ПЕТЕРБУРГСКИЙ МЕЖДУНАРОДНЫЙ ЭКОНОМИЧЕСКИЙ ФОРУМ

16–18 ИЮНЯ 2011

ЧАСТНОГО ПРОСТРАНСТВА БОЛЬШЕ НЕ СУЩЕСТВУЕТ?

Технологии, расширяющие горизонты

17 июня 2011 г. — 14:00–15:15, Павильон 5, Зал 5.1

Санкт-Петербург

2011

Персональные данные все чаще оказываются в сети Интернет и становятся общедоступными. Это превращается в серьезную проблему для отдельных граждан, правительств и бизнеса. Есть ли у нас повод для беспокойства?

Модератор:

Тина Канделаки, Телеведущая

Выступающие:

Элизабет Бьюз, Президент группы стран, Visa Inc.

Орит Гадиш, Председатель совета директоров, Bain & Company

Питер Грауэр, Председатель правления, Bloomberg L.P.

Андрей Дубовсков, Президент, Главный исполнительный директор, ОАО «МТС»

Наталья Касперская, Председатель совета директоров, «Лаборатория Касперского»; Генеральный директор, InfoWatch

Игорь Щеголев, Министр связи и массовых коммуникаций Российской Федерации

Т. Канделаки:

Добрый день, уважаемые дамы и господа, рада вас всех приветствовать, спасибо за то, что пришли на нашу панель. Хотя вчера все говорили, что в Санкт-Петербурге будет плохая погода, я вот сегодня приехала — а погода хорошая, и я думаю, что настроение у всех тоже. Тем не менее, дискуссия будет очень серьезная, и я на вас очень надеюсь — надеюсь, что все участники панели выступят. У каждого из вас появится желание задать вопрос и получить сегодня ответ от людей, которые в том ряду, о котором мы говорим, являются одними из самых компетентных. Это, наверное, здорово, что сегодня, опять-таки благодаря Петербургскому экономическому форуму, у каждого из вас есть возможность получить более доскональный, более компетентный, более профессиональный ответ на вопросы, которые вас волнуют в связи с информационной безопасностью.

А сейчас, если позволите, я начну.

Т. Канделаки:

Я рада приветствовать вас на дискуссии в рамках Санкт-Петербургского международного экономического форума. Как общественного деятеля и телеведущую, меня очень интересует тема нашего сегодняшнего обсуждения — тема частного пространства. Как и многие другие глобальные темы форума, она касается каждого из нас. Стоит только ввести свое имя, номер телефона или адрес где-нибудь в Интернете, как вы навсегда теряете свою свободу и независимость.

С большинством из нас это уже произошло. Мы покупаем книги через Amazon, и кто-нибудь может увидеть, какие покупки вы совершали в течение года. Если вы оставите свое резюме на Headhunter или LinkedIn, то человек, с которым вы даже не знакомы, может узнать о вас больше, чем ваш супруг или супруга: что вы умеете делать, какая у вас работа и, даже зарплата. Я вообще-то не хочу, чтобы кто-то знал, какая у меня зарплата.

О. Гадиш:

Особенно муж, да?

Т. Канделаки:

Но я разведена, в том-то и проблема. Мы очень чувствительны к своей свободе, но большинство из нас даже не замечают, что давно ее потеряли, — или нет? Это на самом деле так, или это просто паранойя сегодняшнего времени? У нас сегодня здесь очень интересная группа экспертов. К сожалению, Джулиан Ассанж не смог прибыть. Очень жаль, поскольку ему есть что сказать, я уверена. Зато сегодня присутствуют:

Элизабет Бьюз, президент Visa'sGroup по Азии, Центральной Европе, Среднему Востоку и Африке;

Андрей Дубовсков, президент ОАО «МТС»;

Орит Гадиш, председатель совета директоров, Bain & Co;

Питер Грауэр, председатель правления Bloomberg LP;

Наталья Касперская, председатель совета директоров ЗАО «Лаборатория Касперского» и генеральный директор InfoWatch;

и Игорь Щеголев, министр связи и массовых коммуникаций России.

Мой первый вопрос — к Ориту Гадишу. Мы согласны с тем, что технологии и Интернет перевернули нашу жизнь, но, может быть, вместе с тем мы что-то потеряли. Не думаете ли Вы, что частное пространство — это та цена, которую нам приходится платить? Не уходит ли оно в прошлое?

О. Гадиш:

Спасибо. Я окружен людьми, которые используют действительно современные технологии. Я же пользуюсь старомодными вещами, так что извините.

