Источники

Авторы: Нате Кардосо [Nate Cardozo], Курт Опзаль [Kurt Opsahl], Рейни Райтман [Rainey Reitman]

Редакторы: Паркер Хиггинс [Parker Higgins], Дейв Маасс [Dave Maass]

Форматирование: Паркер Хиггинс Публикация Electronic Frontier Foundation, 2015

Оригинал: см. на www.eff.org/who-has-your-back-government-data-requests-2015

Статья «Кто защищает ваши данные?» — сокращенная версия «Кто прикрывает вам спину?» 2015: Защита ваших данных от правительственных запросов от Electronic Freedom Foundation

Кто защищает ваши данные?

Вышел пятый годовой отчет Electronic Frontier Foundation по конфиденциальности и прозрачности онлайн, где объясняются последствия для всех наших данных.

Мы живем цифровыми жизнями: от размещения видео в социальных сетях до приложений, определяющих наше местонахождение на мобильном телефоне; от ввода данных для проверки почты до сохраненных документов, и, конечно же, нашего журнала посещений. Личное, скрытое и даже смешное — все это переносится в пакеты данных и разлетается по оптоволоконным артериям сети.

Хотя в нашей обычной жизни на дворе XXI век, законодательство не успевает за временем. На данный момент, Конгресс США не удосужился обновить Закон о конфиденциальности электронных коммуникаций 1986 г. [Electronic Communications Privacy Act], чтобы зафиксировать, что электронная почта, которая хранится дольше шести месяцев, должна иметь такую же защиту, что и почта, которая хранится менее шести месяцев. Конгресс также умышленно затягивает прекращение неизбирательной слежки АНБ за онлайн-коммуникациями, и должен провести сильные реформы, которых мы заслуживаем. Более того, Конгресс готов еще сильнее ухудшить ситуацию, рассматривая предложения узаконить правительственное «проникновение с черного хода» (как и правительство Великобритании в данный момент) в технологии, которые мы используем для цифровых коммуникаций.

В подобных условиях мы все больше ожидаем, что сами технологические компании начнут придерживаться самой строгой политики по защите прав пользователя. Однако какие компании будут защищать пользователей, настаивая на прозрачности и строгом соответствии закону при использовании правительством пользовательских данных? И какие компании сделают эту политику общедоступной, позволяя всему миру — и своим пользователям — судить о том, как они защищают наше право на конфиденциальность?

Уже четыре года Electronic Frontier Foundation документирует работу основных интернет-компаний и провайдеров услуг, оценивая публично провозглашаемую политику каждой из них и выбирая наилучшие. За время подготовки первых четырех отчетов мы были свидетелями изменений в работе основных технологических компаний.

> «Хотя в жизни на дворе XXI век, законодательство не успевает за временем.»

В большинстве случаев техногиганты стали публиковать ежегодные отчеты о запросах данных правительством, обещая уведомить пользователей, если правительство захочет получить доступ к их данным и требуя ордера

на обыск перед предоставлением доступа к пользовательскому контенту. Подобного рода замечательная практика, которую мы зафиксировали в ранних отчетах EFF, стала промышленным стандартом буквально через несколько лет, и мы гордимся той ролью, которую сыграли наши ежегодные отчеты, подталкивая компании к внедрению этих изменений. Однако времена меняются, и теперь пользователи ожидают большего.

Критерии, которые мы применяли для оценки компаний в 2011 г., были весьма смелы для своего времени, но за прошедшие годы стали практически нормой. Теперь пользователи должны рассчитывать на то, что компании намного превосходят стандарты, изначально сформулированные в отчете «Кто прикрывает вам спину?». Пользователи вправе ожидать, что такие компании, как Google, Apple, Facebook и Amazon, придерживаются политики прозрачности по поводу контента, заблокированного или удаленного ими в ответ на правительственные запросы, а также по поводу того, какие удаленные данные продолжают сохраняться, на случай, если правительство вздумает искать их в будущем. Мы также рассчитываем, что эти компании займут четкую позицию против разрешенных правительству лазеек [backdoors].

В данном, пятом ежегодном отчете «Кто прикрывает вам спину?» мы взяли основные принципы предыдущих отчетов и отнесли их в единую категорию: Наилучшая практика, принятая в индустрии [Industry Accepted Best Practices]. Мы также уточнили наши требования по предоставлению пользователям уведомлений и добавили новые категории, чтобы выделить другие важные проблемы прозрачности и защиты прав пользователей. Мы считаем, что пора начать ожидать большего от Кремниевой Долины.

