НЕОБХОДИМОСТЬ И ПРОПОРЦИОНАЛЬНОСТЬ

МЕЖДУНАРОДНЫЕ ПРИНЦИПЫ ПО СОБЛЮДЕНИЮ ПРАВ ЧЕЛОВЕКА ПРИ ИСПОЛЬЗОВАНИИ СЛЕЖКИ В КОММУНИКАЦИЯХ

ОБ АВТОРАХ

Международные принципы в области прав человека при использовании слежки в коммуникациях – результат совместной работы ряда организаций и экспертов в области неприкосновенности частной жизни со всего мира, включая (но не ограничиваясь) Access, Article 19, Asociación Civil por la Igualdad y la Justicia, Asociación por los Derechos Civiles, Association for Progressive Communications, Bits of Freedom, Center for Internet & Society India, Comisión Colombiana de Juristas, Electronic Frontier Foundation, European Digital Rights, Reporter Without Borders, Fundación Karisma, Open Net Korea, Open Rights Group, Privacy International, а также Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. Кроме того, мы хотим поблагодарить IP Justice, SHARE Foundation - SHARE Defense, IFEX Network и Instituto NUPEF за помощь в координации наших усилий.

Более подробная информация здесь:
necessaryandproportionate.org/text

ПРЕДЫСТОРИЯ

Более сорока экспертов в области приватности и безопасности участвовали в подготовке чернового варианта Принципов на встрече в Брюсселе в октябре 2012 года. После консультаций с широким кругом коллег, в том числе на второй встрече в Рио-де-Жанейро в декабре 2012 года, Access, EFF и Privacy International возглавили работу по получению экспертных мнений от специалистов в области прав человека и цифровых прав по всему миру. Первая версия Принципов была готова 10 июля 2013 года и официально представлена на Совете по правам человека ООН в Женеве в сентябре 2013 года. Принципы имели успех и были поддержаны более чем 400 организациями из разных стран. Это потребовало внесения в текст ряда поправок, в основном второстепенных, стилистических, чтобы обеспечить общность интерпретаций Принципов и их применимость в различных юрисдикциях. С марта по май 2013 года проводились дополнительные консультации для выявления этих стилистических недостатков и их исправления. Изменения не затронули сущность и цели Принципов. В данном документе приводится окончательный результат описанной работы, официальный текст Принципов.

Международные принципы по соблюдению прав человека при использовании слежки в коммуникациях

ОКОНЧАТЕЛЬНАЯ ВЕРСИЯ, май 2014 года*

По мере развития технологий государственной слежки в коммуникациях государства оказываются не в состоянии обеспечить соответствие законов, правил, деятельности, полномочий и органов власти, связанных со слежкой в коммуникациях, международным соглашениям и стандартам в области прав человека. В этом документе сделана попытка прояснить, как международное право в области прав человека соотносится с современной цифровой средой, в частности с учетом роста и изменений в технологиях и способах слежки. Данные Принципы могут помочь организациям гражданского общества, бизнесу, государствам и прочим институтам оценить, соответствуют ли действующие или предлагаемые законы и практики слежки правам человека.

Настоящие принципы – результат консультаций с гражданскими организациями, бизнесом и международными экспертами в сфере законодательства о слежке в коммуникациях, политики и технологий по всему миру.

ПРЕАМБУЛА

Право на неприкосновенность частной жизни (приватность) является одним из основных прав человека и краеугольным камнем при строительстве демократического общества. Приватность крайне важна для обеспечения человеческого достоинства и усиливает другие права, такие как свободу слова, право на доступ к информации, свободу ассоциаций.[1] Приватность признана международными соглашениями в области прав человека. Слежка в коммуникациях нарушает некоторые права человека, включая приватность. Таким образом, слежка может быть оправдана только если её предписывает закон, если она необходима для достижения законной цели и пропорциональна этой цели.[2]

До того, как в обществе стал популярен интернет, государственную слежку в коммуникациях сдерживали устоявшиеся принципы в законодательстве и внутренние формальные ограничения самих способов слежки. В последние десятилетия эти формальные барьеры понизились, а применимость юридических принципов в новом технологическом контексте стала неясной. Взрывной рост цифровых потоков информации, данные о коммуникациях отдельного человека и о том, какие электронные устройства он использует, резкое удешевление хранения и обработки данных, передача персональной информации через провайдеров услуг (третьих лиц) – все это сделало государственную слежку в коммуникациях возможной в невиданном до сих пор масштабе.[3] Между тем принципы существующих законов в области прав человека не приведены в соответствие с современными технологиями и способами государственной слежки в коммуникациях, возможностями государства сопоставлять и организовывать данные, полученные с помощью разных технологий и способов слежки, а также увеличением объема доступных данных деликатного характера.