И. Щеголев:

Так безопаснее.

О. Гадиш:

Вот именно. И это прямо подводит нас к вопросу о частном пространстве.

Вас могут взломать. А меня нельзя взломать. Вы спросили, уходит ли частное пространство в прошлое. Я бы сказал, пока нет. Есть ли серьезный повод для беспокойства? Да. Насколько это важно? Вам судить. Говорят, что со времен появления демократий был нужен четкий баланс между свободой отдельного человека и властью большинства.

Это привело к установлению определенных принципов и законов, которые охраняют этот баланс, что большинство из нас считают очень важным. Право на частную жизнь является классическим примером, и это как раз то, о чем мы сегодня говорим. Никто из нас не хочет жить в стеклянном доме. Мы также понимаем, что правительству необходимо знать некоторые личные вещи в общественных интересах или в целях безопасности. Тем не менее, если что-то интересно для других, то это необязательно будет в интересах общества.

Именно поэтому во многих странах для прослушивания вашего телефона или проведения обыска властям необходимо получить специальное постановление суда. Демократии понадобилось несколько столетий, чтобы прийти к этому. Итак, мы говорим об очень важном принципе.

Это помещение на самом деле не является звуконепроницаемым. Поговорим о хакерах: неприкосновенность частной жизни — это важнейший принцип, а технологии ему сегодня угрожают. Чего мы не должны делать, так это случайно нарушать этот принцип только потому, что частное пространство стало уязвимее, чем раньше. Позвольте мне коротко обозначить три основных направления, в которых Интернет угрожает частному пространству.

Первое: Бенджамин Франклин однажды сказал, что три человека могут сохранить тайну только в том случае, если двое из них мертвы. Наша проблема сегодня состоит в том, что один из тех людей, одна из трех сторон — это, по всей видимости, Интернет. Он не умирает, никогда ничего не забывает и всегда доступен.

Второе: благодаря Интернету информацию можно найти практически без усилий, так как он собирает и сортирует данные, что ранее было практически невозможно. Возьмите медицинские записи, возьмите сведения о покупках, о которых вы говорили.

Третье: в отличие от листа бумаги, который нужно физически найти, скопировать и унести, информацию в Интернете намного легче перемещать. И потому она более уязвима. Короче говоря, Интернет способствует так называемым утечкам.

Это может быть случайный выплеск конфиденциальных данных, как, например, списков держателей кредитных карт, когда компания действительно не заметила, что непреднамеренно сделала это. Это может быть результатом поисков частных структур, собирающих сведения о людях из онлайновых источников — таких, как как Facebook, Apple, Google. Это может быть прямое вторжение, например, хакерские действия в отношении файлов компании, что произошло буквально в последние две недели. Sony, Citibank, Chase, Google, — список можно продолжать. Думаю, мы все об этом читали. Это происходит ежедневно. Или, например, государства, которые, прикрываясь национальной безопасностью, осуществляют контроль за разговорами по мобильным телефонам и информацией в Интернете, или организации, крадущие информацию у других оранизаций, как это произошло в случае с WikiLeaks и Госдепартаментом США.

Традиционные утечки превратились в настоящее наводнение. Всего несколько лет назад такие мгновенные разоблачения в мировом масштабе были невозможны, и все это является проявлением нескольких ключевых

тенденций. Я назову три таких тенденции, затем их последствия и на этом остановлюсь, чтобы позволить другим ответить на вопрос.

Первое — это количество времени, которое мы проводим в Интернете, и растущий информационный след, который мы оставляем за собой. Например, на тех из вас, — а я думаю, это почти каждый присутствующий — у кого есть компьютер, BlackBerry и iPad, приходится по три часа машинного времени в течение каждых 60 минут. Довольно пугающе, по крайней мере для меня, выглядит использование сети среднестатистическим человеком: это 36 часов машинного времени в сутки, то есть времени, на протяжении которого он подключен к чему-то. По прогнозам, через два года будет уже 48 часов. Подумайте о количестве информации. И, кстати, когда вы просыпаетесь утром, вам тоже приходится иметь с ней дело, но это уже другой вопрос. Кроме того, есть вопрос скорости передачи данных и количества каналов, по которыми информация может идти. И, наконец, растет число людей и организаций, находящихся в сети.

По некоторым оценкам, к 2020 году объем информации, проходящей через Интернет, увеличится в 40 раз. Так вот, подумайте о том, какое невероятное количество данных производит Интернет. И он остается навсегда и будет доступен всегда. Это лавинное накопление данных имеет последствия для бизнеса, правительства, для отдельного человека, для общества в целом.