Мы создали этот отчет, чтобы еще выше поднять принципы «Кто прикрывает вам спину?» и посмотреть, какие компании по-прежнему лидируют в списке.

Критерии оценки

С этой целью мы использовали следующие пять критериев для оценки работы и политики компаний:

1 **Наилучшая практика, принятая в индустрии.** Это комбинированная категория, которая оценивает компании по трем критериям, которым они должны соответствовать, чтобы это засчитывалось:

» Требует ли компания, чтобы правительство получило судебный ордер перед тем, как передать ему содержание сообщений пользователя?

» Публикует ли компания прозрачный отчет [transparency report], т. е. регулярные полезные данные о том, сколько раз правительство требовало предоставить данные пользователей и как часто компания предоставляла эти данные правительству?

» Публикует ли компания руководство по укреплению законности, объясняя, как именно она отвечает на требования со стороны правительства?

2 **Сообщайте пользователям о том, что правительство требует предоставить данные.** Чтобы заработать звездочку в этой категории, интернет-компании должны обещать сообщать пользователям о том, что правительство США требует предоставить их данные, если это не запрещено законом, что возможно в крайне узких и чрезвычайных ситуациях, или если подобное действие окажется бесполезным или неэффективным.

Уведомление даст пользователям шанс защититься от правительственных запросов на получение их данных. Наилучшей практикой будет предупредить пользователей заранее, чтобы они могли опротестовать эти запросы в суде. Так что мы уточнили наш критерий прошлых лет. Теперь мы требуем, чтобы компания предоставляла пользователям уведомление заранее, исключая те случаи, когда это запрещено законом или в случае чрезвычайной ситуации, и чтобы компания также предоставляла уведомление впоследствии, после прекращения чрезвычайной ситуации или после того, когда у нее

В отчете 2015 г. EFF подняли планку.

вынут кляп. При составлении прошлогоднего отчета мы сообщили компаниям, что мы собираемся вводить это уточнение в 2015 г., чтобы дать им целый год на реализацию процедур по предоставлению отложенного уведомления при необходимости.

3 **Публичная огласка политики хранения данных компании.** Эта категория награждает компании, которые сообщают, как долго они хранят данные о своих пользователях, недоступные пользователям — в частности, включая записи IP-адресов пользователя и удаленный контент — в форме, доступной правоохранительным органам. Если период хранения изменяется по техническим или иным причинам, компания должна сообщить об этом и опубликовать примерный средний или обычный период с указанием верхней границы при наличии таковой. Мы даем эту звезду любой компании, политика которой доступна для общественности — даже если это политика, с которой категорически не согласен EFF; например, если компания сообщает, что хранит данные о своих пользователях на постоянной основе.

4 **Сообщать, сколько раз правительство требовало удаления контента или учетных записей пользователей и сколько раз компания соглашалась на это требование.** Сейчас в индустрии стало стандартной практикой предоставлять transparency report. Мы считаем, что обязательство компаний »

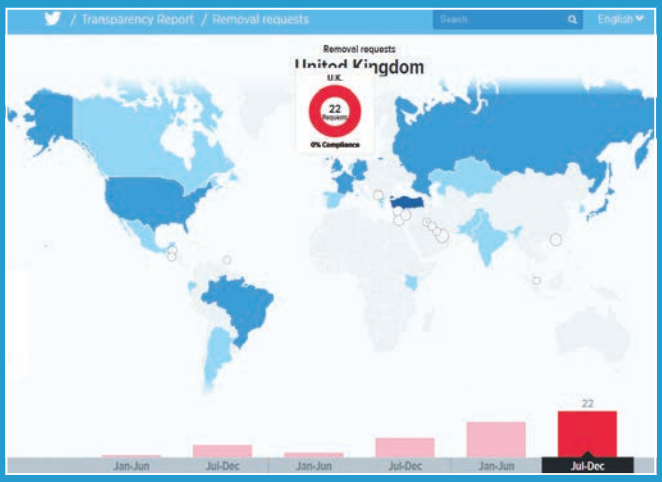
Правительственные требования удаления данных

Более года ведущий исследователь EFF Дейв Маасс сообщал, что Facebook сотрудничает с тюремными системами по всей территории США, блокируя заключенным доступ к социальной сети. Facebook даже настроил спецформу «Запрос на удаление учетной записи заключенного [Inmate Account Takedown Request]», чтобы облегчить работникам тюрем пометку учетных записей для их блокировки, даже если эти записи не нарушают Условий предоставления услуг Facebook.