Интенсивность, с которой государство ищет доступ к коммуникациям и к метаданным, резко возросла, но проблема остается слабо изученной.[4] Коммуникационные метаданные могут образовывать досье на человека, включая состояние здоровья, политические и религиозные взгляды, связи, контакты и интересы. Метаданные раскрывают не меньше подробностей о человеке, чем само содержание коммуникаций. Метаданные обладают значительным потенциалом вторжения в жизнь человека и негативного влияния на политические и прочие ассоциации.[5] Несмотря на это, законы, правила, полномочия и органы власти часто обеспечивают коммуникационные метаданные более низким уровнем защиты и не вводят достаточных ограничений на соответствующее использование метаданных государством.

ОБЛАСТЬ ПРИМЕНЕНИЯ

Принципы и преамбула обладают целостностью и соотносятся сами с собой. Каждый принцип и преамбулу следует читать и воспринимать как часть более ёмкой структуры. Все вместе они выполняют одну задачу: обеспечивать соответствие законов, правил и действий, связанных со слежкой в коммуникациях, международному законодательству и стандартам в области прав человека и адекватно защищать права каждого человека, такие как приватность и свободу слова. Чтобы государство могло на самом деле выполнять свои международные обязательства в области прав человека в связи со слежкой в коммуникациях, оно должно следовать каждому из принципов, изложенных ниже.

Эти принципы относятся к слежке как в границах государства, так и за его пределами. Принципы применяются вне зависимости от задачи слежки, будь то работа правоохранительных органов, защита национальной безопасности, сбор разведывательных данных или иная государственная деятельность.

Принципы также относятся к обязанности государства уважать и претворять в жизнь права человека, защищать эти права от посягательств третьих сторон, включая коммерческий сектор.[6] Коммерческие организации несут ответственность за уважение приватности и других прав человека, особенно учитывая ключевую роль этих структур в создании, развитии и распространении технологий, предоставлении услуг связи, выполнении определённых действий по слежке в пользу государства. Тем не менее, когда речь идет о слежке в коммуникациях, Принципы подчеркивают обязанности и ответственность государства.

ТЕХНОЛОГИЧЕСКИЙ ПРОГРЕСС И ОПРЕДЕЛЕНИЯ

В современном мире понятие «слежка в коммуникациях» охватывает мониторинг, перехват, сбор, получение, анализ, использование, хранение, защиту, вмешательство, доступ или иные действия с информацией, которая включает, отражает, возникает из или рассказывает о коммуникациях человека в прошлом, настоящем или будущем.

Под «коммуникациями» понимаются действия, взаимодействие и передача данных средствами электронной связи. Речь может идти о содержании сообщений, личностях участников коммуникаций, данных об их местонахождении, времени и продолжительности коммуникаций, данных, содержащих IP-адреса, а также идентифицирующих признаках коммуникационного оборудования.

«Защищённой информацией» считается информация, которая включает, отражает, исходит от или рассказывает о коммуникациях человека при условии, что эта информация не подготовлена для раскрытия и к ней не осуществляется