Сейчас основная тема разговоров в обществе — что также отмечалось сегодня утром, во время выступления Президента — это та огромная ценность, которую представляет собой Интернет. Она измеряется в эффективности, в возросшей продуктивности, увеличившейся скорости, способности взаимодействия со многими людьми, — все это верно. Кстати, я считаю, что в России Президент Медведев сильно поспособствовал этому. Однако об обратной стороне процесса говорится меньше.

Например, большинство пользователей Интернета рассматривают его с положительной стороны. И они идут обмениваться информацией на Facebook. Мало кто всерьез беспокоится или хотя бы осознает потенциальную опасность для своей репутации, пока не получит прямого удара, как это уже произошло с некоторыми людьми и будет происходить дальше, даже если вы попытаетесь отмахнуться от всего этого. Люди все чаще осуществляют покупки через Интернет, но там вы не можете платить анонимными наличными деньгами. Наличные деньги анонимны. Ваше имя с ними не ассоциировано. Информация же о вашей кредитной карте и истории ваших покупок есть везде. Сегодня легко найти сообщества тех, кто разделяет ваши интересы и убеждения. Это здорово. Но это также означает, что люди часто перестают слушать или общаться с теми, кто не разделяет их интересов и убеждений, если только не хотят оскорбить их или запугать.

Можно ли все это контролировать, изменив законодательство? Теоретически — да. Но для этого должен быть решен вопрос конфликта целей, что редко происходит. Правительства в США и Европе старались действовать и в этом направлении. Разрабатываются законы, есть попытки создать соответствующее законодательство. Но реальность такова, что правительствам по-прежнему нужна информация о вас, которую они все больше используют по соображениям безопасности.

Поэтому, пока это происходит, правительство фактически дейтвует в обоих направлениях. Настоящие тоталитарные режимы, как все мы видели, заходят еще дальше и запрещают любые медийные каналы, которые им мешают. Частные структуры тоже ведут двойную игру. Они обещают своим пользователей защиту и контроль за сохранностью их данных, но вместе с тем находят выгодные для себя способы предоставления доступа к этим данным третьей стороне, причем часто без ведома пользователей.

Теперь, я уверен, люди будут пользоваться Интернетом все время. Мы будем видеть все больше и больше технологий, созданных для того, чтобы защищать нас от подобного рода вещей, но мы также увидим и такие технологии, которые смогут обходить эти технологии. Такого рода перетягивание каната мы уже видели раньше.

У меня нет готового ответа. И, похоже на то, что его ни у кого нет. На недавней встрече «большой восьмерки» в Париже как раз обсуждались эти конфликты, и я закончу словами, которые сказал президент Николя Саркози в разговоре с интернет-разработчиками. Он в основном говорил о тех демократических принципах, с которых я начал свое выступление.

Вот что он сказал: «Мир, который вы представляете, — это не параллельная вселенная. В нем применяются правовые и моральные нормы, вообще все основные нормы, которые лежат в основе общества и демократических политических систем». Я с этим абсолютно согласен. Итак, уходит ли в прошлое частное пространство? Как я сказал, пока нет. Есть ли серьезный повод для беспокойства? Если для вас немаловажно частное пространство, думаю, что да. Спасибо.

Т. Канделаки:

Прекрасный пример у нас перед глазами, когда технологии опережают образование, и невозможно ими не воспользоваться. Мы сегодня много говорили до начала панели о том, как сделать, чтобы дети не пользовались технологиями. Дети же понимают, что они есть, понимают, что ими надо пользоваться. И не могу не добавить: для меня лично было открытием, какую литературу читают дети, сейчас все-таки период каникул и многие, наверное, следят за этим. В нашем детстве прочитать «Войну и мир» за лето — это было большим подвигом. Сегодня уже полностью доказан тот факт, что за четыре дня человек потребляет ровным счетом такое же количество информации, которое содержится в «Войне и мире», то есть

количество информации будет увеличиваться. И количество технологий, которые дадут возможность, с одной стороны, переваривать эту информацию, с другой стороны, использовать ее — кому-то во благо, кому-то во вред — тоже будет все время увеличиваться и ускоряться. Но здесь, если позволите, я продолжу нашу панель.

Я хотела бы задать свои следующие вопросы и Игорю Щеголеву, и Андрею Дубовскову. Поскольку Интернет не имеет границ, имеет ли смысл вводить правила в одной только стране, например, России? И правда ли, что большинство современных международных соглашений в этой сфере на самом деле не работают?