Такая практика вдохновила EFF на создание новейшей категории: отслеживание того, как часто компании удаляют контент или блокируют учетные записи по требованию правительства. Чтобы быть отмеченными в этой категории, компаниям не надо отказывать по всем или даже некоторым правительственным требованиям удаления контента. Они просто должны придерживаться политики прозрачности по поводу того, как часто они блокируют или удаляют контент или учетные записи.

Хотя это несложно, многие компании в этой области проштрафились, включая Facebook — компанию-вдохновителя данной категории. Мы оценивали 24 компании, и 15 были отмечены положительно, хотя часть их вообще не размещает контента.

Ярчайший пример хорошей практики — Twitter: опубликованные ими данные включают интерактивные карты, позволяющие навести курсор на страну и узнать о запросах на удаление контента за шесть месяцев.



Twitter обеспечил настоящий прорыв в демонстрации всех полученных требований на удаление контента и их выполнения.

придерживаться политики прозрачности включает не только сообщение о том, когда правительство требует предоставить данные пользователя, но и о том, как часто правительство требует удалить контент или заблокировать учетную запись пользователя, и как часто компания выполняет эти требования. Мы присваиваем звезду в этой категории компаниям, которые регулярно публикуют эту информацию, в своем отчете или в иной столь же доступной форме. Компании должны включать туда официальные законные процессы, а также неофициальные правительственные запросы, поскольку правительственная цензура способна принимать самые разные формы.

5 Общественная политика, направленная на защиту пользователя: противодействие лазейкам. Каждый год мы посвящаем одну категорию состоянию опубликованной политики компании. Уже три года мы воздаем должное компаниям, которые открыто содействуют обновлению и реформированию Закона о защите конфиденциальности электронных коммуникаций. В прошлом году мы отметили компании, открыто противостоявшие массовой слежке. В этом году, принимая во внимание яростные дебаты насчет шифрования, мы просим компании занять ясную позицию противодействия вынужденному включению уязвимостей в системе безопасности или иных вынужденных лазейках. Эта позиция может быть выражена в блоге, в отчете, посредством подписания коллективного письма или в ином общественном, официальном, письменном формате. Мы рассчитываем, что эта категория будет развиваться, чтобы мы могли следить за поведением предприятий в решении ряда важных вопросов защиты конфиденциальности.

› Полные результаты ежегодного отчета EFF отражают весьма неутешительный результат работы популярного сервиса обмена сообщениями, WhatsApp.

	Следует индустрии, избирая лучшие практики	Сообщает о запросах правительства на данные	Публикует свою политику хранения данных	Сообщает о запросах правительства на удаление	Публично за пользователя: противодействие лазейкам
Adobe	★	★	★	★	★
amazon.com	★	☆	☆	★	★
Apple	★	★	★	★	★
at&t	★	☆	☆	N/A	☆
COMCAST	★	☆	★	N/A	★
CREDO mobile	★	★	★	★	★
Dropbox	★	★	★	★	★
facebook	★	★	★	☆	★
Google	★	☆	☆	★	★
LinkedIn	★	★	★	☆	★
Microsoft	★	★	☆	☆	★
Pinterest	★	★	☆	★	★
reddit	★	★	★	★	☆
slack	★	☆	★	★	★
snapchat	★	☆	★	N/A	★
SONIC.	★	★	★	★	★
tumblr.	★	★	☆	☆	★
Twitter	★	☆	★	★	★
verizon	★	☆	☆	★	☆
WhatsApp	☆	☆	☆	N/A	★
WICKR	★	★	★	N/A	★
WIKIMEDIA	★	★	★	★	★
WordPress.com	★	★	★	★	★
YAHOO!	★	★	★	★	★

> «Техноиндустрия против проникновения правительства с черного хода.»

Хороший, плохой, злой

Мы рады сообщить, что девять компаний заслужили звезды в каждой доступной для них категории (см. справа). Следует также отметить, что некоторые компании размещают очень малый объем контента или не размещают его вообще, и поэтому политика прозрачности по поводу правительственных запросов на удаление данных может не иметь к ним отношения. Эти компании демонстрируют, что для основных технологических компаний практично применять лучший опыт по поводу прозрачности и вставать на сторону пользователя, когда к нему пытается вломиться правительство. К сожалению, не все компании применяют столь дальновидную практику. Две основных телекоммуникационных компании — Verizon и AT&T — продемонстрировали особенно плохие результаты, продолжив, таким образом, тенденцию, которую мы определили в предыдущих отчетах: крупные телекоммуникационные провайдеры отстают от остального технологического сектора.

