|  |  |
| --- | --- |
| **Protecting yourself** | **Защити себя самостоятельно** |
| The world isn’t a binary choice between living in a surveillance state and opting out of all technological developments. You can use the technology and opt out of sharing your private information at the same time — you just have to know how. | Мир - это не двойной выбор между жизнью в состоянии наблюдения и отказом от всех технологических разработок. Вы можете использовать технологию и одновременно отказаться от обмена личной информацией - вам просто нужно знать, как это сделать. |
| A new kind of service is trying to help ordinary users take control of their digital lives. Companies such as Disconnect and Jumbo act like a digital concierge for their users, changing privacy settings, deleting sensitive data and making surveillance difficult. However, to use the privacy apps to their fullest means giving them a level of control over your digital life that would be very easy to abuse — and it’s hard to be certain that any company can be trusted with such sensitive information. | Новый вид сервиса пытается помочь обычным пользователям взять под контроль свою электронную жизнь. Такие компании, как Disconnect и Jumbo, действуют как цифровой консьерж для своих пользователей, изменяя настройки конфиденциальности, удаляя персональные данные и затрудняя наблюдение. Однако, использовать приложения для обеспечения конфиденциальности в полной мере означает предоставить им такой уровень контроля над вашей цифровой жизнью, которым было бы очень легко злоупотребить - и трудно быть уверенным, что какой-либо компании можно доверять такую ​​секретную информацию. |
| **Changing settings** | **Изменение настроек** |
| The main reason for the rise of privacy apps is the increase in “settings” and “preferences” screens in our lives and the powerful options within them. Web platforms are complex, with large networks of linked services, spin-offs and acquisitions. Each of them treats users differently, has a separate place to change privacy settings and could theoretically expose some information you would rather keep private. | Главной причиной роста количества приложений для обеспечения конфиденциальности является увеличение количества экранов «настроек» и «предпочтений» в нашей жизни, а также их важных опций. Веб-платформы являются комплексом, с обширными сетями связанных сервисов, дочерних компаний и приобретений. Каждый из них относится к пользователям по-разному, имеет отдельное место для изменения настроек конфиденциальности и теоретически может раскрыть некоторую информацию, которую вы предпочли бы сохранить в тайне. |
| What your settings are at any given moment probably depends on when you opened your account, when you last logged in and how good you are at reading pop-ups that flash in front of you when you just want to find out the address of the party you’re going to. | В каком состоянии находятся ваши настройки в любой момент, вероятно, зависит от того, когда вы открывали свою учетную запись, когда последний раз входили в систему и насколько хорошо вы читаете всплывающие окна, которые высвечиваются, когда вы просто хотите узнать адрес вечеринки на которую собираетесь. |
| Facebook has even actively changed privacy settings in the past, a practice for which it was given a “consent decree” by the US Federal Trade Commission in 2011 (which it then broke during the Cambridge Analytica scandal, leading to a $5 billion (€4.5 billion)fine). But even if a company hasn’t changed your privacy settings, it can still be hard to find out exactly how much information you are making public. | Facebook даже активно менял настройки конфиденциальности в прошлом. Практика, на которую в 2011 году Федеральная торговая комиссия США дала «указ о согласии» (который затем был нарушен во время скандала с Cambridge Analytica, что привело к выплате 5 млрд. долларов (4,5 млрд. евро) штрафа). Но даже если компания не изменила ваши настройки конфиденциальности, может быть по-прежнему сложно в точности определить, какой объем информации вы публикуете. |
| For instance, whether or not Google is tracking your physical location 24/7 on an Android phone depends on when you first used Google Maps and whether you have changed any settings since. The company used to turn “location history” on by default. Now, it does not. | Например, отслеживает ли Google ваше физическое местоположение 24/7 на телефоне Android, зависит от того, когда вы впервые использовали Google-Карты и изменили ли вы какие-либо настройки с тех пор. Раньше компания по умолчанию включала «историю местоположений». Теперь такая функция отсутствует. |
| **Acting as an advocate** | **Действуя как защитник** |