И. Щеголев:

Начну, наверное, я, Андрей потом добавит.

Конечно же, есть попытки отрегулировать Интернет в отдельно взятой стране, что само по себе выглядит достаточно странно, потому что это частная структура, которая возникла в совершенно другом отдельно взятом государстве. Но за время, прошедшее с момента появления Интернета, он превратился в большой глобальный ресурс, который влияет и на политику, и на социальную жизнь людей, и на экономику, и на технологии... Представить себе современную цивилизацию без этого ресурса трудно. Тем не менее, он глобально не управляется. И сама эта конструкция сделана так, чтобы быть непотопляемой, неубиваемой и самовосстанавливающейся. Данные, которые там хранятся, находятся там вечно и, соответственно, те злоупотребления, которые совершаются с помощью этого инструмента, тоже носят глобальный характер, — идет ли речь о целенаправленном вредительстве или просто о невинных шутках, которые потом парализуют целые отрасли экономики, а иногда и целые страны.

Вопрос, можно ли отрегулировать Интернет в отдельно взятой стране — он скорее риторический. Стоит закрыть какой-либо ресурс, как он тут же мигрирует в те страны, где запретительное право не применяется, и продолжает действовать оттуда: умельцы всегда обойдут любые фильтры и любые попытки цензуры. Вот почему, с нашей точки зрения, национальное регулирование в запретительном смысле абсолютно бесперспективно: оно противоречит самому смыслу этой технологии и в значительной степени — настрою в обществе.

Другая проблема — есть ли преступления и правонарушения, которым государство должно противостоять? Конечно, они есть. И в значительной степени этим правонарушениям, которые совершаются в национальном масштабе, можно противостоять с помощью тех правовых инструментов, которые уже имеются. Ведь Интернет — это лишь среда. И преступления, которые совершаются в Интернете, точно так же являются преступлениями, как если бы они совершались на улице. Если у вас украли кошелек на улице — это преступление, если у вас украли данные и с их помощью похитили средства со счета — это такое же преступление. И здесь можно бороться — если эти преступления совершены на территории вашей страны. Если они совершены за границей, это уже гораздо сложнее, это уже гораздо более трудная задача — до тех пор, пока представители разных государств не сядут и не договорятся, как этому противостоять.

Одна такая попытка была предпринята. Это так называемая Будапештская конвенция Совета Европы, которая, между прочим, допускала действия на чужой территории для преследования злоумышленников в Интернете, без предупреждения властей этой страны. В значительной степени именно поэтому конвенция не заработала, многие страны, в том числе и Россия, не сочли возможным ее ратифицировать по этой причине. И Россия, в частности, ставит вопрос о том, что нужны общие правила для борьбы с очевидными преступлениями, которые являются таковыми в любой

цивилизации и любой культуре, для любой нации. Нужно договариваться. Но пока такого консенсуса нет, хотя площадка, где это можно было бы сделать, на наш взгляд, существует. Это Международный союз электросвязи — старейшая международная организация, в два раза старше ООН.

Нужно договориться о базовых принципах, сказать, что вот это или то — абсолютное зло, все с этим согласны, и мы должны сделать все возможное, все от нас зависящее, чтобы с этим злом бороться. Мы считаем, что это можно сделать на примере детской порнографии, потому что нет культуры, в которой это было бы допустимо. И мы усиленно ищем союзников по всему миру, которые поддержали бы наш подход.

Конечно же, один из существенных факторов при решении этого вопроса — это как раз частная жизнь, это данные о человеке, которые находятся в Интернете, это вопрос о том, как с ними поступать. Есть оборотная сторона — это анонимность Интернета: все-таки большая часть Интернета у нас по-прежнему анонимна, это в значительной степени подстегивает злоумышленников, но с другой стороны, это является защитой для очень многих людей, которые делятся в Интернете какой-либо информацией, ищут эту информацию. Так что здесь есть две стороны и всегда нужно искать баланс.

Отвечая на ваш вопрос, скажу, что в пределах одной страны невозможно эффективно противостоять всем тем нарушениям, которые возможны в Интернете. Мы не видим смысла вводить на национальном уровне запретительный режим для Интернета, но считаем, что на международном уровне координация нужна. Нужны общие правила игры, которые отвечали бы, прежде всего, интересам пользователей и интересам граждан.

