функционирующими программами, потому код – это закон.

ДЖЕЙКОБ: Именно, и, следовательно, можно создавать альтернативы, особенно в части программного обеспечения, но еще и в части 3D-принтеров или сообществ вроде существующих хакспейсов – тоже [133] . Ты можешь содействовать созданию альтернатив, и самое главное тут – убедить людей в нормальности этого процесса, чтобы они социально привыкли создавать свои трехмерные объекты, модифицировать свое программное обеспечение, чтобы они знали: если кто-то – кто бы он ни был – запрещает все это делать, он не предоставляет доступ в интернет – он заманивает клиентов в «фильтрнет», в «цензорнет» и не заботится о них так, как должен. Каждый из нас живет ради свободного будущего, и люди должны знать, что они могут внести свой вклад в лучший мир для грядущих поколений, да и для нашего тоже. Вот почему я здесь: если я не поддержу Джулиана сейчас, не помогу ему выстоять, какой лучший мир я создам? Какой знак я подам, если позволю помыкать собой стаду свиней? Никогда и ни за что! Мы обязаны строить новый мир, мы обязаны преобразовывать существующий. Как говорил Ганди: «Если хочешь что-то изменить, ты должен измениться сам», – и если ты желаешь, чтобы машина дала сбой, ты должен стать сбоем [134] . Я процитировал веб-комикс A Softer World, а не совсем то, что сказал Ганди, но, я думаю, люди должны осознать, что нельзя сидеть и ничего не делать, что нужно действовать, – и, хочется надеяться, они это поймут [135] .

ЭНДИ: Полагаю, у нас есть все шансы увидеть, как кто-то примет от нас эстафету и отправится дальше. Альтернативы создаются теми, кто не удовлетворен нынешней ситуацией или предлагаемым выбором.

ДЖУЛИАН: Расскажи в этом контексте о компьютерном клубе Chaos.

ЭНДИ: Опять Chaos… фнорд! [136]

ДЖУЛИАН: Другого такого в мире нет.

ЭНДИ: Компьютерный клуб Chaos – это галактическая хакерская организация, пропагандирующая свободу информации и прозрачность технологии. Наша цель – свести людей и технический прогресс, чтобы общество и технология взаимодействовали друг с другом.

ДЖУЛИАН: При этом вы вторгаетесь в политику.

ЭНДИ: Chaos стал площадкой для хакерских дискуссий, в которых участвуют несколько тысяч членов клуба, часть из них – немцы, но мы не считаем, что живем в Германии, мы считаем, что живем в Сети, и, может быть, такое мировоззрение тоже привлекает людей. Мы отлично ладим с хакерскими группами во Франции, Америке и других странах.

ДЖУЛИАН: Как ты думаешь, почему Chaos появился именно в Германии? Там его сердце, оттуда он распространился по всему свету.

ЭНДИ: Немцы всегда пытаются структурировать реальность.

ЖЕРЕМИ: Немецкие инженеры – лучшие.

ДЖУЛИАН: Я думаю, тут есть еще кое-что. Берлин, падение Восточной Германии.

ЭНДИ: Тут есть много всякого. Германия поступила с другими странами так ужасно, как никто до нее, и, возможно, мы чуть лучше защищены от таких вещей, как милитаристские настроения. Мы через них прошли, мы развязали войну, нас очень сильно

наказали, мы вынесли из этого урок, так что сегодня в немецких школах учат децентрализованному мышлению и антифашистскому поведению, учат тому, как противостоять созданию тоталитарного государства, – ведь мы его уже создавали, причем наихудшее в истории. Отчасти поэтому можно сказать, что Chaos – немецкий феномен. Вау Холланд, отец-основатель нашего клуба, тоже был политическим активистом. Я стоял рядом с отцом Вау у его могилы – сын ушел раньше, – и отец не произносил красивых речей. Он сказал: «Чтобы на немецкой земле никто и никогда не создал воинственное тоталитарное государство». Для меня эти слова человека, который хоронил сына, стали ключом к пониманию того, почему Вау старался убеждать других, заботился о них, был миротворцем, делился идеями, а не ограничивал их, действовал неагрессивно и всегда стремился к сотрудничеству. Концепция совместного создания чего-либо – движения за открытый исходный код и т. п. – быстро распространилась по миру и совпала с концепциями американских шифропанков, Джулиана Ассанжа с его WikiLeaks и пр. Теперь это глобальная концепция, швейцарские, немецкие, итальянские хакеры привносят в нее очень разные децентрализованные культурные установки – и это хорошо. Итальянские хакеры ведут себя совсем не так, как немецкие, – куда бы итальянцы ни приехали, они повсюду готовят вкусную пищу, а немцам нужно, чтобы все было разложено по полочкам. Я не говорю, что кто-то лучше, а кто-то хуже, я лишь хочу сказать, что у каждой децентрализованной культуры есть свои прекрасные аспекты. На итальянской конференции ты идешь на кухню и попадаешь в рай; в немецком хакерском лагере у тебя есть чудесный интернет, а на кухню лучше не смотреть. Но все мы так или иначе создаем что-то. И, я думаю, нас объединяет какое-то общее сознание, не имеющее никакого отношения к национальной идентичности – не важно, немец ты, итальянец или американец, – мы все хотим решать проблемы, мы хотим работать сообща. Мы рассматриваем цензуру в интернете и войну, объявленную властью новой технологии, как некие эволюционные трудности, которые нам надо преодолеть.

Мы на пути к пониманию того, как решать проблемы, а не просто их выявлять, и это не может не радовать. Вероятно, нам придется сражаться со всякой ерундой не знаю сколько еще лет, но в конце концов придет поколение политиков, для которого Сеть не будет врагом, и оно поймет, что это не проблема, а часть решения проблемы. Наш мир по-прежнему зиждется на оружии, на власти секретов, на соответствующем экономическом базисе, однако ситуация меняется, и я уверен, что мы сегодня – важный фактор в процессе принятия политических решений. Мы обсуждаем различные темы с самых разных сторон – собственно, именно этим давно и успешно занимается Chaos. Мы не однородная группа, в клубе есть люди с самыми разными взглядами. По-моему, здорово то, что мы сейчас собрались и не можем сразу дать ответы – мы только ставим вопросы, бомбардируем друг друга разными идеями и смотрим на итог. Такое обсуждение должно продолжаться, и для этого нам нужен свободный интернет.

ДЖУЛИАН: Я спросил о том, что нас ждет при наиболее благоприятном варианте развития событий. Самопознание, разнообразие и сети свободного волеизъявления. Высокообразованные люди по всему земному шару – я имею в виду не формальное образование, а понимание того, как функционирует наша цивилизация на политическом, промышленном, научном и психологическом уровне, – как результат свободного коммуникационного обмена, стимулирующего новые живые культуры и максимальную диверсификацию индивидуальной мысли, более эффективного волеизъявления регионов, волеизъявления групп по интересам, способных быстро образовывать сети и обмениваться ценностями, невзирая на географические границы. Возможно, именно это мы видели во время «арабской весны» – панарабские активисты объединялись через интернет. Когда мы работали с сайтом Nawaat.org, создавшим Tunileaks, который в обход цензуры дореволюционного Туниса публиковал переписку местного МИДа, я напрямую ощущал фантастическую силу Сети, доставлявшей информацию туда, где она была нужна, и эта работа себя оправдала – благодаря в том числе нашим усилиям в Тунисе началась революция [137] . Я думаю, что борьба за свободное волеизъявление неотделима от нашей борьбы. При

благоприятном сценарии наша цивилизация начнет познавать саму себя, потому что прошлое не может быть уничтожено. А значит, новые тоталитарные государства не возникнут – им станут препятствовать свободное движение информации, возможность общаться приватно и сговариваться против тоталитарных тенденций, а также способность микрокапитала бесконтрольно уходить из государств, негостеприимных к людям.

С подобными предпосылками можно создать самые разные политические системы. Если бы Утопия существовала, для меня она была бы антиутопией. Я считаю, что настоящие идеалы утопии – это прежде всего разнообразие систем и моделей взаимодействия. Посмотрите на бурное развитие новых культурных продуктов, на то, как меняется язык, как субкультуры формируют не существовавшие ранее механизмы взаимодействия, невозможные без Сети, – и вы поймете, что интернет действительно открывает нам новое будущее.

Вместе с тем я вижу очень сильные тенденции к однородности и универсальности, к тому, что вся наша цивилизация превратится в один большой рынок, где действуют нормальные для рынка факторы и в разрезе каждого сервиса и продукта есть лидер, второй и третий по значимости игроки, а также аутсайдеры, которые никак не влияют на ситуацию. Возможно, нас ждут массовая гомогенизация языка, массовая гомогенизация культуры и массовая стандартизация, благодаря чему быстрый обмен информацией станет еще более эффективным. Боюсь, пессимистический сценарий тоже весьма вероятен, между тем уже сегодня мы живем в мире транснациональной слежки и бесконечных войн дронов.

Я вспомнил о том, как тайком пробрался в Сиднейскую оперу, чтобы послушать «Фауста». Сиднейская опера в темноте необычайно красива, это величественное, ярко освещенное здание, восстающее из воды и возносящееся в ночное небо. После представления я вышел на улицу и увидел трех женщин, которые разговаривали у парапета перед потемневшим заливом. Та, что постарше, говорила о проблемах с работой – а работала она, как выяснилось, агентом ЦРУ, – о том, как жаловалась в особый комитет Сената по разведке и т. д., и все это она излагала тихим голосом своей племяннице и еще одной женщине. Я подумал: «Ух ты! Агенты ЦРУ и правда ходят развлекаться в Сиднейскую оперу!» Потом я заглянул через массивные стеклянные панели в фойе – и вдруг увидел среди роскошества и великолепия водяную крысу, которая бежала по полу, то и дело останавливалась, запрыгивала на столы, покрытые изящными скатертями, лакомилась любыми яствами, прыгала на стойку с билетами и вообще развлекалась как могла. Я понял, что это и есть самый вероятный сценарий будущего: ограничивающая, однородная, постмодернистская транснациональная тоталитарная структура невероятной сложности, полная абсурда, девальвирующая всё и вся, а внутри этой невероятной сложности – пространство, по которому могут перемещаться только умные крысы.