легкий публичный доступ. Традиционно инвазивный характер слежки в коммуникациях ранее оценивался на основе искусственных и формальных категорий. Действующие законы разделяют понятия «содержание» и «не-содержание», «информация о подписчике» и «метаданные», хранящиеся и передаваемые данные, данные, которые хранятся дома, и данные, которые хранятся у третьей стороны – провайдера услуг.[7] Но это разделение более не подходит для измерения степени возникающего в результате слежки в коммуникациях вторжения в частную жизнь человека и связанных с ним людей. Уже давно было признано, что содержание коммуникаций нуждается в серьёзной защите закона, поскольку велик риск раскрытия данных деликатного характера. В наше время становится ясно, что прочие данные, связанные с коммуникациями – метаданные и иные формы данных, не относящихся к содержанию – могут раскрывать больше информации о человеке, чем содержание коммуникаций, а значит, эти данные требуют такой же защиты. Сегодня каждый из этих видов данных, рассматриваем ли мы его индивидуально или анализируем вместе с другими, может раскрывать личность человека, его поведение, связи, физическую форму или состояние здоровья, расу, цвет кожи, сексуальную ориентацию, национальность или взгляды. Также эти данные могут сделать возможным определение местонахождения человека, его перемещений или взаимодействия с другими людьми на протяжении определённого времени[8] или с теми, кто находится в определённом месте, например, на публичной демонстрации или ином политическом мероприятии. Таким образом, защищённая информация должна быть обеспечена самым высоким уровнем законодательной защиты.

Оценивая инвазивность слежки в коммуникациях, необходимо принимать во внимание как потенциал слежки в раскрытии защищённой информации, так и

цель сбора информации государством. Всякая слежка в коммуникациях является нарушением прав человека, и к ней применимы международные соглашения в области прав человека. Слежка в коммуникациях, которая, предположительно, приведет к раскрытию защищённой информации и как следствие, подвергнет человека риску стать объектом расследования, дискриминации или нарушения его прав, представляет собой серьезное вторжение в частную жизнь этого человека и подрывает его возможность пользоваться другими основными правами, включая свободу слова, свободу ассоциаций и участие в политическом процессе. Причина в том, что перечисленные права подразумевают свободное общение людей без давящего эффекта государственной слежки. Поэтому в каждом случае необходимо определять как характер сбора информации, так и ее потенциальное использование.

Одобряя новые методы слежки в коммуникациях или расширяя масштаб использования существующих методов, государство должно еще до начала сбора данных выяснить, попадает ли интересующая его информация в категорию защищённой информации. Для этого используются судебные органы или иной демократический механизм надзора. При рассмотрении вопроса об отнесении информации, получаемой с помощью слежки в коммуникациях, к категории защищённой информации, форма, объем и продолжительность слежки считаются взаимосвязанными факторами. Подробный или систематический мониторинг или иная инвазивная технология, используемая в целях слежки в коммуникациях, обладает потенциалом раскрывать приватную информацию значительно в большем масштабе, чем задумывается изначально. Это может поднять слежку за незащищённой информацией на такой уровень, что потребуется её полная защита, как для защищённой информации.[9]

Решение, может ли государство вести слежку в коммуникациях в отношении защищённой информации, должно приниматься в соответствии с представленными ниже принципами.

13 ПРИНЦИПОВ

13 ПРИНЦИПОВ

ЗАКОННОСТЬ

Всякое ограничение прав человека должно происходить в соответствии с законом. Государство не должно одобрять или осуществлять меры, которые вторгаются в сферу этих прав, если отсутствует действующий и публично доступный законодательный акт, соответствующий критериям ясности и точности. Этот законодательный акт должен быть таким, чтобы люди были о нем предупреждены и могли предвидеть последствия его применения. Учитывая темпы изменений в технологиях, законы, ограничивающие права человека, должны периодически пересматриваться в области законотворчества или правоприменения с участием всех заинтересованных сторон.

ЗАКОННОСТЬ ЦЕЛИ

Законы должны позволять слежку в коммуникациях только определённым государственным органам для достижения законных целей. Эти цели должны соответствовать основополагающим законным интересам, которые необходимы в демократическом обществе. Никакая мера не должна применяться способом, вызывающим дискриминацию по расе, цвету кожи, полу, языку, религиозным, политическим или иным воззрениям, национальности, социальному происхождению, имущественному положению, рождению и другим статусам.

НЕОБХОДИМОСТЬ

Законы о слежке, правила, правоприменение, полномочия и органы власти должны быть четко ограничены необходимостью достижения законной цели. Слежка в коммуникациях должна проводиться

только в том случае, если она оказывается единственным способом достижения законной цели. Если способов несколько, слежка применяется лишь в том случае, когда она меньше всего нарушает права человека. Ответственность за эту оценку всегда лежит на государстве.