Т. Канделаки:

Прежде чем Андрей продолжит эту дискуссию, я бы хотела спросить Вас, Игорь. Вы наверняка в курсе конфликта, связанного с блоггером Матвиенко, который оказался в итоге мужчиной. Уважаемые средства массовой информации, многие издания публиковали цитаты из этого блога, и это стало темой для дискуссии во всей мировой прессе. Как вы считаете, в данном случае можно ли было как-то это предотвратить, проверить этого человека? Он ведь тоже определенным образом наносит ущерб целой стране.

И. Щеголев:

Каждое общество должно для себя решить, что для него ценнее — анонимность или транспарентность. И здесь дать четкий ответ невозможно. Это предмет для общественной дискуссии, это вопрос формирования этой среды, это вопрос баланса интересов гражданина и общества. И я считаю, что дискуссии, подобные нашей, способствуют поиску такого баланса.

Т. Канделаки:

Андрей, пожалуйста.

А. Дубовсков:

На одной из предыдущих открытых площадок, которая имела место не так давно, — я имею в виду выставку «Связь-Экспоком», которая проходила в мае месяце в Москве, — мы с уважаемым министром разошлись во мнениях по одному из вопросов. Так вот, внимательно послушав Игоря Олеговича сейчас, я рад сообщить вам, что баланс будет восстановлен. Я, безусловно, готов поддержать его позицию, но при этом хотел бы обратить ваше внимание на саму постановку вопроса. Понимаете, вопрос не звучит так: «имеет ли смысл трансграничное регулирование или каждой стране надо замкнуться в своих границах». Замыкание в своих границах

происходит априори. Это всегда так происходит, когда возникают новые технологии, новые возможности. Государство всегда пытается подстроить имеющиеся в его распоряжении ресурсы под эти новые возможности. Это нормальный процесс. Не надо говорить, что это правильно или неправильно. Так происходит всегда. Другой вопрос, что свои собственные национальные, ментальные и прочие приоритеты — и в том числе, безусловно, важнейший среди них, суверенитет в вопросах безопасности, — мы должны суметь ввести все эти исходные данные в некую трансграничную договоренность. Мы должны достичь соглашения, которое удовлетворяло бы все заинтересованные стороны. Да, есть неудачи, допустим, с Будапештской конвенцией, но опять же, это нормальное явление. Это просто первый шаг на пути к созданию наднациональной системы, регулирующей взаимоотношения индивидуума и общества в сетевом пространстве. Ограничусь этим, спасибо.

Т. Канделаки:

Вы знаете, я не могу не спросить, потому что мы много говорим о частном пространстве и его защите: а Вы зарегистрированы в социальных сетях? Вообще ими пользуетесь? Или как человек, который все-таки понимает, какой фидбэк от этого может быть, вы себя охраняете, не регистрируясь нигде или регистрируясь под чужим именем?

А. Дубовсков:

Что называется, welcome. Я очень неактивный пользователь социальных сетей и действительно, зарегистрирован в одной из них, это произошло очень давно, когда она только зародилась. Но, собственно говоря, никаких новых там движений на протяжении последних нескольких лет не было с моей стороны.

Т. Канделаки:

В этой социальной сети, Вы имеете в виду?

А. Дубовсков:

Да.

Т. Канделаки:

То есть у Вас все прошло нормально?

А. Дубовсков:

Вы знаете, я считаю, что, приступая к обсуждению такой серьезной темы, хорошо бы воспользоваться какими-то статистическими данными. Вот у меня, например, нет информации, какому проценту людей ситуация с такой неурегулированностью нанесла реально какой-то вред. Это с одной стороны. С другой стороны, интересно было бы иметь какие-то маркетинговые исследования на эту тему, понять в принципе, насколько проблема значима. То, что она есть, скажем, на уровне парадокса: там все остается навсегда и как-то на тебя может повлиять, а ты бы этого не хотел, — это очевидно. То есть этот парадокс есть. Но насколько этот парадокс значим? Понимаете, на свете есть огромное количество парадоксов. Очень интересно было бы узнать какие-то данные, основанные на маркетинговых исследованиях. Что считают люди для себя проблемой, с одной стороны, и с другой стороны — для какого количества людей это действительно явилось проблемой? Мне вот почему-то кажется, что огромное количество людей будет считать это проблемой, но процент людей, для кого это действительно явилось проблемой, не превысит процент людей, — ну, или, по крайней мере, будет на уровне статистической погрешности, — для которых проблемой явились, например, правонарушения, не связанные с виртуальным сетевым пространством. Возможно, я ошибаюсь. Но мне

кажется, что для нашей дискуссии такие сведения были бы небезынтересны.