Примечательно, что некоторые компании, выступающие в роли интернет-провайдеров, и провайдеры телекоммуникационных услуг лидируют в области проведения сильной политики по защите прав пользователей. В частности, Credo и Sonic снова были отмечены в каждой категории. Comcast слегка им уступает, заработав 3 из 4 возможных звезд. Надеемся, за будущие годы остальные телекоммуникационные компании смогут дотянуться до этих стандартов.

Кроме того, ясно, что техноиндустрия дружно противится узаконенному проникновению правительства с черного хода. Мы обнаружили, что из 24 оцениваемых нами компаний 21 сделал публичное заявление против лазеек, которые ослабляют систему безопасности и угрожают конфиденциальности пользователя. Интернет-провайдеры, провайдеры облачного хранения, webmail и социальных сетей единодушно противостоят санкционированному властями ослаблению системы безопасности.

Лучший опыт

Эти стандарты разрабатывались в течение четырех лет составления отчетов EFF, и они охватывают три основных проблемы в «Кто прикрывает вам спину?»: требование наличия ордера перед передачей пользовательского контента, публикация регулярных отчетов и инструкций по соблюдению законодательства. Последние помогают пользователям понять, как часто и при каких обстоятельствах компании соглашаются на требования правительства о предоставлении данных, а наличие ордера на изъятие контента обеспечивает юридическую поддержку до передачи данных правоохранительным органам.

В 2011 г. ни одна компания не получила награды во всех этих категориях. В этом году 23 из 24 компаний в нашем отчете внедрили эти принципы. Очевидно, этот лучший опыт действительно воспринят технологической индустрией; однако WhatsApp весьма заметно отстает.

Уведомление пользователей

В этом году мы попросили компании не просто обещать уведомлять пользователей о запросах правительства на предоставление данных, а сделать нечто большее: уведомлять пользователей заранее, до передачи данных властям. В случаях, когда

Беглецы Linux

Отчет EFF касается США, но, поскольку немалая часть населения Земли использует сервисы, размещающиеся в США, он затрагивает большинство из нас. Как сторонник открытого кода, среднестатистический читатель *Linux Format* гораздо лучше знаком с вопросами конфиденциальности и подготовлен к принятию мер по этой проблеме. Мы уже рассказывали о постоянно улучшающемся *OwnCloud* [см. Учебники, **LXF190**] и видели, как легко создать собственную систему сотрудничества и разделенного доступа к документам на основе облака.

Это означает возможность создания собственных средств избежать корпоративных правил, постановлений и проблем конфиденциальности. Реальность такова, что не все на это способны, и в наших интересах, чтобы компании, предлагающие онлайн-услуги, могли защитить нас всех, не прогибаясь перед требованиями властей. Или, как минимум, сообщать людям о том, как хранятся их данные, и когда — если это происходит — доступ к ним выдается властным структурам.

Число облачных сервисов будет расти, как и объем хранимых там данных. **LXF** будет следить за новыми возможностями облака с открытым кодом, по мере появления таких новых сервисов, как www.onlyoffice.com.

› Запуск собственного сервиса облачного хранения с помощью *OwnCloud* — один из способов обезопасить свою конфиденциальность.

компаниям запрещалось это делать, мы попросили компании пообещать предоставить уведомление по окончании чрезвычайной ситуации или снятия запрета. Поскольку мы осознавали, что реализация подобной практики потребует от компании значительных изменений в инжиниринге и системе работы, мы уведомили их о том, что этот критерий будет включен в отчет 2015 г., более чем за год.

Две компании, Google и Twitter, которые наш прошлый отчет одобрил за сообщения пользователям о запросах правительства на предоставление данных, в этом году не были отмечены, поскольку у них нет политики уведомления пользователей по окончании чрезвычайной ситуации или снятии запрета.