СООТВЕТСТВИЕ ЦЕЛИ

Каждый разрешённый законом случай слежки в коммуникациях должен соответствовать конкретной, идентифицируемой и законной цели.

ПРОПОРЦИОНАЛЬНОСТЬ

Слежка в коммуникациях должна рассматриваться как существенное нарушение прав человека и создание угрозы основам демократического общества. Решения о проведении слежки в коммуникациях должны иметь в виду деликатный характер информации, к которой будет получен доступ, а также серьезность нарушения прав человека и других сопоставимых по значимости интересов.

До начала слежки в коммуникациях с целью исполнения закона, защиты национальной безопасности или ведения разведывательной деятельности государство должно, как минимум, подтвердить компетентному судебному органу выполнение следующих условий:

1) высокая вероятность, в настоящем или в будущем, совершения тяжкого преступления или возникновения конкретной угрозы законной цели;

2) высокая вероятность того, что улики и материалы об этом тяжком преступлении или о конкретной угрозе законной цели могут быть получены благодаря доступу к защищённой информации;

3) прочие инвазивные техники были исчерпаны или оказались бы бесполезны, предложенный вариант наименее инвазивен;

4) полученная информация будет ограничена лишь относящейся к тяжкому преступлению или конкретной угрозе законной цели;

5) всякая избыточная собранная информация не будет храниться, но будет быстро удалена или возвращена;

6) доступ к информации будет осуществляться только тем органом, только с той целью и в течение только того времени, которые указаны в разрешении;

7) мероприятия и методы слежки не подрывают основы приватности или фундаментальных свобод.

КОМПЕТЕНТНЫЙ СУДЕБНЫЙ ОРГАН

Решения, связанные со слежкой в коммуникациях, должны приниматься компетентным, беспристрастным и независимым судебным органом. Этот орган должен соответствовать трем условиям:

1) быть отдельным и независимым от органов, осуществляющих слежку в коммуникациях;

2) быть компетентным в соответствующей теме для принятия юридических решений о законности слежки в коммуникациях, используемых технологиях и правах человека;

3) иметь достаточные ресурсы для выполнения возложенных на него функций.

НАДЛЕЖАЩАЯ ПРАВОВАЯ ПРОЦЕДУРА

Надлежащая правовая процедура требует от государства уважения и соблюдения прав человека путем обеспечения надлежащего изложения в законе, единообразной практики и доступности широкой общественности правовых процедур в области прав человека. В частности, в отстаивании своих прав каждый имеет право на честное и публичное разбирательство в течение разумного времени независимым, компетентным и беспристрастным судом, действующим на законных основаниях,[10] за исключением экстренных случаев, когда существует недвусмысленная угроза человеческой жизни. В таких случаях должны быть приложены усилия для получения разрешения «пост фактум» в течение разумного периода времени. Явные риски утраты или уничтожения улик никогда не должны рассматриваться как достаточные основания для получения разрешения «пост фактум».

УВЕДОМЛЕНИЕ ПОЛЬЗОВАТЕЛЯ

Лица, за коммуникациями которых осуществляется слежка, должны быть уведомлены о принятом в отношении них решении о слежке в коммуникациях. Этим лицам должны быть предоставлены достаточное время и необходимая информация для оспаривания решения или поиска других средств. Лица должны иметь доступ к материалам, приложенным к обоснованию запроса на слежку. Задержка уведомления допускается только при одновременном выполнении следующих условий:

1) уведомление подвергнет серьезному риску задачу, ради которой было получено разрешение на слежку в коммуникациях, или создаст непосредственную угрозу человеческой жизни;

2) разрешение на задержку уведомления дано компетентным судебным органом;

3) после устранения угрозы пользователь, о котором идет речь, получит уведомление установленным компетентным судебным органом способом.

Обязанность уведомления лежит на государстве, но провайдеры должны иметь свободу уведомлять частных лиц о слежке в коммуникациях по своей инициативе или по запросу.

