Александра Куликова
Независимый исследователь,
магистр наук в области управления медиа и коммуникациями,
Лондонская школа экономики и политических наук

15 апреля 2014 г.

Отчет о прозрачности и политика конфиденциальности ИКТ-корпораций до и после разоблачений Сноудена

«Отчет о прозрачности» (ОП), или *transparency report*, как формат отчетности возник на пересечении существующих стандартов корпоративной отчетности и тенденций развития в области информационных и коммуникационных технологий, в результате которых крупнейшие интернет-компании оказались хранителями огромной массы данных пользователей сети Интернет. Стремительный рост глобальных операторов интернет-сервисов – поисковых машин, социальных сетей, телеком-компаний – в сочетании с конвергенцией в медиа-индустрии и развитием сервисов Web 2.0 позволил им построить централизованную систему данных о пользователях и ими произведенного контента (UCG). Относительная олигополия ряда таких операторов (всемирно известные интернет-гиганты Google, Facebook, Yahoo, Microsoft, Twitter и др.) означает эксклюзивный доступ к этой системе, в которой сами пользователи выступают добровольными *со-создателями* в результате принятия пользовательских соглашений при открытии аккаунтов в сервисах.

Такое господство в индустрии, которая строит бизнес на использовании данных пользователей для целевой контекстной рекламы, с одной стороны, предполагает большую долю ответственности со стороны компаний в отношении обеспечения сохранности и приватности данных пользователей. С другой стороны, оно ставит их в уникальное положение централизованного контроля огромного количества информации об экономически и социально-политически активных граждан по

всему миру. Такая инфраструктура не могла не остаться незамеченной спецслужбами безопасности ряда стран мира. Интернет-компании встроены в систему отчетности службам безопасности различных стран через механизмы предоставления данных о пользователей в рамках ОРД. Треугольник взаимоотношений между пользователями, частным сектором и государствами, таким образом, был дополнен ОП как форматом раскрытия информации о запросах таких данных со стороны правоохранительных органов в адрес конкретных компаний-агрегаторов данных. При этом раскрытие информации по запросу служб обязательно в соответствии с законодательством большинства стран, тогда как отчетность перед пользователями/гражданами является инициативой саморегулирования в рамках корпоративной ответственности.

Однако лишь летом 2013 г. жанр ОП получил ощутимый толчок к эволюции до отраслевого стандарта, благодаря разоблачениям программ электронной слежки Агентством Национальной Безопасности США.

Отчет доброй воли

Как во многих других технологиях и подходах в области интернет-бизнеса, пионером ОП был Google. Возникновение самой идеи такого продукта связано с попытками компании выйти на китайский рынок без ущерба для принципов ведения бизнеса. Практика фильтрации онлайн-контента и блокирования URL и целых сайтов с неугодным содержанием (пресловутый *firewall*), вынудила компанию свернуть бизнес в континентальном Китае в 2010 г., что в свою очередь стало предпосылкой к участию (вместе с Microsoft и Yahoo) в основании Global Network Initiative, организации продвигающей защиту прав человека в киберпространстве. Это также поспособствовало рождению идеи ОП, что, кстати, произошло в рамках тех самых 20% рабочего времени, которые сотрудники компании могут тратить на собственные проекты.

Статистика запросов государств о данных пользователей сервисов Google, а также о снятии или блокировании контента в случае нарушения авторских прав и прочего внутреннего законодательства была впервые опубликована в 2010 г. за отчетный период июль-декабрь 2009 г. С тех пор функциональность, интерактивность и детализация продукта постоянно развивались. Неизменным оставался принцип правовой экспертизы поступающих запросов относительно существующего законодательства в соответствующих странах, равно как и ограничения по типу и количеству раскрываемых данных (США). Тем не менее, в июле 2012 г. эту практику ввел Twitter, выпустив практически идентичный на тот момент по формату продукт (период отчетности и категоризация раскрываемых запросов) под тем же названием transparency report.Microsoft присоединился к инициативе в марте 2013 г., выпустив свой Law Enforcement Requests Report. На тот момент, при своем новаторстве в области корпоративного управления, продукт оставался нишевым, интересным прежде своего профессионалам в отрасли и правоохранительным органам. Кроме того, едва ли было в интересах самих компаний привлекать повышенное внимание к самой теме доступа властей к персональным данным.

Однако разоблачения Сноудена привлекли к ОП более широкий интерес, так как, по понятным причинам, прозрачность поведения интернет-гигантов, равно как и американского АНБ, неожиданно оказались в фокусе внимания общественности.