Таков положительный аспект неблагоприятного развития событий. Мы идем к транснациональному государству тотальной слежки, вооруженному дронами, с сетевым неофеодализмом транснациональной элиты. Это будет не элита в классическом смысле слова, а сложное многостороннее взаимодействие, в которое выльется общение и смешение разнообразных национальных элит. Вся коммуникация окажется под контролем, ее станут непрерывно отслеживать и записывать, в процессе слежки каждый человек будет идентифицирован, и новый истеблишмент получит о вас полную информацию – от вашего рождения до вашей смерти. Десять лет назад все это казалось невозможным, а сегодня тотальная слежка – почти реальность. В результате нас ждет мир всеобщего контроля. Если бы вся собранная информация была обнародована, глобальная цивилизация смогла бы поколебать систему и сама решила бы, каким путем ей идти. Но без существенных перемен этого не произойдет. За большинством так или иначе следят, и власть внутри этой схемы принадлежит избранным, которые, я подозреваю, тоже обрадуются дивному новому миру. Одним из элементов системы станет гонка армий дронов, которые уничтожат четкие границы между странами – эти границы сложились в результате борьбы за физические элементы ландшафта, а дроны преодолеют их и начнут бесконечную войну, когда

борющиеся за влияние сети станут трясти мир, требуя от врагов уступок. На этом фоне людей буквально похоронит под собой невозможная бюрократическая математика.

Как нормальный человек может быть свободным внутри такой системы? Ответ очень прост: никак. Это нереально. Конечно, внутри любой системы существуют те или иные ограничения, но в грядущем все те свободы, которые мы получили в ходе биологической эволюции и культурной адаптации, будут полностью уничтожены.

Думаю, единственными, кто сохранит свободу, которой человечество обладало, скажем, двадцать лет назад – а тотальная слежка уничтожила почти всю нашу свободу, только мы этого пока не осознали, – будут высокообразованные элементы системы. Свободной останется только взбунтовавшаяся элита, разбирающаяся в технологиях. Умные крысы, бегающие по зданию оперы.

Примечания

1

Говоря по-простому, криптография (с *греч.* «тайное письмо») – это практика зашифрованной коммуникации.

2

Oxford English Dictionary Updates Some Entries & Adds New Words; Bada-Bing, Cypherpunk, and Wi-Fi Now in the OED, ResourceShelf, 16 сентября 2006 года: http://web.resourceshelf.com/go/resourceblog/43743 (проверено 24 октября 2012 года).

3

Проект WikiLeaks: http://wikileaks.org.

4

Подробнее о rubberhose см. «The Idiot Savants' Guide to Rubberhose» Сьюлетт Дрейфус: http://marutukku.org/current/src/doc/maruguide/t1.html (проверено 14 октября 2012 года).

5

Подробнее о книге «Компьютерное подполье» см.: http://www.underground-book.net.

Подробнее о фильме «Подполье: история Джулиана Ассанжа» см. Internet Movie Database: http://www.imdb.com/title/tt2357453/ (проверено 21 октября 2012 года).

6

Хакспейс, или хакерспейс, – место, где собираются люди с общими интересами к интернету и компьютерным технологиям. – *Прим. пер* .

7

Noisebridge – хакспейс в Сан-Франциско, обеспечивающий инфраструктуру для техническо-творческих проектов и управляемый совместно всеми членами: https://www.noisebridge.net/wiki/Noisebridge. Компьютерный клуб Chaos Berlin – берлинский филиал компьютерного клуба Chaos (см. ниже): https://berlin.ccc.de/wiki/Chaos_Computer_Club_Berlin.

8

Проект Tor: https://www.torproject.org.

9

Компьютерный клуб Chaos – крупнейшая хакерская ассоциация Европы. Ее деятельность варьируется от технических исследований до кампаний, мероприятий, публикаций и политических консультаций. Сайт компьютерного клуба Chaos: http://www.ccc.de.

10

EDRi: http://www.edri.org.

11

ICANN: http://www.icann.org.

12

buggedplanet: http://buggedplanet.info.

13

Cryptophone: http://www.cryptophone.de.

14

La Quadrature du Net: http://www.laquadrature.net.

15

«Сопутствующее убийство»: http://www.collateralmurder.com. Логи войны в Ираке: http://wikileaks.org/irq. «Дневник войны в Афганистане»: http://wikileaks.org/afg. «Кабельгейт»: http://wikileaks.org/cablegate.html.

16

Congressional committee holds hearing on national security leak prevention and punishment, Reporters Committee for Freedom of the Press, 11 июля 2012 года: http://www.rcfp.org/browse-media-law-resources/news/congressional-committee-holds-hearing-national-security-leak-prevent (проверено 21 октября 2012 года).

17

Подробнее о Большом жюри по WikiLeaks см. хронологию событий, описанную журналистом-фрилансером Алексой О'Брайен: http://www.alexaobrien.com/timeline_us_versus_manning_assange_wikileaks_2012.html (проверено 22 октября 2012 года).

18

Bradley Manning's treatment was cruel and inhuman, UN torture chief rules, Guardian, 12 марта 2012 года: http://www.guardian.co.uk/world/2012/mar/12/bradley-manning-cruel-inhuman-treatment-un (проверено 24 октября 2012 года).

19

WikiLeaks: guilty parties "should face death penalty", Telegraph, 1 декабря 2010 года: http://www.telegraph.co.uk/news/worldnews/wikileaks/8172916/WikiLeaks-guilty-parties-should-face-death-penalty.html (проверено 22 октября 2012 года).

20

CIA launches task force to assess impact of U.S. cables' exposure by WikiLeaks, Washington Post, 22 декабря 2010 года: http://www.washingtonpost.com/wp-dyn/content/article/2010/12/21/AR2010122104599.html?hpid=topnews&sid=ST2010122105304 (проверено 22 октября 2012 года).

21

WikiLeaks fights to stay online after US company withdraws domain name, Guardian, 3 декабря 2012 года: http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns (проверено 23 октября 2012 года).

22

Don't Look, Don't Read: Government Warns Its Workers Away From WikiLeaks Documents, New York Times, 4 декабря 2010 года: http://www.nytimes.com/2010/12/05/world/05restrict.html?hp&_r=2& (проверено 23 октября 2012 года).

23

Banking Blockade, WikiLeaks: http://www.wikileaks.org/Banking-Blockade.html (проверено 22 октября 2012 года).

24

Советуем прочесть описание самого Джейкоба: «Air Space – a trip through an airport detention center», boingboing, 31 октября 2011 года: http://boingboing.net/2011/10/31/air-space-a-tripthrough-an-ai.html. Рекомендуем также интервью с Джейкобом на сайте Democracy Now. National Security Agency Whistleblower William Binney on Growing State Surveillance, Democracy Now, 20 апреля 2012 года: http://www.democracynow.org/2012/4/20/exclusive_national_security_agency_whistleblower_william (обе ссылки проверены 23 октября 2012 года).

25

Официальное название дела – In the Matter of the 2703 (d) Order Relating to Twitter Accounts: Wikileaks Rop_G IOERROR; and BirgittaJ.

26

Secret orders target email, Wall Street Journal, 9 октября 2011 года: http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html (проверено 22 октября 2012 года).

27

Twitter Ordered to Yield Data in WikiLeaks Case, New York Times, 10 ноября 2011 года: https://www.nytimes.com/2011/11/11/technology/twitter-ordered-to-yield-data-in-wikileaks-case.html?_r=1 (проверено 22 октября 2012 года).

28

ACLU & EFF to Appeal Secrecy Ruling in Twitter/WikiLeaks Case, пресс-релиз Фонда электронных рубежей, 20 января 2012 года: https://www.eff.org/press/releases/aclu-eff-appeal-secrecy-ruling-twitterwikileaks-case (проверено 22 октября 2012 года).

29

Речь идет об акции протеста в поддержку подавленной забастовки текстильных рабочих города Махалла-эль-Кубра. Незадолго до забастовки в Facebook сформировалась группа «Молодежное движение 6 апреля» с целью призвать египтян поддержать забастовку в Махалле акциями протеста в Каире и других городах. Группе не удалось добиться желаемого, ее члены, в том числе администраторы Эзраа Абдель Фатта Ахмед Рашид и Ахмед Махер, были арестованы. Махера пытали, требуя выдать пароль от страницы на Facebook. «Молодежное движение 6 апреля» сыграло свою роль в египетской революции 2011 года. См. «Cairo Activists Use Facebook to Rattle Regime», Wired, 20 октября 2008 года: http://www.wired.com/techbiz/startups/magazine/1611/ff_facebookegypt?current-Page=all (проверено 23 октября 2012 года).

30

Брошюра «Как протестовать по-умному» анонимных авторов распространялась на начальном этапе 18-дневного восстания, которое свергло президента Мубарака. На арабском языке: http://www.itstime.it/Approfondimenti/EgyptianRevolutionManual.pdf. Отрывки переведены на английский и опубликованы, см. «Egyptian Activists' Action Plan: Translated», Atlantic, 27 января 2011 года: http://www.theatlantic.com/international/archive/2011/01/egyptianactivists-action-plan-translated/70388 (обе ссылки проверены 23 октября 2012 года).