Т. Канделаки:

Спасибо большое. Я думаю, что Вы абсолютно правы, тем более, что какие-нибудь яркие примеры, если кто-то из панелистов их приведет, они будут очень показательны. Все прекрасно знают, что тот же Джулиан Ассанж начинал как хакер, которого потом, если не ошибаюсь, после некоторого условного срока, пригласили работать, наоборот, уже в службу безопасности банка. И вот это движение, которое тоже вызывает много вопросов — оно является, в определенном смысле, как раз примером того, о чем Вы говорите. Было бы неплохо услышать и от участников, и от аудитории примеры того, что на самом деле нас беспокоит. Кто-нибудь когда-нибудь сталкивался лично с распространением информации о себе, которую он дал, зарегистрировавшись в сетях?

Наталья Касперская. Мой следующий вопрос к Вам. Мы только что обсуждали правила «с точки зрения государства». Как человек, разрабатывающий компьютерные программы, скажите нам правду: достаточно ли у государства, у регулятора, инструментов — я имею в виду технологии и программное обеспечение — чтобы регулировать Интернет? Мы не можем разрешить им защищать нас, но мне очень интересно: способны ли они на самом деле делать это?

Н. Касперская:

Да, я поняла вопрос. С одной стороны, теоретически я, конечно, должна согласиться с министром в том, что регулирование путем запретов — вещь бессмысленная. С другой стороны, когда мы говорим про безопасность вообще, то не надо валить все в одну кучу. Мы начинаем говорить про безопасность здесь, здесь и здесь... Надо делить совершенно четко: есть

безопасность частных лиц, это первый уровень. Особенно страдают дети. Есть следующий уровень — безопасность компаний, которую они должны в какой-то степени обеспечивать сами. Следующий уровень — это безопасность государства, о которой в государстве должны, безусловно, заботиться. Пример вируса «стакснэт», — для тех, кто не знает: это вирус, написанный по совместному заказу правительств Соединенных Штатов и Израиля, для атаки важных инфраструктурных объектов Ирана, — пример этого вируса, сложнейшего, который вирусные аналитики всего мира разбирали на протяжении трех месяцев, показывает, что атаки одной страны против другой с помощью киберсредств возможны. Значит, если страна не будет от этого никак защищаться, — это как минимум глупо.

С другой стороны, регулирование — если мы просто анонсируем, что мы будем регулировать сейчас весь Интернет — вещь совершенно бессмысленная. Можно говорить о технических средствах, потому что когда мы говорим, что против нас воюют техническими средствами, когда люди взламывают аккаунты, нападают, устраивают массовые акции в Интернете, направленные против государства, — если мы говорим о государстве, в принципе, с этим можно бороться. Какими методами? Существует система фильтрации, те же самые веб-фильтры, особенно фильтры с лингвистическими технологиями, могут с этим спокойно справляться. Существуют файерволы, появляются сейчас новые системы мониторинга, которые мониторят информацию о чем угодно. Задаешь им, например, «терроризм», и они будут мониторить все термины, которые связаны с терроризмом или являются заменителями слова «терроризм». Да, они будут давать определенное количество ложных срабатываний, но в любом случае это будет какая-то картинка. Я точно знаю, что спецслужбы всех стран этим занимаются. Конечно, такие системы фильтрации существуют, и с их помощью ведется наблюдение и проводится реальная работа: какие-то одиозные сайты периодически закрывают, периодически с этим борются.

Насколько это эффективно? Ну да, они могут возникнуть в другом месте. Но если ничего не делать, то и ничего не будет.

Еще я на вопрос Андрея отвечу, потому что он задал вопрос, какую опасность представляют собой социальные сети. У меня есть определенные цифры именно по соцсетям. Вот данные по России: в 2009 году в открытый доступ было выложено более 130 тысяч учетных записей пользователей в контакте. Это меньше 1% от пользователей сети, это примерно 0,1% от всех пользователей «ВКонтакте». Дальше, если мы возьмем мир в целом, то за прошлый год особенно, он стал прорывным в этом смысле, на Facebook, на Pirate Bay были выложены учетные записи более ста миллионов пользователей, а это, заметим себе, если в Facebook сейчас 640 миллионов, то сто миллионов — это где-то 10%, нет, почти 20%. Это много. То же самое на Myspace и Facebook — персональные данные миллионов пользователей передавались через коммерческие приложения. Тут другая уязвимость была использована, но общее количество атак на социальные сети за последний год выросло на сто тысяч. В штуках. То есть, допустим, одна атака — это данные ста миллионов пользователей украли — это одна атака. Проблема на самом деле есть. Но я не буду говорить про Sony, потому что Sony это уже такой, навязший в зубах случай.