Как известно, первые публикации о повсеместной слежке АНБ, выпущенные The Guardian и The Washington Post в июне 2013 г. предполагали, что спецслужбы имеют прямой доступ к данным пользователей крупнейших телеком- и интернет-компаний – Apple,Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype и YouTube – не только на законных основаниях по решению суда, но и в обход существующих практик через так называемый *backdoor* доступ. Последующие публикации уточнили, что службы располагают технологиями, позволяющими доступ к данным пользователям на корпоративных серверах и без ведома самих компаний, но первоначальный репутационный ущерб (безотносительно того как на самом деле выстраиваются отношения между службами безопасности и компаниями) был значительный. Компании, упомянутые в первоначальной публикации, поспешили выступить с опровержениями (формулировка которых была очень схожей). В ситуации, когда доверие пользователей могло чревато отразиться на бизнесе компаний, на первый план вышла именно внутрикорпоративная практика управления данными пользователей, а слово transparency вышло на первые полосы. Те операторы, которые на тот момент уже выпускали ОП, оказались в более выгодной ситуации с «козырем» в руках, демонстрирующим их приверженность защите пользовательской информации от несанкционированного доступа. Те, кто его не имел, и в первую очередь Facebook и Yahoo, опубликовали разовую отчетность за последние полгода, а также заявили о возможности тоже начать такую практику на постоянной основе.

Facebook опубликовал свой первый Global Government Requests Report 27 августа 2013 г., Yahoo опубликовал свой первый Transparency Report 6 сентября 2013 г. С осени 2013 г. к этой практике присоединился Apple, а зимой 2014 года также впервые телеком операторы – американские Verizon и AT&T, австралийский Telstra и другие. Пока не заостряя внимание на содержании отчетов и сопоставимости данных, можно отметить, что название, формат и принципы создания этого продукта аналогичны и соответствуют подходу «пионера» Google. Таким образом, можно говорить о рождении нового стандарта корпоративной ответственности в области ИКТ-сектора, развитие которого во многом подхлестнули разоблачения Сноудена. Однако стоит обратить внимание не только на обстоятельства развития, а также и популяризации ОП, но и на эволюцию методики его составления, что во многом определяет его истинный смысл и назначение.

Раскрыть нельзя утаить

Каждая из компаний, выпускающих ОП, описывает процедуру обработки и ответа на запросы властей, подчеркивая необходимость судебного ордера на выдачу такой информации, а также тщательный анализ запросов на соответствие законодательству страны-заявителя. Например, после принятия «антипиратского

закона» в РФ общее количество российских запросов на снятие контента выросло в разы, как и число удовлетворенных запросов – при наличии законного основания.

Также в последнем ОП Google отмечает рост числа запросов властей о данных пользователей по всему миру на 120% за все время отчетности (с 2009 г.). Разница в их количестве от разных странах отражает и популярность используемых сервисов среди населения. Так, например, за отчетный период с июля по декабрь 2013 г. Google получил 90 запросов о раскрытии данных от российских властей по 202 аккаунтам, из которых было удовлетворено лишь 3%. Для сравнения, за тот же период от США поступило 10 574 запроса по 18 254 аккаунтам, из которых было выдано 83% данных.

В отношении статистики запросов по данным пользователей пример США в отчете Google особенно показателен – во-первых, потому что компания работает под американской юрисдикцией по всему миру и имеет основную массу пользователей в США. А во-вторых, потому что именно выступление Эдварда Сноудена приковало широкое внимание к типологии запросов со стороны США, некоторые из которых не могли быть отражены в ОП по закону. Помимо стандартных запросов, направляемых по решению суда в порядке уголовного делопроизводства, существует также типология писем-запросов биллинговой информации от операторов связи (телеком и интернет) по вопросам национальной безопасности (National Security Letters), поступление которых компании хранили в секрете в соответствии со своими обязательствами перед спецслужбами. Только в марте 2013 г. было разрешено опубликовать агрегированное количество таких запросов за полугодовой период и лишь в виде диапазона в 1000 штук.

Однако лишь после утечки информации о тотальной слежке АНБ уже в феврале 2014 г. в результате исков против американских властей по факту электронной слежки, интернет-гигантам (Google, Facebook, Yahoo, Microsoft) удалось пролоббировать также разрешение на частичную публикацию запросов в соответствии с Законом о надзоре за иностранной разведкой (запросы FISA). Этот закон, принятый в 1978 г. и регламентирующий контрразведывательную деятельность американских спецслужб, не раз дополнялся поправками после трагедии 11 сентября 2001 г. – прежде всего Патриотическим Актом (US Patriot Act) 2001 г., расширяющим полномочия этих служб при сборе информации о не-американцах с учетом современных технических коммуникационных возможностей. Поправка 2008 г. (FISA Amendment Act) выводит эти полномочия за пределы страны при условии их применения к не-американцам (приватность американских граждан защищена 4-й поправкой Конституции США). Это значит, что спецслужбы США имеют легальные основания в соответствии с американским законом осуществлять электронную слежку за гражданами всего мира с целью обеспечения национальной безопасности США. Такая размывчатая формулировка позволяет применять ее буквально повсеместно.