31

Паноптикон – тюрьма, придуманная в 1878 году философом Иеремией Бентамом. В такой тюрьме один охранник может тайно следить за всеми заключенными сразу. См. Иеремия Бентам (под редакцией Миран Бозовиц) «The Panopticon Writings» (Verso, 1995), доступно в Сети: http://cartome.org/panopticon2.htm (проверено 22 октября 2012 года).

32

Иоганн Гутенберг (1398–1468) – немецкий кузнец, изобретатель механического передвижного печатного станка, положившего начало одному из самых значительных социальных потрясений в истории. Изобретение печатного станка – ближайшая историческая аналогия созданию интернета.

33

Джон Гилмор – один из первых шифропанков, основатель Фонда электронных рубежей и гражданский активист. Фраза, которую цитирует Энди, впервые появилась в статье «First Nation in Cyberspace», Time Magazine, 6 декабря 1993 года. См. сайт Джона Гилмора: http://www.toad.com/gnu (проверено 22 октября 2012 года).

34

«Оригинальные технологии – это любые типы систем, инструментов или технических процессов, которые разработаны данной компанией для себя самой… Идеи, которые развили

или подали работники компании, обычно считаются интеллектуальной собственностью работодателя, позволяя тому называть технологию оригинальной». Определение взято с сайта wiseGEEK: http://www.wisegeek.com/what-is-proprietary-technology.htm (проверено 22 октября 2012 года).

35

Кори Доктороу «The coming war on general-purpose computing», boingboing, 10 января 2012 года (на основе доклада, сделанного на компьютерном конгрессе Chaos в декабре 2011 года): http://boingboing.net/2012/01/10/lockdown.html (проверено 15 октября 2012 года).

36

Stuxnet – чрезвычайно хитроумный компьютерный червь, разработанный, согласно популярной версии, США и Израилем для нападения на компьютеры Siemens, предположительно использовавшиеся Ираном для обогащения урана. Общую информацию см. в Wikipedia: http://en.wikipedia.org/wiki/Stuxnet. См. также «WikiLeaks: US advised to sabotage Iran nuclear sites by German thinktank», Guardian, 18 января 2011 года: http://www.guardian.co.uk/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear. Проект WikiLeaks обнародовал один из первых отчетов о последствиях аварии на заводе по обогащению урана в Нетензе в результате, как считается сегодня, запуска в систему вируса Stuxnet. См. «Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation», WikiLeaks, 17 июля 2009 года: http://wikileaks.org/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief%27s_mystery_resignation. Данные специализирующейся на международной разведке компании Stratfor, обнародованные WikiLeaks, заставляют предположить участие Израиля. См. Email ID 185945, The Global Intelligence Files: http://wikileaks.org/gifiles/docs/185945_re-alpha-s3-g3-israel-iran-barak-hails-munitions-blast-in.html (все ссылки проверены 16 октября 2012 года).

37

Пентест (от *англ* . penetration testing, «тестирование на проникновение») – термин из техники обеспечения безопасности. В ходе теста производится санкционированная атака на компьютерную систему или сеть, позволяющая оценить, насколько последние безопасны. Специалистов, которые проводят пентесты, часто набирают из хакерского сообщества.

38

«Захват флага» – изначально уличная игра, в которой обычно участвуют две команды: каждая занимает некую территорию и охраняет свой флаг. Цель – заполучить флаг противника и вернуться на свою территорию. На хакерских конференциях принято играть в компьютерную версию этой игры: команды атакуют и защищают компьютеры и сети.

39

Кубок сисадмина (сисадмин, системный администратор – это IT-специалист, поддерживающий работу компьютерной системы или сети) – Джейкоб имеет в виду, что задача наводила его на мысль о турнире системных администраторов.

40

Ты можешь так говорить, потому что ты немец (*нем* .).

41

Aaron says encryption protects privacy, commerce, USIS Washington File, 13 октября 1998 года: http://www.fas.org/irp/news/1998/10/98101306_clt.html (проверено 21 октября 2012 года).

42

Сайт Вассенарских соглашений: http://www.wassenaar.org (проверено 21 октября 2012 года).

43

Энди говорит о различных событиях «первых криптовойн» 1990-х годов. Когда активисты шифропанка стали распространять сервисы с сильной криптографией в качестве бесплатного программного обеспечения, правительство США начало препятствовать эффективному использованию последних. Оно приравняло криптографию к вооружениям и

запретило ее экспорт; оно попыталось вывести на рынок конкурирующие, заведомо дефектные технологии, позволявшие правоохранительным органам дешифровать любую информацию; оно также попыталось реализовать весьма спорную схему «депонирования ключей». В начале 2000-х годов на протяжении недолгого времени считалось, что попытка бороться с криптографией потерпела фиаско. Однако сейчас разворачивается «вторая криптовойна» – используя и законы, и технологии, власти пытаются обойти или маргинализовать использование криптографии.

44

Такие же расчеты были проделаны для обнародованных 196,4 миллиарда минут звонков по наземной сети Германии за 2010 год, оцифрованных голосовым кодеком с качеством 8 Кбит/с, в сумме – 11 784 петабайт, округленно с запасом – 15 петабайт. Учитывая, что стоимость хранения одного петабайта составляет около 500 тысяч долларов США, мы получим 7,5 миллиона долларов, или 6 миллионов евро. Добавим расходы на приличное оборудование дата-центра, вычислительные мощности, соединения и фонд заработной платы. Даже если включить в расчет еще 101 миллиард минут звонков по мобильной сети Германии за 2010 год, что составляет еще 50 петабайт и 18,3 миллиона евро, хранение этих данных будет стоить меньше, чем один военный самолет вроде Eurofighter (90 миллионов евро) или F22 (150 миллионов долларов).

45

Подробнее о VASTech см. на сайте buggedplanet: http://buggedplanet.info/index.php?title=VASTECH (проверено 21 октября 2012 года).

46

Дело о несанкционированной слежке АНБ, рассматривавшееся в суде на территории США, – самый значительный скандал с массовой слежкой в истории Соединенных Штатов. Американский закон о слежке за иностранной разведкой 1978 года (FISA, Foreign Intelligence Surveillance Act 1978, FISA) запрещал госучреждениям шпионить за гражданами США без санкции суда. После событий 11 сентября АНБ стало в массовом порядке нарушать FISA, получив на это секретное распоряжение президента Джорджа Буша. Администрация Буша утверждала, что отдать распоряжение позволило чрезвычайное законодательство, принятое Конгрессом в 2001 году, – разрешение на применение вооруженных сил (The Authorization for the Use of Military Force, AUMF) и патриотический закон. Программа АНБ по несанкционированной слежке на территории США – включая взаимодействие с частными компаниями, в числе которых и AT&T, – оставалась секретной до 2005 года, когда ее разоблачила газета New York Times. См. «Bush Lets U. S. Spy on Callers Without Courts», New York Times, 16 декабря 2005 года, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

Журналисты New York Times узнали о несанкционированной программе слежения АНБ от анонимного информатора. В 2004 году тогдашний ответственный издатель газеты Билл Келлер согласился с требованием администрации Буша не предавать эту информацию огласке в течение года, пока Буш не будет переизбран на новый срок. Однако в 2005 году New York Times поспешила опубликовать материал, когда узнала о том, что власти пытаются получить судебное решение о предварительном запрете на публикацию, как это было в истории с «документами Пентагона».

Администрация Буша отрицала тот факт, что программа АНБ незаконна. Министерство юстиции сразу же стало искать источник утечки информации, бросив на дело 25 федеральных агентов и пять прокуроров. Руководство Республиканской партии призвало наказать New York Times по закону о шпионаже.

После того как New York Times опубликовала материал, на контакт с прессой вышли другие информаторы, и постепенно стала вырисовываться подробная картина беззакония и бесполезной траты средств вследствие решений, принятых на высшем уровне АНБ. Адвокатские группы вроде Американского союза защиты гражданских свобод (АСЗГС) и Фонда электронных рубежей (ФЭР) подали ряд групповых исков. В одном из этих дел,

«АСЗГС против АНБ», суд отказал в удовлетворении иска, поскольку истцы не смогли доказать, что слежка осуществлялась за ними персонально. В другом, «Hepting против AT&T», информатор из AT&T Марк Клейн дал под присягой письменные показания и тем самым разоблачил сотрудничество AT&T с программой слежки. См. раздел «Hepting v. AT&T» на сайте ФЭР: https://www.eff.org/cases/hepting.

Марк Клейн проходил по делу «Хептинг против AT&T» свидетелем. В письменных показаниях бывшего работника AT&T из Фолсома, Сан-Франциско, утверждалось, что существует «комната 641A» – объект, на котором корпорация осуществляет стратегический перехват телефонных звонков для АНБ. На объекте имеется доступ к оптоволоконным магистралям, что позволяет отслеживать весь интернет-трафик, проходящий через здание, как иностранный, так и американский. По оценке информатора из АНБ Уильяма Бинни, таких объектов существует по меньшей мере два десятка, и все они размещены в ключевых узлах телекоммуникационной сети Соединенных Штатов.

Клейн сообщил важные сведения о характере программы слежки, подтвержденные информаторами из АНБ. Это пример «стратегического перехвата информации» – весь сетевой трафик, проходящий через США, копируется и хранится неограниченное время. Можно с уверенностью сказать, что весь внутриамериканский трафик также перехватывается и хранится, поскольку с технологической точки зрения при таком объеме данных невозможно отфильтровать ту их часть, для которой необходима санкция по FISA. Нынешнее официальное юридическое толкование этого закона гласит, что перехват имеет место, когда сотрудники АНБ получают доступ к сохраненному в базе данных внутриамериканскому трафику – только на этом этапе необходима санкция суда. Граждане США должны сделать вывод, что весь их телекоммуникационный трафик (включая телефонные звонки, SMS, электронные письма и информацию, просматриваемую через браузер) отслеживается и навечно сохраняется в дата-центрах АНБ.