ПРОЗРАЧНОСТЬ

Государство должно обеспечивать прозрачность использования и масштаба, правил, действий, полномочий и органов власти в области слежки в коммуникациях. Государство должно публиковать как минимум обобщённую информацию о точном числе запросов на слежку, которые были одобрены и отклонены, разделяя запросы от провайдеров сервиса и следственных органов, вид слежки, цель слежки и точное число объектов слежки. Государство должно представлять людям достаточную информацию, чтобы те полностью осознавали масштаб, природу и применение законов, разрешающих слежку в коммуникациях. Государство не должно препятствовать провайдерам услуг публиковать информацию об используемых ими процедурах при получении от государства запросов на слежку в коммуникациях, о следовании этим процедурам и об учете государственных запросов на слежку в коммуникациях.

ОБЩЕСТВЕННЫЙ КОНТРОЛЬ

Государство должно иметь механизмы независимого контроля, чтобы обеспечить прозрачность и подотчетность слежки в коммуникациях.[11]

Контрольные механизмы должны иметь следующие полномочия: доступ ко всей потенциально релевантной информации о действиях государства, включая, где это возможно, доступ к секретным и конфиденциальным данным; оценка того, насколько разумно государство использует свои законные полномочия; оценка того, публикует ли государство обстоятельно и аккуратно информацию об использовании и масштабе слежки в коммуникациях в соответствии со своими обязательствами по прозрачности; публикация периодических отчетов и прочей информации, связанной со слежкой в коммуникациях; объявление публичных выводов о законности этих действий, включая степень их соответствия настоящим Принципам. Международные механизмы контроля должны быть допущены в дополнение к любому контролю, который уже осуществляется через другую государственную структуру.

ЦЕЛОСТНОСТЬ КОММУНИКАЦИЙ И СИСТЕМ

С целью обеспечения целостности, безопасности и приватности систем коммуникаций, а также признавая тот факт, что ограничение безопасности в интересах государства почти всегда означает ограничение безопасности в целом, государство не должно принуждать провайдеров услуг, а также поставщиков оборудования и программного обеспечения встраивать функции слежки или мониторинга в свои продукты, собирать либо хранить ту или иную информацию для целей государственной слежки в коммуникациях. Хранение и сбор данных априори никогда не должны рассматриваться как часть деятельности провайдеров услуг. Люди имеют право свободно выражать свое мнение анонимно; следовательно, государство должно воздержаться от идентификации пользователей.[12]

ГАРАНТИИ В ОБЛАСТИ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА

Реагируя на изменения в потоках информации, в технологиях и сервисах коммуникаций, государство может нуждаться в помощи других государств и зарубежных провайдеров услуг. Если слежка в коммуникациях регулируется законами более одного государства, то договора о взаимной правовой помощи и прочие межгосударственные соглашения должны предусматривать применение правовых норм, обеспечивающих наиболее высокий уровень защиты личности. Если государства ищут сотрудничества в целях исполнения закона, должен действовать принцип обоюдного признания соответствующего деяния преступлением. Государства не могут использовать процедуры взаимной правовой помощи и зарубежные запросы относительно защищённой информации, чтобы обойти национальные законодательные ограничения о слежке в коммуникациях. Механизмы предоставления взаимной правовой помощи и прочие соглашения должны быть четко задокументированы, находиться в публичном доступе и соответствовать гарантиям процедурного равенства.

ЗАЩИТА ОТ НЕЗАКОННОЙ СЛЕЖКИ

Государство должно принимать законы, криминализирующие незаконную слежку в коммуникациях, независимо от того, производится она государственным или частным субъектом. Законы должны предусматривать достаточную и значительную гражданскую и уголовную ответственность для нарушителей, защиту информаторов и механизмы возмещения для пострадавших. Законы должны устанавливать, что любая информация, полученная способом, несовместимым с данными принципами, не

допускается в качестве улики и не учитывается в любых процессуальных действиях, как и любая улика, которая основана на такой информации. Государства также должны принимать законы, согласно которым после того, как материал, полученный с помощью слежки в коммуникациях, использован в целях, ради которых предоставлялась информация, этот материал не будет храниться, но будет уничтожен или возвращен тем, к кому он относится.