Из 24 компаний, которые мы оценивали, 15 соответствовали этому более строгому критерию, и мы рады видеть, что индустрия развивается в должном направлении. Особенно нас впечатлила строгая политика, практикуемая Dropbox, которая заявляет следующее:

«Политика Dropbox заключается в предоставлении пользователям уведомлений о запросах правоохранительных органов на предоставление их информации до исполнения этого запроса, если это не запрещено законом. Мы можем задержать предоставление такого уведомления при угрозе жизни или нанесения телесных повреждений или эксплуатации детей».

Политика хранения данных

В этом году мы впервые расширили оценку наших компаний, выясняя, прозрачна ли их политика по поводу удаленных данных, которые они продолжают хранить. Очень часто пользователи не подозревают, что удаленные ими данные продолжают храниться у провайдера услуг электронной почты или социальных сетей и могут быть предоставлены правоохранительным органам по их запросу.

Прозрачность — это первый шаг на пути просвещения пользователей по вопросу судьбы их удаленных данных, и мы оцениваем компании по их политике прозрачности в данной категории. Учтите, что мы не предъявляем каких-то особых требований, чтобы компания удаляла данные через определенное время. На самом деле некоторые компании открыто заявляют, что продолжают поддерживать удаленные данные и журнал сервера бесконечно — подобная практика, по нашему мнению, ужасна для пользователей. Однако для данного отчета мы просто просим компании указать срок хранения ими удаленных данных, которые не могут быть легко просмотрены пользователем (включая IP-адреса и данные DHCP), а также удаленного пользователем контента.

И снова мы увидели 15 компаний из 24, оцениваемых нами, достойных награды в этой категории. Особенно нас впечатлила ясность и подробность информации, предоставленной Comcast. Эта компания ведет хронологические подробные записи о звонках для телефонной службы Xfinity Voice в течение двух лет. Сюда входят записи о местных, международных и междугородних звонках. В ограниченном числе случаев более старые записи тоже могут быть доступны, но на их предоставление потребуется дополнительное время и ресурсы. Более подробную информацию по их политике хранения данных вы найдете в Comcast Law Enforcement Handbook на http://bit.ly/LXFitsthelaw.

Противостояние лазейкам

Одна из основных тенденций, которую мы наблюдаем по всей техноиндустрии — яркое неприятие ослабления системы безопасности, санкционированное властями. Фактически, из 24 компаний, которые мы оценивали, 21 заняли четкую публичную позицию противодействия использованию лазеек. Это мощное заявление со стороны технологического сообщества, которое стоит принять во внимание и Конгрессу, и Белому Дому. Многие компании подписали письмо, организованное Институтом открытых технологий [Open Technology Institute], который выступает против умышленного ослабления системы безопасности, говоря:

«Мы настоятельно просим вас отклонять любые предложения для компаний США, которые умышленно ослабляют безопасность наших продуктов... Называйте их «парадным входом» или «черным ходом», введение намеренных уязвимостей в безопасный продукт для использования властями сделает этот продукт менее защищенным от других злоумышленников. Все эксперты по компьютерной безопасности, открыто выступившие по этому вопросу, согласны с этим, в том числе и собственно правительственные эксперты».

Выводы EFF

Мы рады отметить, что основные технологические компании конкурируют в борьбе за защиту конфиденциальности и прав пользователей. Практические меры, поощряющие политику прозрачности в отношении запросов правительства на предоставление данных пользователей становятся мерами по умолчанию для компаний по всей Сети. И хотя мы можем оценить лишь небольшой сегмент технической индустрии, мы полагаем, что все это свидетельствует о сдвиге в целом. Возможно, в ответ на непрекращающиеся дебаты по поводу правительственной слежки и на рост общественного внимания к этим вопросам, все больше и больше компаний добровольно и открыто сообщают о правительственных запросах на предоставление данных и дают пользователям инструменты для принятия ответных мер.

Мы полагаем, что подобного рода прозрачность может способствовать более широкому обсуждению и систематическим изменениям в вопросе того, как и когда власти могут получать доступ к пользовательским данным, и в конечном итоге сподвигнуть Конгресс на уточнение и улучшение законов о защите конфиденциальности цифровых данных. Мы также признаем, что технологические компании способны знать о растущих правительственных запросах и сопротивляться им, поэтому нам надо сделать все возможное, чтобы помочь им открыто высказываться и оказывать противодействие. Передавая свои данные этим компаниям, мы налагаем на них большую ответственность сделать все возможное для защиты конфиденциальности. И мы счастливы, что многие из тех компаний, которые мы оценивали, стараются справиться с этой задачей. LXF