В 2008 году в ответ на большое количество исков, поданных по следам скандала с прослушкой, Конгресс США принял поправки к закону FISA 1978 года, немедленно подписанные президентом. Они позволяют тем, кто виновен в нарушении FISA, воспользоваться весьма спорной «неподсудностью, имеющей обратную силу». Сенатор Барак Обама во время своей президентской кампании сделал «прозрачность» частью предвыборной платформы и пообещал информаторам защиту, но после того как в 2009 году Обама возглавил администрацию, Министерство юстиции продолжило политику Буша, в итоге AT&T воспользовалось «имеющей обратную силу неподсудностью» в деле Hepting и других.

Министерству юстиции не удалось обнаружить человека, снабдившего информацией газету New York Times, однако оно изобличило информаторов, появившихся после публикации этого материала. Один из них, Томас Дрейк, бывший руководитель высшего ранга из АНБ, много лет жаловался в комитет Конгресса по контролю над разведывательной деятельностью на коррупцию и бесполезную трату средств в программе АНБ «Следопыт». Внутренним жалобам так и не дали хода; все правительственные чиновники, желавшие что-либо сделать, ничего не добились. После статьи в New York Times Дрейк рассказал о программе «Следопыт» газете Baltimore Sun. Большое жюри предало Дрейка суду, назвало его «врагом государства» и обвинило в нарушении закона о шпионаже. См. The Secret Sharer, New Yorker, 23 мая 2011 года: http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?currentPage=all.

В июне 2011 года на дело Томаса Дрейка обратила пристальное внимание общественность, и оно развалилось. После неудачных попыток принудить обвиняемого к сделке и признанию вины Министерство юстиции смирилось с тем, что суд признал Дрейка виновным в части единственного мелкого проступка. Дрейк был осужден на один год условно.

Шлейф скандала со слежкой АНБ тянется до сегодняшнего дня. АСЗГС оспаривает конституционность принятых в 2008 году поправок к FISA в деле «Amnesty и другие против

Клэппер». См. FISA Amendment Act Challenge, ACLU, 24 сентября 2012 года: http://www.aclu.org/national-security/amnesty-et-al-v-clapper.

В деле «Джуэл против АНБ» ФЭР пытался положить конец несанкционированной слежке АНБ. В 2009 году дело было прекращено, после того как администрация Обамы объявила агентство неподсудным в силу сохранения государственной тайны. См. сайт ФЭР о деле «Джуэл против АНБ»: https://www.eff.org/cases/jewel. Тем не менее в декабре 2011 года Девятый окружной апелляционный суд разрешил возобновить дело. Показания по нему дают Томас Дрейк, а также Уильям Бинни и Керк Вибе – информаторы из АНБ. Администрация Обамы, обещавшего сделать государство «прозрачным», обвинила в нарушении закона о шпионаже большее число информаторов, чем предыдущие администрации, вместе взятые. (Все ссылки в этом примечании проверены 23 октября 2012 года.)

47

См. запись о системе Eagle на сайте buggedplanet: http://buggedplanet.info/index.php?title=AMESYS#Strategic_.28.22Massive.22.29_Appliances (проверено 22 октября 2012 года).

48

German court orders stored telecoms data deletion, BBC, 2 марта 2010 года: http://news.bbc.co.uk/1/hi/world/europe/8545772.stm (проверено 15 октября 2012 года).

49

Директива 2006/24/ЕС Европейского парламента и совета требует от стран Европы сохранять данные телекоммуникации граждан от шести месяцев до двух лет. В Германии применение этой директивы в отношении тамошних законов было признано неконституционным. В мае 2012 года Комиссия ЕС передала дело Германии в Европейский суд за неподчинение директиве (см. пресс-релиз Комиссии: http://europa.eu/rapid/press-release_IP-12–530_en.htm (проверено 15 октября 2012 года)).

50

См. Sweden approves wiretapping law, BBC, 19 июня 2008 года: http://news.bbc.co.uk/1/hi/world/europe/7463333.stm. Подробнее о FRA-lagen см. Wikipedia: http://en.wikipedia.org/wiki/FRA_law (обе ссылки проверены 10 октября 2012 года).

51

Метаданные – «данные о данных». В контексте обсуждения термин обозначает информацию, не относящуюся к собственно контенту электронной коммуникации. Это что-то вроде надписи на конверте, а не текст находящегося в нем письма. Отслеживание метаданных затрагивает не содержание электронных сообщений, а всю остальную информацию: кто отправил письмо и кто его получил, IP-адрес (а значит, и физическое место), откуда было послано письмо, время и дата отправки и т. д. Фокус, однако, заключается в том, что технология для перехвата метаданных используется та же самая, что и для перехвата контента. Если вы наделяете кого-то правом следить за вашими метаданными, оборудование будет перехватывать и содержимое коммуникации. Кроме того, большинство людей не понимают, что «метаданные в сумме есть содержание»: если метаданные собрать вместе, они дают фантастически подробную картину чьей-либо коммуникации.

52

Amesys входит в концерн Bull, некогда конкурировавший с Dehomag, филиалом IBM, за право поставлять нацистам системы перфокарт. См.: Эдвин Блэк «IBM and the Holocaust» (Crown Books, 2001). Подробнее о том, как Каддафи шпионил за ливийцами в Великобритании, используя оборудование Amesys, см. Exclusive: How Gaddafi Spied on the Fathers of the New Libya, OWNI.eu, 1 декабря 2011 года: http://owni.eu/2011/12/01/exclusive-how-gaddafi-spied-on-the-fathers-of-the-newlibya (проверено 22 октября 2012 года).

53

Проект WikiLeaks начал выкладывать The Spy Files («Шпионские файлы»), по которым

можно судить о масштабах массовой слежки, в декабре 2011 года. Эти документы находятся по адресу http://wikileaks.org/the-spyfiles.html.

54

Подробнее см. buggedplanet: http://buggedplanet.info/index.php?title=LY.

55

Коммуникационный конгресс Chaos – ежегодное международное собрание хакеров, организуемое одноименным компьютерным клубом.

56

Джейкоб говорит о ZTE, одном из двух китайских производителей (вместе с Huawei) электроники, в которой, как подозревают, есть «черные ходы». Он имеет в виду, что бесплатных пирожных не бывает: «подарок» в виде коммуникационной инфраструктуры предположительно спроектирован так, что работает на китайскую разведку.

57

«Убей свой телевизор» (Kill Your Television) – название движения против массовых коммуникаций, призывающего отказаться от телевидения ради общественной активности.

58

Эффект сети можно наблюдать, когда действие одного человека влияет на вероятность того, что подобное совершат и другие люди.

59

Подробнее о Большом жюри см. заметку «О попытках преследования проекта WikiLeaks и связанных с ним людей» перед обсуждением.

60

Согласно Wall Street Journal: «Как явствует из имеющихся в нашем распоряжении документов, власти США использовали весьма спорную форму секретного судебного ордера, чтобы принудить Google и локального интернет-провайдера Sonic.net выдать данные аккаунтов электронной почты работающего на проект WikiLeaks добровольца Джейкоба Аппельбаума… Ранее в этом году дело WikiLeaks уже стало полигоном для трактовки закона, когда Twitter опротестовал судебный ордер с требованием выдать записи аккаунтов людей, поддерживающих WikiLeaks, включая мистера Аппельбаума… Ордер предписывал сообщить “интернет-протокол”, то есть IP-адреса устройств, с которых люди заходили на свои аккаунты. IP-адрес – это уникальный номер, закрепленный за устройством, соединенным с интернетом. Ордер также предписывал сообщить адреса электронной почты тех, с кем общались упомянутые аккаунты. Содержание ордера запрещалось разглашать, но Twitter успешно отстоял в суде право оповестить подписчиков о том, какая у него затребована информация… Оказавшиеся в наших руках судебные ордера предписывают выдать тот же тип информации, который суд требовал от Twitter. Тайный ордер Google датирован 4 января и предписывает передать властям IP-адрес, с которого мистер Аппельбаум заходил на свой аккаунт на gmail.com, а также имейлы и IP-адреса пользователей, с которыми он общался, начиная с 1 ноября 2009 года. Неясно, опротестовал ли Google ордер или выполнил его требования. Секретный ордер Sonic.net датирован 15 апреля и предписывает выдать ту же информацию об аккаунте мистера Аппельбаума, начиная с 1 ноября 2009 года. 31 августа суд согласился снять запрет на передачу копии ордера мистеру Аппельбауму». Secret orders target email, Wall Street Journal, 9 октября 2011 года: http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html (проверено 11 октября 2012 года). Подробнее см. заметку «О попытках преследования проекта WikiLeaks и связанных с ним людей» перед обсуждением.

61

WikiLeaks demands Google and Facebook unseal US subpoenas, Guardian, 8 января 2011 года: http://www.guardian.co.uk/media/2011/jan/08/wikileaks-calls-google-facebook-us-subpoenas (проверено 16 октября 2012 года). Подробнее см. заметку «О попытках преследования проекта WikiLeaks и связанных с ним людей» перед обсуждением.

62

См. заметку «О попытках преследования проекта WikiLeaks и связанных с ним людей» перед обсуждением.

63

Подробнее см. сайт «Европа против Facebook»: http://www.europe-v-facebook.org/EN/Data_Pool/data_pool.html (проверено 24 октября 2012 года).

64

Повестка национальной безопасности (National Security Letter, NSL) – это письмо от госучреждения США, требующее передать «данные, не связанные с контентом», или «метаданные», такие как записи о финансовых транзакциях, IP-логи или реквизиты имейла. Человек, получивший такой документ, обязан выдать запрошенную информацию, иначе он понесет наказание. Повестка национальной безопасности не требует санкции суда – она может быть послана напрямую федеральным агентством. В этом смысле она похожа на так называемую административную повестку – ордер, предписывающий выдать информацию и требующий только административного, а не судебного надзора. Ввиду этого повестки национальной безопасности могут нарушать четвертую поправку, защищающую граждан США от необоснованных обысков и конфискаций.