Социальные сети, поскольку они концентрируют огромное количество людей, становятся очень хорошей приманкой, наживкой: туда хочется идти — там же много людей. Люди выкладывают массу информации о себе, они выкладывают все свои данные, ну почему же их не украсть? Особенно если мы соединим это с данными их кредитных карт, которые довольно легко соединяются, если используется единый почтовый аккаунт, — вот и все. Мы можем воровать и то, и то. Вытаскиваем пароль, сажаем троянца, который превращает его в ботный отель или во что-то еще, и пожалуйста...

Т. Канделаки:

Наталья, не могу не спросить у Вас — может быть, вопрос не по адресу, но уверена, что у вас есть очень интересное мнение по этому поводу. Вы говорили о том, что воровство в оффлайне естественным образом переходит в онлайн. Если кто-то воровал в обычном режиме, почему бы не своровать что-то в Интернете — тем более что там тоже можно украсть деньги? Возникает первый вопрос: вот Вы сказали об атаках, а есть ли информация о раскрываемости этих атак, о том, что важно для людей, чтобы понимать, насколько мы уязвимы? Это первое. И второе: вот, например, в каждой стране есть свои механизмы наказания, в зависимости от законодательства. Разные преступления наказываются по-разному. Как вы считаете: в будущем все страны должны объединиться, чтобы уровень наказания за преступления в Интернете был одинаковым, или этого никогда не будет? Где-то наказания будут жестче, где-то мягче. И что правильнее, как Вы думаете?

Н. Касперская:

Ситуация с раскрываемостью интернет-преступлений совершенно чудовищная. За прошлый год было раскрыто несколько десятков случаев и поймано несколько десятков команд, которые занимались распространением троянских программ, вирусописательством, взломами, хищением кредитных карт. Это — капля в море. Я даже не могу сказать, какой это процент, но думаю, что тысячная доля процента. Если мы сравним с раскрываемостью преступлений оффлайн, то там это все-таки десятки процентов. Все-таки совершивших убийство в 60-80% случаев ловят. Совершивших воровство, ограбление банка ловят в 90% случаев. Просто так войти в банк, в маске, с автоматом — вероятность неуспеха намного больше вероятности успеха. А в онлайне наоборот — именно из-за анонимности, именно из-за такой организации.

Более того, это система, которая работает. Но нужно понимать, это не организованная преступность, это такая роевая структура, наподобие пчелиного роя. Есть люди, которые пишут вирусы, вирусописатели. Они там где-то внизу. Они получают деньги от тех, кто эти вирусы заказывает. Есть люди, которые размещают заказы в Интернете на вирусописательство. Есть люди, которые рекламируют эти услуги. Есть люди, которые обналичивают деньги, потому что это деньги черные и их надо как-то извлечь. И эта вся система как-то работает, причем там нет единого правительства. Но очень часто говорят, что это русские программисты пишут. Часто пишут русские программисты и китайские программисты, а заказывают где-то еще, то есть это международная система. В прошлом году, по-моему, поймали, раскрыли группу украинских программистов, у которых центр был в Нью-Йорке, мозговой центр, который им давал работу, а программисты — они просто программируют.

Понимаете, даже непонятно, как их искать. Где у них центр? Кто этим всем управляет?

Т. Канделаки:

Я просто хочу добавить, что когда мы говорим о классических ограблениях, то все представляем американский блокбастер, «Двенадцать друзей Оушена». Мы понимаем, что есть заказчик, есть люди, которые это реализуют. И то, о чем Вы говорите, свидетельствует, прежде всего, о том, что этих людей очень сложно отследить. Но, исходя из того, что воруют базы данных, Вы можете увидеть себя в числе фигурантов крупных преступлений, хотя не совершали их. Если это случится — не удивляйтесь. Я правильно понимаю? Вы же свои данные опубликовали, ваши данные кто-то украл, под вашими данными это может быть совершено, правильно?

Н. Касперская:

Теоретически да, вы можете быть членом ботнет-сети, и при этом вы об этом даже знать не будете. Садится просто троянская программа, сидит она тихо, и у вас просто увеличивается трафик с вашего компьютера. А вы между тем рассылаете спам или делаете еще что-то по заказу. Миллионы компьютеров соединены в ботнет-сети. И миллионы несчастных пользователей об этом не подозревают. Они просто жертвы этой ситуации. Сажать их — в общем, тоже нечестно. Их-то за что?