| Jumbo is an app for iOS and Android launched in 2019. Its goal is to cut through some of this confusion. The offer is simple: by downloading the app and checking a few boxes, the app automatically locks down your privacy settings on platforms that include Facebook, Google, Twitter and Amazon. Instead of you having to find every individual preferences screen and decide which settings are harmless — and which are worded to sound harmless — the app does it for you. | Jumbo - это приложение для iOS и Android, запущенное в 2019 году. Его цель - избавиться от данного беспорядка. Предложение простое: загрузив приложение и установив несколько галочек, оно автоматически блокирует ваши настройки конфиденциальности на платформах, включая Facebook, Google, Twitter и Amazon. Вместо того, чтобы искать каждый экран индивидуальных предпочтений и решать, какие настройки безвредны, а какие лишь сформулированы так, чтобы казаться безобидными - приложение сделает это за вас. |
| Pierre Valade, the company’s Brooklyn-based founder, describes its role as an advocate for users everywhere. “It’s an unfair game between users at one end and companies at the other. Companies write privacy policies with lawyers, and they make it harder for you to figure out how to opt out, how to delete your data, but as a user, you’re supposed to figure out all of that yourself. That’s the idea here: it’s about representing people and working for them, to simplify a complex system.” | Пьер Валад, основатель компании из Бруклина, описывает роль приложения как защитника интересов пользователей во всем мире. «Это нечестная игра между пользователями с одной стороны и компаниями с другой. Компании создают политику конфиденциальности вместе с юристами, и вам становится сложнее понять, как отказаться от нее, как удалить свои данные, но, как пользователь, вы должны выяснить всё это самостоятельно. В этом суть идеи: представлять людей и работать для них, чтобы упростить сложную систему». |
| The service Jumbo offers is possible because the largest technology companies can be shamed into giving users the ability to opt out of the worst violations of their privacy. Google doesn’t want you to turn off all of its ad personalization, but, the company rationalizes, most people probably won’t even know about the setting, and it satisfies the privacy warriors to have the option to remove themselves from the tracking apparatus, even if most of the world leaves the options exactly as they are. | Услуга, которую предлагает Jumbo, возможна, потому что крупнейшим технологическим компаниям может быть стыдно за то, что они дают пользователям возможность отказаться от самых худших нарушений их конфиденциальности. Google не хочет, чтобы вы отключили всю его рекламную персонализацию, но, по мнению компании, большинство людей, вероятно, даже не узнают о настройке, что удовлетворяет борцов с конфиденциальностью, которые имеют возможность удалить себя из устройства отслеживания, даже если большая часть мира оставляет параметры в исходном виде. |
| But for the rest of the internet, shame doesn’t work. Most of the companies that track you across the internet aren’t polite enough to give you the ability to opt out, nor are they open enough for you to know they’re snooping on you in the first place. You might remember to go into the cookie settings for some websites, if you’re diligent, but eventually, you’ll forget — or visit a dubious site that disregards the law. For those sites, you need a rather pushier sort of advocate: something like Disconnect. | Но остальной части Интернета незнакомо понятие стыда. Большинство компаний, которые отслеживают вас через всемирную паутину, недостаточно вежливы, чтобы дать вам возможность отказаться, также они недостаточно открыты для того, чтобы знать, что за вами с самого начала ведётся слежка. Возможно, вы не забудете войти в настройки файлов cookie для некоторых веб-сайтов, если будете стараться, но в конечном итоге вы забудете или посетите сомнительный сайт, нарушающий закон. Для таких сайтов вам нужен более настойчивый защитник: что-то наподобие Disconnect. |
| The company offers a service that uses ad blockers, firewalls and virtual private networks (VPNs) to sit between you and the snoopers, letting through only the information you intend to make public. | Компания предлагает услугу, которая использует блокировщики рекламы, брандмауэры и виртуальные частные сети (VPN), чтобы находиться между вами и наблюдателями, пропуская только ту информацию, которую вы собираетесь опубликовать. |
| “Without protection like ours, thousands of trackers collect information about our online activity when we simply use our phones or computers,” says Casey Oppenheim, the company’s co-founder. “Most of these trackers are companies we’ve never interacted with directly, yet they collect detailed profiles including our location data, browsing history and more.” | «Без такой защиты, как наша, тысячи трекеров собирают информацию о нашей онлайн-активности, когда мы просто используем наши телефоны или компьютеры», - говорит Кейси Оппенгейм, соучредитель компании. «Большинство этих трекеров - это компании, с которыми мы никогда не взаимодействовали напрямую, однако они собирают подробные досье, включая данные о нашем местоположении, историю просмотров и многое другое». |