NSL также содержат «запрет на разглашение», иначе говоря, сообщить кому-либо о том, что ты получил такую бумагу, – значит совершить уголовное преступление. Ввиду этого повестки национальной безопасности могут нарушать первую поправку, защищающую свободу слова. В деле «Доу против Гонсалеса» запрет на разглашение NSL был признан неконституционным. Поправка к закону наделила получателей повесток национальной безопасности правом оспаривать их в суде, и это решение удовлетворило Второй окружной суд, постановивший, что использование NSL более не является неконституционным. Повестки по-прежнему критикуют защитники гражданских свобод, оспаривают их в судах.

Использование повесток национальной безопасности участилось после принятия в 2001 году патриотического закона. Получатели – как правило, поставщики услуг, например интернет-провайдеры и финансовые учреждения. Запрашиваемые сведения обычно касаются клиентов получателя. Последний не может сообщить клиенту о том, что данные последнего затребованы судом. Хотя получатели NSL имеют право оспорить их в суде, запрет на разглашение не дает человеку, чьи данные были запрошены, узнать о самом факте существования повестки и, следовательно, оспорить ее в суде. Хорошей иллюстрацией того, как трудно противодействовать повесткам национальной безопасности, является видеозапись, в которой заместитель юрисконсульта ФБР пытается ответить на вопрос Джейкоба Аппельбаума: «Как я могу пойти в суд, если третьей стороне запрещено сообщать мне, что вы запросили мои данные?» Ее ответ: «Иногда мы должны на это идти», – пугает: http://youtu.be/dTuxoLDnmJU (запись вместе с сопроводительным материалом можно найти также на сайте Privacy SOS: http://privacysos.org/node/727).

Согласно Фонду электронных рубежей: «Из всех опасных инструментов правительственной слежки, список которых расширил патриотический закон, такое средство, как повестка национальной безопасности (NSL, раздел 18 свода законов США, § 2709, дополнено статьей 505 патриотического закона), – одно из самых пугающих и агрессивных. Эти повестки, посылаемые поставщикам услуг вроде операторов телефонной связи и интернет-провайдеров, позволяют ФБР тайно требовать информацию о конфиденциальной коммуникации и сетевой активности обычных американских граждан, все это – без какого-либо значимого надзора или предварительного судебного контроля. Получателям NSL запрещено сообщать об этих повестках коллегам, друзьям, даже членам семьи, а тем более – общественности». См.: https://www.eff.org/issues/national-security-letters. См. также подборку документов, связанных с NSL, обнародованных по закону о свободе информации, на сайте Фонда электронных рубежей: https://www.eff.org/issues/foia/07656JDB (все ссылки в этом примечании проверены 23 октября 2012 года).

65

См. примечание 41 о «первых криптовойнах» 1990-х годов.

66

Джулиан имеет в виду SSL/TLS, криптографический протокол, используемый сегодня в качестве стандарта во всех браузерах для безопасности интернет-сообщений – например, при осуществлении в Сети банковских операций.

67

Один пример из многих – см. Blackberry, Twitter probed in London riots, Bloomberg, 9 августа 2011 года: http://www.bloomberg.com/news/2011–08–09/blackberry-messages-probed-in-u-k-rioting-as-policesay-looting-organized.html (проверено 16 октября 2012 года).

68

Например, члена группы LulzSec, который обнаружил недостатки системы безопасности Sony, выложив в интернет личные данные клиентов Sony, арестовали, после того как его идентифицировал прокси-сайт HideMyAss.com по требованию ордера, выданного судом США. См. «Lulzsec hacker pleads guilty over Sony attack», BBC, 15 октября 2012 года: http://www.bbc.com/news/technology-19949624 (проверено 15 октября 2012 года).

69

SOPA – это Закон о прекращении онлайн-пиратства (Stop Online Piracy Act), а PIPA – Закон о защите интеллектуальной собственности (Protect Intellectual Property Act). Эти американские законопроекты попали в поле внимания мировой общественности в начале 2012 года. Они представляют собой недвусмысленное юридическое выражение желания контент-индустрии – организаций вроде Американской ассоциации звукозаписывающих компаний – повсеместно применить наиболее жесткие меры закона об интеллектуальной собственности в ответ на свободное распространение в Сети культурных артефактов. Оба они предлагают наделить органы исполнительной власти США, угрожавшие «сломать интернет», широкими полномочиями подвергать Сеть цензуре. Эти законопроекты вызвали ярость у существенной части международного сетевого сообщества и спровоцировали реакцию представителей индустрии, заинтересованных в свободном и открытом интернете.

В начале 2012 года Reddit, Wikipedia и несколько тысяч других сайтов сделали свои страницы черными в знак протеста против данных законопроектов, побуждая тем самым общественность как можно сильнее надавить на народных избранников. Другие поставщики онлайн-услуг, такие как Google, подписали соответствующие петиции. В результате оба законопроекта были заморожены в ожидании пересмотра и итогов дискуссии о том, выражают ли они наилучший подход к проблемам интеллектуальной собственности в интернете. В ходе этих событий впервые проявилось и утвердило себя эффективное лобби интернет-индустрии в Конгрессе.

70

См. заметку «О попытках преследования проекта WikiLeaks и связанных с ним людей» перед обсуждением.

71

ACTA – Международное соглашение по борьбе с контрафактной продукцией (Anti-Counterfeiting Trade Agreement). Это многосторонний межгосударственный договор, инициированный США и Японией и тайно обсуждавшийся на протяжении многих лет. Часть договора узаконивает новые драконовские меры по защите интеллектуальной собственности.

Первые черновики ACTA были обнародованы в 2008 году – их опубликовал WikiLeaks – и вызвали повсеместный протест активистов свободной культуры и защитников интернета. См. раздел ACTA на WikiLeaks: http://wikileaks.org/wiki/Category: ACTA.

Дипломатические телеграммы США, опубликованные в начале 2011 года WikiLeaks и La Quadrature du Net, показывают, что соглашение ACTA обсуждалось в обстановке секретности, чтобы обеспечить скорейшее создание радикальных правил требования выдачи IP, которые впоследствии были бы принудительно распространены на более бедные страны, не участвующие в соглашении. См. «WikiLeaks Cables Shine Light on ACTA History», La

Quadrature Du Net, 3 февраля 2011 года: http://www.laquadrature.net/en/wikileaks-cables-shine-light-on-acta-history (проверено 23 октября 2012 года).

В июле 2012 года после кампании, проведенной La Quadrature du Net и Жереми Циммерманом, Европарламент отверг АСТА.

72

M.A.I.D. ((Mutually) Assured Information Destruction, «(взаимно) гарантированное уничтожение информации») – это файловая система, в которой имеются учитывающее фактор времени дистанционное депонирование ключей и доказуемое установление идентичности с опциональным кодом бедствия. Она автоматически уничтожает криптографические ключи по истечении назначенного пользователем промежутка времени. См. https://www.noisebridge.net/wiki/M.A.I.D.

Правовые акты вроде принятого в 2000 году RIPA (Закон о контроле над правоохранительными органами, Regulation of Investigatory Powers Act) превратили Великобританию в страну, достаточно враждебную в отношении криптографии. RIPA предписывает физическим лицам дешифровывать данные и разглашать пароли по приказу полицейского. Обязательный юридический надзор законом не предусмотрен. Отказ от подчинения может обернуться обвинением в совершении уголовного преступления. Если на последующем суде обвиняемый заявит, что забыл пароль, обязанность доказать это ляжет на него самого. Для того чтобы избежать наказания, ему придется доказать, что не помнил пароля. Критики говорят, что это требование, по сути, означает презумпцию виновности. Для сравнения: в США прошло немало судебных процессов по тем же вопросам, и, хотя ситуация там далека от идеальной, в аналогичных обстоятельствах подсудимым куда успешнее помогало обращение к первой и четвертой поправкам к Конституции. См. отчет «Freedom from Suspicion, Surveillance Reform for a Digital Age», опубликованный JUSTICE 4 ноября 2011 года и доступный здесь: http://www.justice.org.uk/resources.php/305/freedom-from-suspicion.

Подробнее о файловой системе rubberhose см. «The Idiot Savants' Guide to Rubberhose» Сьюлетт Дрейфус: http://marutukku.org/current/src/doc/maruguide/t1.html (все ссылки проверены 24 октября 2012 года).

73

Архив прежней рассылки шифропанков можно скачать отсюда: http://cryptome.org/cpunks/cpunks-92–98.zip. Тим Мэй был одним из создателей этой рассылки. См. его «Шифрономикон» (Cyphernomicon) – вопросы и ответы по истории и философии шифропанка: http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html (обе ссылки проверены 24 октября 2012 года).

74

Proposed US ACTA plurilateral intellectual property trade agreement (2007), WikiLeaks, 22 мая 2008 года: http://wikileaks.org/wiki/Proposed_US_ACTA_multi-lateral_intellectual_property_trade_agreement_%282007 %29 (проверено 21 октября 2012 года).

75

Massive Takedown of Anti-Scientology Videos on YouTube, Фонд электронных рубежей, 5 сентября 2008 года: https://www.eff.org/deeplinks/2008/09/massive-takedown-anti-scientology-videos-youtube (проверено 16 октября 2012 года).

76

EU-India Free Trade Agreement draft, 24 Feb 2009, WikiLeaks, 23 июня 2009 года: http://wikileaks.org/wiki/EU-India_Free_Trade_Agreement_draft,_24_Feb_2009 (проверено 21 октября 2012 года).