* Процесс разработки данных принципов начался в октябре 2012 года на встрече более сорока экспертов по безопасности и приватности в Брюсселе. После консультаций с широким кругом коллег, в том числе на второй встрече в Рио-де-Жанейро в декабре 2012 года, Access, EFF и Privacy International возглавили работу по получению экспертных мнений от специалистов в области прав человека и цифровых прав по всему миру. Первая версия Принципов была готова 10 июля 2013 года и официально представлена на Совете по правам человека ООН в Женеве в сентябре 2013 года. Принципы имели успех и были поддержаны более чем 400 организациями из разных стран. Это потребовало внесения в текст ряда поправок, в основном второстепенных, стилистических, чтобы обеспечить общность интерпретаций Принципов и их применимость в различных юрисдикциях. С марта по май 2013 года проводились дополнительные консультации для выявления этих стилистических недостатков и их исправления. Изменения не затронули сущность и цели Принципов. В данном документе приводится окончательная результат описанной работы, который является официальной версией Принципов.

КОНЦЕВЫЕ СНОСКИ

1. Всеобщая декларация прав человека, статья 12; Международная конвенция о защите прав всех трудящихся-мигрантов и членов их семей, статья 14; Конвенция ООН о правах ребенка, статья 16; Международный пакт о гражданских и политических правах, статья 17; региональные конвенции, включая: ст.10 Африканской хартии прав и благополучия ребенка, ст.11 Американской конвенции о правах человека, ст.4 Принципов свободы самовыражения в Африке, ст.5 Американской декларации прав и обязанностей человека, ст.21 Арабской хартии прав человека, ст.21 Декларации прав человека АСЕАН и ст.8 Европейской конвенции о защите прав человека и основных свобод; Йоханнесбургские принципы в области национальной безопасности, свободы выражения и доступа к информации; Кэмденские принципы в области свободы выражения и равенства.

2. Всеобщая декларация прав человека, статья 29; Общий комментарий № 27, принят Комитетом по правам человека в соответствии с пар.4 ст.40 Международного пакта о гражданских и политических правах (CCPR/C/21/Rev.1/Add.9, 2 ноября 1999 г.). См. также Мартин Шейнин (Martin Scheinin), «Доклад специального докладчика ООН по продвижению и защите прав человека и фундаментальных свобод в борьбе с терроризмом», 2009 г. (A/HRC/17/34). См. также Фрэнк Ла Рю (Frank La Rue), «Доклад спецдокладчика Совету по правам человека ООН по вовлечению государств в слежку в коммуникациях на примере прав человека на приватность и свободу мнения и выражения», 2013 г. (A.HRC.23.40 EN).

3. Коммуникационные метаданные могут включать информацию о личности (данные подписчика, данные об устройстве), информацию о контактах (точках отправки и получения информации, особенно это касается просмотренных сайтов, прочитанных книг и прочих материалов, контактных лиц, друзей, членов семьи, знакомых, поисковых запросов, использованных ресурсов), а также данные о местонахождении (место, время, расстояние от других людей). В целом метаданные представляют собой «окно» почти в каждое действие человека в современном мире, в его душевное состояние, область интересов, намерения, самые сокровенные мысли.

4. Например, только в Великобритании число запросов на коммуникационные метаданные ежегодно составляет около 500000. Эти запросы осуществляются в режиме «самоавторизации», то есть правоприменительные органы имеют возможность подтверждать собственные запросы о доступе к информации, находящейся у провайдеров услуг. Между тем, согласно отчетам Google о доступности сервисов и данных, число запросов касательно пользовательских данных только из США выросло с 8888 в 2010

году до 12271 в 2011 году. В Южной Корее в 2011-2012 годах было зарегистрировано 6 миллионов запросов о подписчиках/авторах публикаций ежегодно и около 30 миллионов запросов метаданных в других видах коммуникаций. Почти все запросы были удовлетворены. Данные 2012 года доступны здесь: http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586

5. Примеры можно увидеть в обзоре Сэнди Петланд «Reality Mining» (Technology Review, MIT, 2008 г.) по адресу http://www2.technologyreview.com/article/409598/tr10-reality-mining/ и в работе Альберто Эскудеро-Паскаль (Alberto Escudero-Pascual) и Гаса Хосейна (Gus Hosein) «Questioning lawful access to traffic data» (Communications of the ACM, Volume 47 Issue 3, март 2004 г., стр. 77 - 82).