| For trackers across the net, that means the app keeps a blacklist, preventing the worst offenders from loading up to protected devices at all. Then, in situations where the snoopers might be sitting between the device and the internet — think an airport Wi-Fi — the app offers a simple VPN service that turns on automatically when needed, preventing anyone else on the connection from seeing what’s being shared. | Для трекеров в сети это означает, что приложение хранит черный список, не позволяя злоумышленникам вообще загружаться на защищенные устройства. Затем, в ситуациях, когда наблюдатели могут находиться между устройством и Интернетом - подумайте о Wi-Fi в аэропорту - приложение предлагает простую службу VPN, которая автоматически включается при необходимости, не позволяя никому, кто находится в соединении, видеть, что передается. |
| **Collecting your private information** | **Сбор вашей личной информации** |
| Anyone, that is, other than Disconnect. Because the difficult problem with the new wave of privacy apps is that, to use them, you have to trust them with your most sensitive information. Services such as Jumbo make an even bigger demand than most internet services: for that app to work, it must request and store your usernames and passwords for every service you want it to work with. These are probably the most sensitive passwords you have, considering the importance of accounts on Facebook, Google and Amazon. Both apps make it clear that they have no intention of using that information. | Это может делать кто угодно, кроме Disconnect. Потому что сложная проблема с новой волной приложений для обеспечения конфиденциальности заключается в том, что для их использования вы должны доверить им свою самую личную информацию. Такие сервисы, как Jumbo, пользуются даже большим спросом, чем большинство интернет-сервисов: для того, чтобы это приложение работало, оно должно запрашивать и хранить ваши логины и пароли для каждой службы, с которой вы хотите, чтобы оно работало. Это, вероятно, самые конфиденциальные пароли, что у вас есть, учитывая важность учетных записей в Facebook, Google и Amazon. Оба приложения дают понять, что не собираются использовать эту информацию. |
| Disconnect’s Oppenheim says: “We don’t want, and don’t ask, users to trust us with any sensitive information. In fact, we collect as little data as possible; we don’t even require email or any personal information, and our technology is architected to not collect any user data. As per our privacy policy: ‘We don’t collect any of your personal info, including your IP address, other than information you voluntarily provide.’” | Оппенгейм из Disconnect говорит: «Мы не хотим и не просим пользователей доверять нам какую-либо секретную информацию. Фактически, мы собираем как можно меньше данных; нам даже не требуется электронная почта или какая-либо личная информация, а наша технология спроектирована так, чтобы не собирать никаких пользовательских данных. В соответствии с нашей политикой конфиденциальности: «Мы не собираем никакой вашей личной информации, включая IP-адрес, кроме информации, которую вы предоставляете нам добровольно». |
| Jumbo goes a step further: the app is carefully constructed so that the most sensitive information never leaves the user’s device. It would be a lot easier for Jumbo to work as a web service, connecting to various sites from a centralized server. Instead, it operates more like a heavily automated web browser by logging on to Twitter, Facebook and the rest for you. | Jumbo идёт на шаг впереди: приложение тщательно разработано так, чтобы самая секретная информация никогда не покидала устройство пользователя. Было бы намного проще для Jumbo работать как веб-сервис, подключаясь к различным сайтам с централизованного сервера. Вместо этого он больше похож на полностью автоматизированный веб-браузер, выполняя вход в Twitter, Facebook и т.д. за вас. |