77

Пиринговой (peer-to-peer, «равный с равным», сокращенно P2P) называется сеть, в

которой каждый компьютер функционирует как клиент или как сервер для всех остальных (то есть может и отсылать, и принимать информацию), позволяя быстро делиться контентом, таким как музыка, фильмы, документы или любой другой вид цифровой информации.

78

Облачный компьютинг означает, что многие функции, традиционно выполняемые компьютером, – такие как хранение информации (включая личные данные пользователя для различных приложений), хостинг и запуск ПО, а также обеспечение необходимых для этого мощностей – работают дистанционно, вне самого компьютера, «в облаке»; существуют компании, предлагающие услуги облачного компьютинга через интернет. Пользователю уже не нужен укомплектованный персональный компьютер – ему хватит устройства с выходом в Сеть, а остальное он получит оттуда. Метафора «облако» скрывает тот факт, что все данные и метаданные пользователя на самом деле оказываются в компьютере далеко-далеко в дата-центре, скорее всего, принадлежащем крупной корпорации наподобие Amazon, так что пользователь уже не контролирует ситуацию полностью – зато ее контролирует кто-то другой.

79

См. заметку «О попытках преследования проекта WikiLeaks и связанных с ним людей» перед обсуждением.

80

Diaspora – это социальная сеть, в которой компьютер каждого пользователя, инсталлировавшего соответствующее программное обеспечение, функционирует как отдельный сервер и контролирует распространение своих личных данных. Diaspora была создана как альтернатива Facebook, не нарушающая приватности. Это некоммерческая социальная сеть, которой владеют ее пользователи. Ее адрес http://diasporaproject.org.

81

Первый Napster (1999–2001) был пионером в области пиринговых сетей для обмена музыкой. Сервис имел безумную популярность, однако после иска Американской ассоциации звукозаписывающих компаний, которая обвинила его в нарушении авторских прав, сервис закрыли. После банкротства название Napster приобрел и использовал онлайн-магазин, продающий музыку за деньги.

82

См. заметку «О попытках преследования проекта WikiLeaks и связанных с ним людей» перед обсуждением.

83

Англ. peers, откуда и происходит название пирингового движения peer-to-peer – «от равного к равному». – *Прим. пер.*

84

Бенжамен Байяр – президент French Data Network, старейшего интернет-провайдера Франции, сторонник нейтральности сети и бесплатного программного обеспечения. См. раздел о нем в «Википедии» (на французском): http://fr.wikipedia.org/wiki/Benjamin_Bayart (проверено 15 октября 2012 года).

85

Ларри Лессиг – американский ученый и активист, наиболее известный своими концепциями копирайта и свободной культуры. Его блог: http://lessig.tumblr.com (проверено 15 октября 2012 года).

86

WikiLeaks опубликовал немало увлекательных дипломатических телеграмм США на эту тему. Любопытную дискуссию можно найти в следующих телеграммах (см. по ID-номерам телеграмм, все ссылки проверены 24 октября 2012 года):

07BEIRUT1301: http://wikileaks.org/cable/2007/08/07BEIRUT1301.html

08BEIRUT490: http://wikileaks.org/cable/2008/04/08BEIRUT490.html

08BEIRUT505: http://wikileaks.org/cable/2008/04/08BEIRUT505.html

08BEIRUT523: http://wikileaks.org/cable/2008/04/08BEIRUT523.html

87

См. телеграмму с ID-номером 10MOSCOW228, WikiLeaks: http://wikileaks.org/cable/2010/02/10MOSCOW228.html (проверено 24 октября 2012 года).

88

Подробнее об убийстве без суда и следствия американских граждан Анвара аль-Авлаки и его сына Абдулрахмана аль-Авлаки см.: Гленн Гринуолд, «The due-process-free assassination of U.S. citizens is now reality», Salon, 30 сентября 2011 года: http://www.salon.com/2011/09/30/awlaki_6. См. также «The killing of Awlaki's 16-year-old son», Salon, 20 октября 2011 года: http://www.salon.com/2011/10/20/the_killing_of_awlakis_16_year_old_son.

«Практически невозможно вообразить более откровенное отрицание основы основ республики, чем создание секретного, абсолютно никому не подконтрольного исполнительного агентства, которое одновременно собирает информацию обо всех гражданах и применяет "матрицу утилизации", чтобы определить, как именно наказать того или иного человека. Это классическая политическая антиутопия, ставшая реальностью», – Гленн Гринуолд, «Obama moves to make the War on Terror permanent», Guardian, 24 октября 2012 года: http://www.guardian.co.uk/commentisfree/2012/oct/24/obama-terrorism-killlist (все ссылки проверены 24 октября 2012 года).

89

Подробнее см. «Библиографию анонимности» и «Выборку статей об анонимности», курируемые Роджером Динглдином и Ником Мэтьюсоном: http://freehaven.net/anonbib (проверено 24 октября 2012 года). Валюты Чома эмитируются централизованно, но используют криптографию для обеспечения анонимности транзакции. Биткоин, другая электронная валюта, подробно обсуждаемая ниже, отличается от валют Чома тем, что все транзакции с ее использованием открыты, но сама валюта не контролируется никем.

90

Подробнее о банковской блокаде WikiLeaks см. заметку «О попытках преследования проекта WikiLeaks и связанных с ним людей» перед обсуждением.

91

Джулиан говорит здесь о плане британских властей расширить использование электронных браслетов. См. «Over 100,000 offenders to be electronically tagged», Guardian, 25 марта 2012 года: http://www.guardian.co.uk/society/2012/mar/25/prisons-and-probation-criminal-justice (проверено 22 октября 2012 года).

На момент обсуждения Джулиан находился под домашним арестом, ожидая разрешения дела об экстрадиции. В декабре 2010 года Джулиана арестовали и поместили в одиночную камеру, после внесения залога в размере более 30 тысяч фунтов стерлингов меру пресечения изменили на домашний арест. Одним из условий было нахождение в конкретные часы в помещении по определенному адресу, и, для того чтобы Джулиан не сбежал, работающая на правительство Великобритании частная охранная фирма закрепила на его лодыжке электронный браслет. Передвижения Джулиана отслеживались, и он должен был отмечаться в полиции ежедневно в течение более 550 дней. На момент публикации книги Джулиан фактически оказался заперт в посольстве Эквадора, круглосуточно окруженном лондонской полицией.

В июне 2012 года Джулиан пришел в посольство в поисках политического убежища от преследования властями США и их союзников. Он получил убежище в августе того же года.

92

Is CCA Trying to Take Over the World?, Американский союз гражданских свобод, 21 февраля 2012 года: http://www.aclu.org/blog/prisoners-rights/cca-trying-take-over-world. «Passing House Bill will worsen already pressing civil rights issue», ANNARBOR.com, 2 августа 2012 года:

http://annarbor.com/news/opinion/passing-house-bill-will-worsen-already-pressing-civil-rights-issue. См. также «Goldman Sachs to invest $9.6m in New York inmate rehabilitation», Guardian, 2 августа 2012 года: http://www.guardian.co.uk/society/2012/aug/02/goldman-sachs-invest-new-york-jail (все ссылки проверены 24 октября 2012 года).

93

Биткоин (http://bitcoin.org) – это первое по-настоящему удачное воплощение в жизнь классической шифропанковской концепции: криптографическая цифровая валюта. Биткоин подробно обсуждается далее; технология и философия этого платежного средства превосходно разъясняются в «Understanding Bitcoin», Al Jazeera, 9 июня 2012 года: http://www.aljazeera.com/indepth/opinion/2012/05/20125309437931677.html (проверено 22 октября 2012 года).

94

e-gold (электронное золото) – уже не существующая цифровая валюта, а также название компании, основанной в 1996 году. Министерство юстиции США обвинило собственников компании в «заговоре с целью отмывания денег». Они признали свою вину и были осуждены на семь лет домашнего ареста и общественные работы. Вынесший приговор судья заявил, что столь мягкое наказание оправданно, так как создатели e-gold не имели намерений заниматься противозаконной деятельностью. См. «Bullion and Bandits: The Improbable Rise and Fall of E-Gold», Wired, 9 июня 2009 года: http://www.wired.com/threatlevel/2009/06/e-gold (проверено 22 октября 2012 года).

95

В доинтернетную эпоху X.25 была основной глобальной сетью для обмена информацией параллельно с телефонной. Стоимость услуг в X.25 зависела от объема отправленных и полученных данных, но не от длительности соединения с телефонной сетью. Устройства связи (так называемые PAD) позволяли подключаться к X.25 через телефонную сеть с модемами или акустическими адаптерами. Подробнее см. в «Википедии»: http://en.wikipedia.org/wiki/X.25 (проверено 24 октября 2012 года).

96

От *англ.* mining – добыча. – *Прим. пер.*

97

Дэвид Чом – криптограф и создатель криптографических протоколов. Он разработал технологию цифровой валюты и создал eCash, первую анонимную криптографическую электронную валюту в мире.

98

О влиянии негативных материалов в СМИ см. «Bitcoin implodes, falls more than 90 percent from June peak», arstechnica, 18 октября 2011 года: http://arstechnica.com/tech-policy/2011/10/bitcoin-implodes-down-more-than-90-percent-from-june-peak (проверено 22 октября 2012 года).

99

См., например, «The Underground Website Where You Can Buy Any Drug Imaginable», Gawker, 1 июня 2011 года: http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable (проверено 22 октября 2012 года).

100

Раньше Лоуренс Лессиг писал о копирайте и культуре (например, в книге «Free Culture» (2004)), но в последние годы его занимает разложение американской демократии лоббистами в Конгрессе. См. The Lessig Wiki: http://wiki.lessig.org.