6. Доклад специального докладчика ООН по продвижению и защите свободы слова и выражения мнения Фрэнка Ла Рю (Frank La Rue), 16 мая 2011 года: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

7. «Люди раскрывают операторам мобильной связи номера телефонов, по которым они звонят и отправляют сообщения, интернет-провайдерам – адреса веб-сайтов, которые они посещают, и адреса электронной почты своих контактов, а онлайн-продавцам – названия книг, продуктов и лекарств, которые они покупают. ... Я бы не стала предполагать, что вся информация, которая на добровольной основе и с ограниченной целью раскрывается какой-либо стороне, действующей публично, должна быть исключена из действия защиты Четвёртой поправки» (дело «США против Джонса» (United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957), 2012 г., совпадающее мнение судьи Сотомайор (Sotomayor)).

8. «Краткосрочный мониторинг действий лица на улицах, открытых для общего доступа, находится в согласии с ожиданиями приватности», но «длительное использование GPS-мониторинга в расследовании по большинству дел отрицательно воздействует на ожидания приватности» (дело «США против Джонса» (United States v. Jones, 565 U.S., 132 S. Ct. 945, 964), 2012 г., совпадающее мнение судьи Алито (Alito)).

9. «Длящаяся слежка раскрывает такие типы информации, которые не обнаруживаются при краткосрочной слежке, например: что человек делает с некоторой периодичностью, что не делает, чем вообще занимается. Каждый из этих типов данных рассказывает о человеке больше, чем отдельное наблюдение за его поездкой. Повторяющиеся визиты в церковь, спортзал, бар или к букмекеру рисуют картину, которая недоступна по данным об одном посещении, как и наблюдение, если человек не посещает ни одно из этих мест

в течение месяца. Последовательность человеческих действий может раскрыть еще больше данных. Единичный визит к гинекологу мало что говорит о женщине, но если через несколько недель она отправляется в магазин детских вещей, это уже другая история.* Если известны все данные о перемещениях человека, можно выяснить, часто ли он ходит в церковь, много ли пьёт, занимается ли регулярно в спортзале, хранит ли супружескую верность, подвергается ли лечению, каковы его связи с конкретными людьми или политическими группами - не единичный факт о человеке, а все подобные факты» (дело «США против Мейнарда» (U.S. v. Maynard, 615 F.3d 544 (U.S., D.C. Circ., C.A.), стр. 562); дело «США против Джонса» (U.S. v. Jones, 565 U.S. __), 2012 г.), совпадающее мнение судьи Алито (Alito)). «Более того, публичная информация может быть фрагментом частной жизни, когда данные систематически собираются и хранятся в государственной базе. Это тем более верно, если такая информация относится к далекому прошлому человека... По мнению суда, такая информация, если её систематически собирают и хранят в базе, подпадает под определение “частной жизни” в соответствии со ст.8(1) Конвенции» (дело «Ротару против Румынии» (Rotaru v. Romania), [2000] ECHR 28341/95, параграфы 43-44).

10. Термин «надлежащая процедура» может применяться взаимозаменяемо с терминами «процессуальные гарантии» и «естественная справедливость». Это понятие в достаточной степени отражено в статье 6(1) Европейской конвенции о защите прав человека и основных свобод и статье 8 Американской конвенции о правах человека.

11. В Великобритании примером такого независимого надзорного механизма является Комиссар по вопросам перехвата коммуникаций. Комиссар публикует отчет, который включает некоторые обобщённые данные, но этот материал не дает достаточной информации для изучения типов запросов, масштабов каждого запроса, целей запросов и проведённых по этим запросам проверок. См. http://www.iocco-uk.info/sections.asp?sectionID=2&type=top

12. Доклад специального докладчика ООН по продвижению и защите свободы слова и выражения мнения Фрэнка Ла Рю (Frank La Rue), 16 мая 2011 года (A/HRC/17/27, параграф 84).