Именно такая законодательная база практически дала спецслужбам США легальные основания применять программы перехвата коммуникаций типа *PRISM,*

XKeyScore и *Stuxnet* для доступа к интернет- и телеком- трафику и данным пользователей интернет-сервисов по всему миру – помимо уже существующей практики формальных запросов FISA. Британский аналог FISA – закон RIPA (Regulation of Investigatory Powers Act 2000) – позволяет такой же перехват коммуникационных данных (и метаданных, и контента) Штабу правительственных служб связи (GCHQ) с помощью программы *Tempora*, а также трафика с трансатлантических волоконно-оптических кабелей. А в рамках действующего еще со времен Второй мировой войны кооперации *альянса «пяти глаз»* (США, Великобритания, Канада, Австралия, Новая Зеландия), это означает совместную слежку и обмен информацией по коммуникациям практически по всему миру, причем в дополнение к имеющимся формальным инструментам получения информации.

Отчет о непрозрачности?

Возникает вопрос, насколько на самом деле значима статистика, представленная в ОП, на фоне продолжающейся борьбы частного сектора и общественных организаций за изменение подхода к сбору и хранению данных о гражданах властями различных стран, и США в первую очередь. Если говорить о полноте публикуемых данных, а также об их сути, что именно говорят рядовому пользователю эти цифры? Какие за ними стоят конкретные расследуемые дела, по которым требуется выдача персональных/коммуникационных данных? И кому это важно?

Прежде всего, естественно, это важно компаниям, от политики прозрачности которых зависит их собственный бизнес и удержание базы пользователей. Озабоченность доверием граждан и желание предоставить как можно более детализированную и понятную информацию о запросах властей по пользовательским данным отметили представители Google, Microsoft, Yahoo и Facebook в интервью в августе 2013 г., подтвердив свою приверженность принципу соблюдения права на частную жизнь. Все четыре компании состоят в Global Network Initiative и недавно прошли ее внутренний аудит на соблюдение прав человека (уже после того как Facebook и Yahoo также выпустили ОП). Они также отметили, что планка, заданная Google в области отчетности по запросам о данных пользователей, действительно теперь видится обязательной для большинства игроков в области ICT (телеком компании также начали присоединяться к практике ОП), и внутрисекторальная конкуренция будет подталкивать все больше компаний к этой практике, несмотря на ее несовершенство. Также постепенно будет расти импульс к улучшению гранулярности этой отчетности на фоне повышенного внимания к существующим практикам тотальной, непропорциональной слежки за гражданами всего мира, несовместимым с понятиями западного демократического общества. Морально-правовые основания для дальнейшего лоббирования к законодательным изменениям уже показали некоторые результаты, что касается деклассификации статистики некоторых запросов: можно предположить, что практика ОП как часть более интенсивного прессинга со стороны частного сектора на власти сыграла не последнюю роль. Как отметили некоторые интервьюируемые,

на данный момент частные компании в некотором роде выполняют работу, которую должны выполнять сами власти.

Практика ОП – это, с одной стороны, прежде всего, PR-инструмент, и его ускоренная эволюция только подтверждает первичность задач избежать последствий кризиса доверия пользователей. Хотя эти последствия – тема отдельного разговора: разоблачения Эдварда Сноудена, конечно, вызвали огромный резонанс, но едва ли можно пока говорить о значимой потере доверия. Вернее, пока она не выражается в тотальном закрытии аккаунтов пользователей в соответствующих сервисах. С другой стороны, уже есть некоторые данные о самоцензуре, особенно в профессиональной писательской среде, и осознание все большей размытости самого понятия приватности в цифровом веке со временем должно оказать воздействие на поведение различных социальных и возрастных групп. И в целом надо сказать, что сам выход ОП из нишевой плоскости в область более широкого общественного внимания означает трансформацию контекста, в котором ведется дискуссия о балансе задач национальной безопасности различных стран и соблюдением права на частную жизнь и сохранность персональных данных граждан. Он вводит новые термины и понятия для определения ответственности и отчетности как крупных компаний, владеющих технологиями эффективной аккумуляции данных граждан, так и соответствующих отраслей властей о доступе и использовании таких данных.

А если такой дискуссии нет? В России формат ОП пока остается нежизнеспособен. Прежде всего, в силу его бессмысленности: разница обработки запросов по судебному ордеру и без него нечеткая, а власти и так имеют необходимый доступ к интересующим их данным в соответствии с законодательством и техническим функционалом СОРМ. Но, пожалуй, ключевая проблема состоит в отсутствии такого запроса и ожиданий со стороны граждан и институтов гражданского общества. В результате формат отчета о прозрачности, который мог бы стать эффективным инструментом корпоративного саморегулирования – и, в конечном счете, общественного блага, остается невостребован своей целевой аудиторией.