101

Ассоциация блюстителей порядка исправительных учреждений Калифорнии – влиятельное лобби, которое постоянно вкладывает в местные выборы семизначные суммы, хотя и не является самым крупным спонсором предвыборной кампании. См. «California

reelin», The Economist, 17 марта 2011 года: http://www.economist.com/node/18359882. См. также «The Golden State's Iron Bars», Reason, июль 2011 года: http://reason.com/archives/2011/06/23/the-golden-states-iron-bars. См. также раздел Ассоциации блюстителей порядка исправительных учреждений Калифорнии на сайте FollowTheMoney Национального института финансирования политики на уровне штата: http://www.followthemoney.org/database/topcontributor.phtml?u=3286&y=0 (все ссылки проверены 22 октября 2012 года).

102

Хейнц фон Фёрстер (1922–2002) – австрийско-американский ученый, один из основоположников кибернетики. Ему принадлежит так называемый этический императив, или девиз «Всегда поступай так, чтобы вариантов выбора стало больше» (*нем.* Handle stets so, daß die Anzahl der Wahlmöglichkeiten größer wird).

103

Джейкоб приписывает это наблюдение Джону Гилмору.

104

Подробнее о притеснениях Джейкоба и других людей, имеющих отношение к WikiLeaks, см. заметку «О попытках преследования проекта WikiLeaks и связанных с ним людей» перед обсуждением.

105

Игра слов: the great firewall of China дословно означает «великая китайская стена огня». – *Прим. пер.*

106

Айзек Мао – китайский блогер, разработчик программного обеспечения и бизнесмен, один из основателей CNBlog.org и член правления проекта Tor.

107

Так у автора. – *Прим. ред* .

108

См. страницу WikiLeaks о Надми Аучи: http://wikileaks.org/wiki/Nadhmi_Auchi (проверено 24 октября 2012 года).

109

Эти материалы можно прочесть на сайте WikiLeaks: http://wikileaks.org/wiki/Eight_stories_on_Obama_linked_billionaire_Nadhmi_Auchi_censored_from_the_Guardian,_Observer,_Telegraph_and_New_Statesman (проверено 24 октября 2012 года).

110

Сайты http://cables.mrkva.eu/ и http://cablegatesearch.net позволяют сравнить отредактированные версии телеграмм с полными и увидеть, какую именно информацию изъяли медиапартнеры WikiLeaks.

111

Qaddafi's Son Is Bisexual and Other Things the New York Times Doesn't Want You to Know, Gawker, 16 сентября 2011 года: http://gawker.com/5840809/qaddafis-son-is-bisexual-and-other-things-the-new-yorktimes-doesnt-want-you-to-know-about. Упомянутый пример относится к телеграмме с ID-номером 06TRIPOLI198, WikiLeaks: https://wikileaks.org/cable/2006/05/06TRIPOLI198.html. Сайт Cablegatesearch показывает историю редактуры телеграмм – исправленные фрагменты выделены розовым цветом: http://www.cablegatesearch.net/cable.php?id=06TRIPOLI198&version=1291757400 (все ссылки проверены 22 октября 2012 года).

112

Исходную телеграмму с ID-номером 10STATE17263 можно прочесть на сайте WikiLeaks: http://wikileaks.org/cable/2010/02/10STATE17263.html. Статья New York Times «Iran Fortifies Its Arsenal With the Aid of North Korea» была опубликована 29 ноября 2010

года: http://www.nytimes.com/2010/11/29/world/middleeast/29missiles.html?_r=0. Эта же телеграмма послужила основой для появившейся в Guardian 30 ноября 2010 года статьи Дэвида Ли «WikiLeaks cables expose Pakistan nuclear fears»: http://www.guardian.co.uk/world/2010/nov/30/wikileaks-cables-pakistan-nuclear-fears. Отредактированный вариант статьи, напечатанный газетой, не содержал ID-номера телеграммы и сократил ее до двух абзацев, относящихся к Пакистану: «US embassy cables: XXXXXXXXXXXX», Guardian, 30 ноября 2010 года: http://www.guardian.co.uk/world/us-embassy-cables-documents/250573. Масштаб редактуры можно оценить визуально на сайте Cablegatesearch, где изъятый текст выделен розовым цветом: http://www.cablegatesearch.net/cable.php?id=10STATE17263&version=1291486260 (все ссылки проверены 22 октября 2012 года).

113

Исходная телеграмма с ID-номером 08KYIV2414 на сайте WikiLeaks: http://wikileaks.org/cable/2008/12/08KYIV2414.html. Отредактированную версию Guardian см. в «US embassy cables: Gas supplies linked to Russian mafia», 1 декабря 2010 года: http://www.guardian.co.uk/world/us-embassy-cables-documents/182121? INTCMP=SRCH. Масштаб редактуры можно оценить визуально на сайте Cablegatesearch, где изъятый текст выделен розовым цветом: http://www.cablegatesearch.net/cable.php?id=08KYIV2414&version=1291255260 (все ссылки проверены 22 октября 2012 года).

114

Исходная телеграмма с ID-номером 10ASTANA72 на сайте WikiLeaks: http://wikileaks.org/cable/2010/01/10ASTANA72.html. Отредактированную версию Guardian см. в «US embassy cables: Kazakhstan – the big four», Guardian, 29 ноября 2010 года: http://www.guardian.co.uk/world/us-embassy-cables-documents/245167? INTCMP=SRCH. Масштаб редактуры можно оценить визуально на сайте Cablegatesearch, где изъятый текст выделен розовым цветом: http://www.cablegatesearch.net/cable.php?id=10ASTANA72&version=1291113360 (все ссылки проверены 22 октября 2012 года).

115

См., например, телеграмму с ID-номером 09TRIPOLI413 о западных энергетических компаниях, которые действуют в Ливии. По тексту телеграммы на сайте Cablegatesearch, где изъятые Guardian места выделены розовым, видно, что газета убрала все упоминания названий энергетических компаний и их руководителей, за исключением российского «Газпрома». Невзирая на то что в данном контексте западные компании выглядят даже выгодно, подвергшийся изощренной правке текст дает совсем другую картину: http://www.cablegatesearch.net/cable.php?id=09TRIPOLI413&version=1296509820 (проверено 22 октября 2012 года).

116

В этом примере исходная телеграмма содержала 5226 слов. В появившейся в Guardian отредактированной версии – всего 1406 слов. Исходная телеграмма с ID-номером 05SOFIA1207 на сайте WikiLeaks: http://wikileaks.org/cable/2005/07/05SOFIA1207.html. Отредактированная версия появилась в Guardian под заголовком «US embassy cables: Organised crime in Bulgaria» 1 декабря 2010 года: http://www.guardian.co.uk/world/us-embassy-cables-documents/36013. Телеграмма легла в основу опубликованной в Guardian статьи «WikiLeaks cables: Russian government “using mafia for its dirty work”», Guardian, 1 декабря 2010 года: http://www.guardian.co.uk/world/2010/dec/01/wikileaks-cable-spain-russian-mafia. Масштаб редактуры можно оценить визуально на сайте Cablegatesearch, где изъятый текст выделен розовым цветом: http://www.cablegatesearch.net/cable.php?id=05SOFIA1207&version=1291757400.

Пример с Болгарией обсуждается «Биволъ», медиапартнером WikiLeaks в этой стране,

в материале «Unedited cable from Sofia shows the total invasion of the state by organized crime (Update: Cable Comparison)», WL Central, 18 марта 2011 года: http://wlcentral.org/node/1480. См. дополнительно «The Guardian: Redacting, censoring or lying?», WL Central, 19 марта 2012 года: http://wlcentral.org/node/1490. См. также комментарии журналиста Guardian Дэвида Ли и ответы на них под обоими материалами WL Central (все ссылки проверены 22 октября 2012 года).

117

Имеется в виду телеграмма с ID-номером 09BERLIN1108. Ее редактуру можно визуально оценить на сайте Cablegatesearch, где изъятый текст выделен розовым цветом: http://www.cablegatesearch.net/cable.php?id=09BERLIN1108&version=1291380660 (проверено 22 октября 2012 года).

118

Другие примеры см. на сайте cabledrum: www.cabledrum.net/pages/censorship.php.

119

«Язык вражды» или «риторика ненависти» (*англ.* hate speech) – обобщенное выражение резко отрицательного отношения к носителям иной системы ценностей. – *Прим. пер.*

120

«Перехват телекоммуникаций. Председатель предоставил информацию о соотношении сил… Он вспомнил о негативном освещении темы в СМИ… На этом фоне председатель признал, что прогресс в данной области идет очень медленно… Различные делегаты выразили опасения в отношении готовящегося пресс-релиза, отметив, что он может спровоцировать цепную реакцию и критические отзывы в прессе. Комиссия отметила, что ее позиция не изменилась, и проинформировала делегатов, что одним из вариантов выхода из тупика могла бы стать стратегия, схожая с той, которая применяется при решении проблемы детской порнографии в интернете. Комиссия признаёт, что это другая тема, но в ней также присутствует аспект перехвата информации». Из обсуждения перехвата телекоммуникаций Рабочей группой по полицейскому сотрудничеству Европейской комиссии (13–14 октября 1999 года). Весь документ: http://www.quintessenz.at/doqs/000100002292/1999_10_13, Police%20Cooperation%20Working%20Group%20mixed%20committee%20meeting.pdf (проверено 24 октября 2012 года).

121

См. заметку «О попытках преследования проекта WikiLeaks и связанных с ним людей» перед обсуждением.

122

Джейкоб говорит о деле «Гилмор против Гонсалеса», 435 F.3d 1125 (9th Cir. 2006). Джон Гилмор, один из первых шифропанков, довел дело до Верховного суда США, пытаясь предать гласности содержание секретного закона, «директивы безопасности», ограничивающей права граждан путешествовать на самолете, не открывая своего имени. Гилмор оспаривал не только конституционность этого правового акта, но и то, что данный правовой акт относится к секретным и не может быть предан гласности, невзирая на то что он распространяется на граждан США. Суд при закрытых дверях сверился с директивой и не удовлетворил требование Гилмора признать ее противоречащей конституции. Содержание директивы не было предано огласке ни на одном заседании. См. Gilmore vs Gonzales на сайте PapersPlease.org: http://papersplease.org/ gilmore/facts.html (проверено 22 октября 2012 года).