| The process is, admittedly, arduous: the first run-through can take a long time to complete and leave your phone rather hot. But founder Pierre Valade hopes it helps people trust his app with their sensitive information. “We’re trying to do a better job in the long run,” he says, “but I think that we do have a good foundation. If you go to a doctor, you have to give them your X-rays, your blood work. If you go to a lawyer, you have to give them the information about your case. You must trust them to work for you. But we’ve designed a technology that only works on the phone; we don’t have access to it. By design, it’s very safe. It’s not completely bulletproof, but it makes it much, much harder.” | По общему признанию, процесс трудоемкий: первый просмотр может занять много времени, из-за чего ваш телефон достаточно нагреется. Но основатель Пьер Валад надеется, что это поможет людям доверять его приложению свою конфиденциальную информацию. «Мы стараемся работать лучше в долгосрочной перспективе», говорит он, «но я думаю, что у нас есть хорошая основа. Если вы пойдете к врачу, то должны будете отдать ему свой рентген и анализ крови. Если вы пойдете к юристу, то вам нужно будет предоставить ему информацию по вашему делу. Вы должны доверить им работу на вас. Но мы разработали технологию, которая работает только на телефоне; у нас нет к ней доступа. По структуре приложение очень безопасно. Оно не обладает полной защитой, но разработка делает его намного надёжнее». |
| **Fighting for your trust** | **Борьба за ваше доверие** |
| Ultimately, it’s about trust. That’s not unusual; after all, nearly every action you take in life is backed up by trust rather than technical guarantees. (There’s no technology, for instance, that stops the postie opening your letters and talking about them with their friends.) But the nature of their access means that the companies that provide privacy apps need to fight harder than most to prove they’re trustworthy. | В конечном счёте, всё дело в доверии. В этом нет ничего необычного; в конце концов, почти каждое ваше действие в жизни подкреплено доверием, а не техническими гарантиями. (Например, нет технологии, которая не позволяла бы почтальонам открывать ваши письма и рассказывать о них своим друзьям). Но характер их доступа означает, что компаниям, которые предоставляют приложения для обеспечения конфиденциальности, нужно бороться сильнее, чем большинству, чтобы доказать, что они заслуживают доверия. |
| For Valade, he tries to move the focus away from the fact that Jumbo is free. “Something that’s been important for us is that we’re not seen as a free product, because everyone knows there is no such thing as a free product,” he says. | Что касается Валаде, он пытается отвлечь внимание от того факта, что Jumbo бесплатен. «Для нас было важно то, что нас не рассматривают как бесплатный продукт, поскольку все знают, что таких не существует», - говорит он. |
| Jumbo planned to introduce a subscription service in March 2020, which adds extra features for people who want to increase their privacy and security. Disconnect already has a similar option, Disconnect Premium, which offers permanent VPN use across up to three devices for $50 (€45) a year. The paid-for features, the companies hope, will convince their users that they aren’t secretly selling data on the side to fund their development. But the free tiers remain available, and, trust aside, it’s hard to see why they aren’t more popular. For some, there may be a feeling that there’s no real option to keep big tech out of our lives, and privacy apps will only ever be a partial solution. | В марте 2020 года Jumbo планирует представить услугу подписки, которая добавляет дополнительные функции для людей, которые хотят повысить свою конфиденциальность и безопасность. У Disconnect уже есть аналогичный вариант Disconnect Premium, который предлагает постоянное использование VPN на трех устройствах за 50 долларов (45 евро) в год. Компании надеются, что платные функции убедят своих пользователей в том, что они тайно не продают данные на стороне для финансирования своих разработок. Но уровни бесплатного пользования остаются доступными, и, если отвлечься от этого, трудно понять, почему они не пользуются большей популярностью. У некоторых может возникнуть ощущение, что нет реальной возможности убрать высокие технологии из нашей жизни, и приложения для обеспечения конфиденциальности будут лишь частичным решением. |
| Valade hopes otherwise: “It’s a bit like saying you shouldn’t lock the door because someone can smash a door. Yes, I think people can stop using their phone, move to India, take hash and live in the mountains. But the reality is that we can get more privacy now, within the world that we actually live in. So, our goal is to make privacy so convenient that you can actually get it. Our point is actually more about control. Are you OK with what you sign up for? | Валаде надеется на иное: «Это все равно что сказать, что нельзя запирать дверь, потому что кто-то может ее взломать. Да, я думаю, что люди могут перестать пользоваться телефоном, переехать в Индию, употреблять хэш и жить в горах. Но реальность такова, что теперь мы можем получить больше конфиденциальности в том мире, в котором на самом деле живем. Итак, наша цель - сделать частную жизнь настолько комфортной, чтобы вы действительно могли ее получить. Хотя в нашем случае речь идёт скорее о контроле. Вы согласны с тем, на что подписываетесь? |