123

Христиания – самопровозглашенная автономная территория в Копенгагене, столице Дании. По сути, это бывшие армейские казармы, которые в 1970-е заняло разношерстное сообщество коллективистов и анархистов. Христиания добилась уникального для Дании юридического статуса.

124

Принцип сетевой нейтральности требует, чтобы провайдером было запрещено (причем

запрещено законом, добавляет большинство) ограничивать пользователям доступ к сетям, являющимся частями интернета, включая ограничение по контенту. См. о сетевой нейтральности на сайте Фонда электронных рубежей: https://www.eff.org/issues/net-neutrality (проверено 24 октября 2012 года).

125

Blocking WikiLeaks emails trips up Bradley Manning prosecution, Politico, 15 марта 2012 года: http://www.politico.com/blogs/under-theradar/2012/03/blocking-wikileaks-emails-trips-up-bradley-manning-117573.html (проверено 21 октября 2012 года).

126

Подробнее о Bay Холланде см. Wau Holland Stiftung: http://www.wauland.de.

127

Министерство государственной безопасности ГДР, сокращенно Штази. – *Прим. пер.*

128

Stasi still in charge of Stasi files, WikiLeaks, 4 октября 2007 года: http://www.wikileaks.org/wiki/Stasi_still_in_charge_of_Stasi_files (проверено 22 октября 2012 года).

129

«Вот что вы можете сделать, чтобы мир стал лучше, прямо сейчас. Возьмите все те деньги, которые мы каждый год расходуем на вооружения и оборону, и вместо этого потратьте их на еду, одежду и образование бедняков по всей планете, столько, сколько потребуется, без каких бы то ни было исключений – и тогда мы сможем исследовать космос, все вместе, внутренний и внешний, всегда, в мире и спокойствии» (Билл Хикс). См. видеозапись выступления «Bill Hicks – Positive Drugs Story»: http://youtu.be/vX1CvW38cHA (проверено 24 октября 2012 года).

130

Закон Сарбейнса–Оксли 2002 года – американский закон, принятый по следам корпоративных и аудиторских скандалов в компаниях Enron, Tyco International, Adelphia, Peregrine Systems и WorldCom. Он нацелен на искоренение коррупционной практики, которая привела к кризису. Раздел 1107, кодифицированный как USC 1513 (e), превращает месть информаторам в уголовное преступление.

131

Евгений Морозов (Evgeny Morozov) «The Net Delusion: The Dark Side of Internet Freedom» (Public Affairs, 2011).

132

О свободном программном обеспечении см. «The Free Software Definition» с сайта GNU: https://www.gnu.org/philosophy/free-sw.html.

Свободное аппаратное обеспечение (АО) – это техника, не обремененная патентами и сконструированная по открытым стандартам. Никакие законы не запрещают анализировать АО или вмешиваться в ход его работы, а принципы создания, инструкции и планы имеются в свободном доступе, так что каждый, кто располагает необходимыми ресурсами, может создать копию АО. Подробнее о свободном АО см. «Exceptionally Hard and Soft Meeting: exploring the frontiers of open source and DIY», EHSM: http://ehsm.eu. См. также статью «Open-source hardware» в «Википедии»: https://en.wikipedia.org/wiki/Open-source_hardware (все ссылки проверены 24 октября 2012 года).

133

О 3D-принтерах, использующих свободное и открытое аппаратное обеспечение, см. видеоклип, представляющий 3D-принтер RepRap: http://vimeo.com/5202148 (проверено 24 октября 2012 года).

134

«Будь сбоем, который ты хотел бы устроить миру» – цитата из фотографического веб-комикса «A Softer World»: http://www.asofterworld.com/index.php?id=189 (проверено 24

октября 2012 года).

135

Для изучения любой поднятой в обсуждении темы Джейкоб рекомендует два ресурса: «Библиографию анонимности» и «Выборку статей об анонимности», курируемые Роджером Динглдином и Ником Мэтьюсоном: http://freehaven.net/anonbib; а также «Библиографию цензуры» и «Выборку статей о цензуре», курируемые Филиппом Уинтером: www.cs.kau.se/philwint/censorbib (обе ссылки проверены 24 октября 2012 года).

136

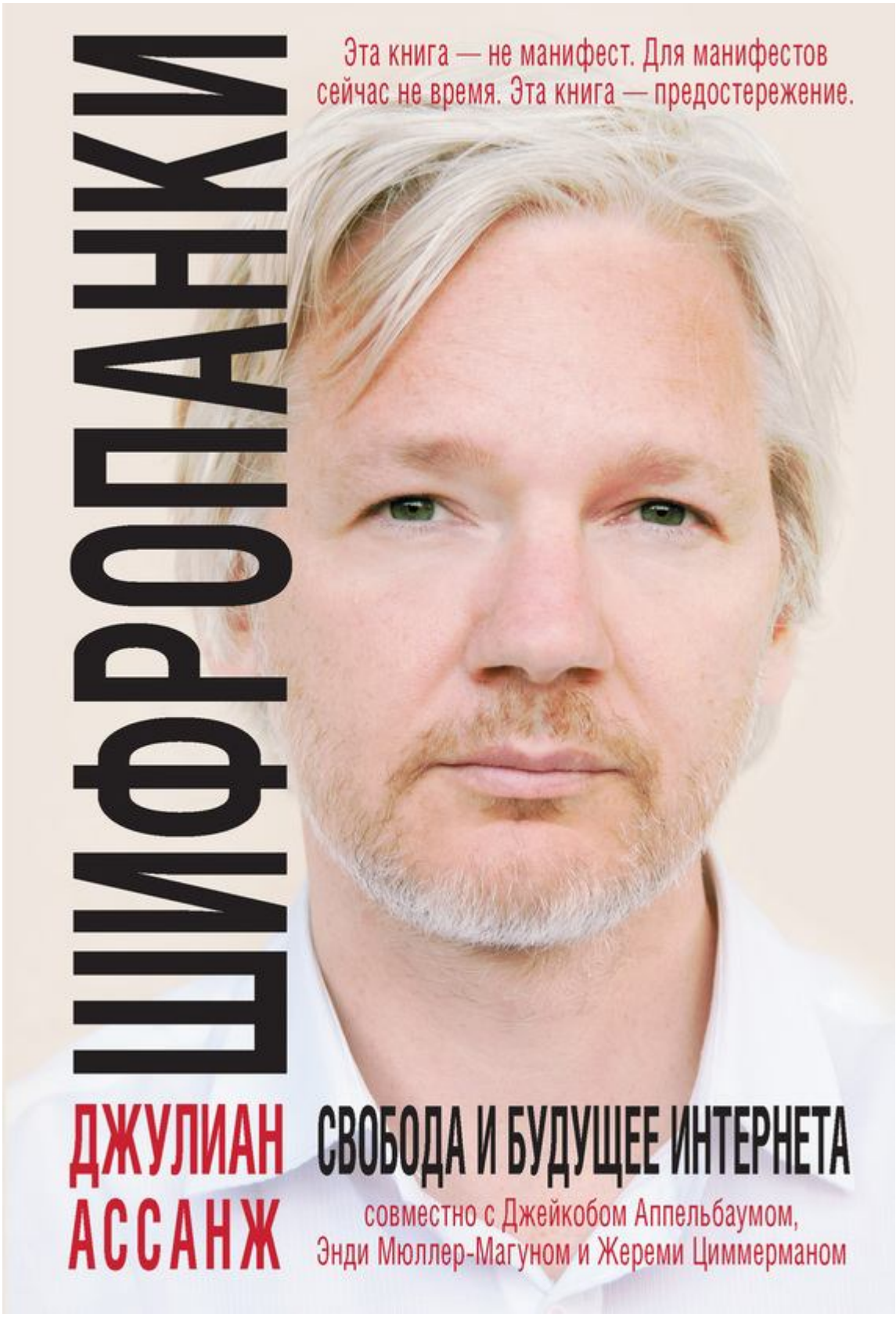
Намеренно пустая сноска. (В фантастической трилогии «Иллюминат!» Роберта Ши и Роберта Энгуса Уилсона слово fnord появляется в текстах, которые должны пробудить в человеке беспокойство и страх, причем непросветленный читатель этого слова не видит, в отличие от просветленного, над чьим сознанием fnord не имеет власти. – *Прим. пер.*)

137

Nawaat.org – тунисский независимый коллективный блог, созданный в 2004 году: http://nawaat.org/portail. Проект Tunileaks был запущен блогерами Nawaat в ноябре 2010 года и публиковал телеграммы из WikiLeaks, имеющие отношение к Тунису: https://tunileaks.appspot.com. Подробнее о Tunilinks и попытке правительства Бен Али подвергнуть этот сайт цензуре см. «Tunisia: Censorship Continues as WikiLeaks Cables Make the Rounds», Global Voices Advocacy, 7 декабря 2010 года: http://advocacy.globalvoicesonline.org/2010/12/07/tunisia-censorship-continuesas-wikileaks-cables-make-the-rounds (все ссылки проверены 24 октября 2012 года).

ШИФРОПАНКИ

Эта книга — не манифест. Для манифестов сейчас не время. Эта книга — предостережение.



ДЖУЛИАН АССАНЖ

СВОБОДА И БУДУЩЕЕ ИНТЕРНЕТА

совместно с Джейкобом Аппельбаумом, Энди Мюллер-Магуном и Жереми Циммерманом