Т. Канделаки:
Спасибо Вам большое.

Т. Канделаки:
Мой следующий вопрос — к Питеру Грауэру. Вернемся к определению частного пространства. Джулиан Ассанж сказал: «Лучший способ сохранить секрет — не иметь секрета». В таком случае меня интересует вот что: верите ли вы в мир без секретов, в честную, прозрачную дипломатию, в честный, прозрачный бизнес?

П. Грауэр:
Я хочу сделать два замечания. Одно из них слегка дополняет сказанное Оритом. Я хотел бы попросить поднять руку всех в этом зале, кто в данный момент тем или иным образом использует сотовый телефон, iPad или планшет. Ну, давайте, сознавайтесь. Вы не говорите правду.
Но я вас вижу. Я говорю это, поскольку заметил, что когда кто-то выступает, вы не смотрите на сцену. Это своего рода показатель масштаба проблемы. А посмотрите на всех находящихся здесь фотографов, они ведут цифровую съемку. Все эти снимки появятся в Интернете, в том или ином виде, через 10-15 минут после того, как мы выйдем отсюда. Это первое замечание. Я хотел просто показать сложность этих проблем. До некоторой степени мы

принимаем как само собой разумеющееся, что личные данные будут защищены, что с нашим частным пространством все будет в порядке. На мой взгляд, думать так очень наивно.

Второе замечание, которое я хотел бы сделать, прежде чем отвечать на поставленный вопрос более конкретно. Месяца полтора-два назад я ужинал с бывшим председателем Объединенного комитета начальников штабов при президенте Соединенных Штатов. На ужине присутствовало около десяти человек, и кто-то спросил у генерала Пэйса (а это генерал с четырьмя звездами на погонах из Корпуса морской пехоты): «Что Вас беспокоит больше всего?».

Так вот, он воевал в Афганистане, в Ираке, помимо этого в его послужном списке есть и Северная Корея, и Мексика, и борьба с наркотерроризмом. И этот человек, который изъездил весь Ближний Восток, бывал во всех других горячих точках мира, ответил: «Меня больше не беспокоит военный терроризм. Меня беспокоит компьютерный терроризм».

И это для всех нас — для тех, кто работает в правительстве, в частном секторе, в бизнесе, в образовании, — вопросы, которыми мы должны заниматься вместе, которые мы должны решать, чтобы успешно двигаться вперед.

Я не думаю, что, в конце концов, введут жесткие, непреложные правила. Однако я действительно считаю, что нам нужны единые стандарты поведения, принятые во всех странах. И нам нужны схемы государственно-частного партнерства, чтобы сообща создать какие-то из этих стандартов и создать у людей чувство ответственности за то, чем они каждодневно занимаются в Интернете.

Наша компания свято верит в концепцию частного пространства, которое, я думаю, все же сохранится, это первое. Второе — это вопрос прозрачности. Прозрачность, я думаю, создает гораздо больше доверия к структурам, которые прозрачны в плане имеющейся у них информации.

Таким образом, я не думаю, что прозрачность уйдет в прошлое. Я думаю, что она сохранится. Но ответственность за это лежит на всех нас, особенно на нашей компании. Элизабет будет говорить об этом через минуту, так как это имеет отношение к ее компании. Мы являемся сегодня одним из крупнейших поставщиков информации в сфере финансовых услуг. Если наша система «полетит» по вине хакеров, мировые рынки капитала остановятся.

А потому мы тратим на эти вопросы непропорционально много времени. Служба безопасности нашей компании докладывает мне о ситуации. Я встречаюсь с главой нашей службы безопасности два раза в неделю, чтобы обсудить текущее положение дел. Мы управляем одной из крупнейших частных коммуникационных сетей в мире. Никто из нас не может противодействовать тому цунами, которое поднялось, чему мы все в определенной степени способствовали. Но мы должны создать какие-то стандарты. Должна существовать концепция частного пространства. Мы все должны чувствовать уверенность в том, что во время путешествия нашей информации, — между членами семьи, коллегами по работе или кем-то еще, — она защищена.

Итак, я верю в частное пространство. И, конечно, я верю в мир, в котором существует прозрачность. Я отвлекусь на секунду. Кое-кто из вас уже видел: мы написали статью, опубликованную в сегодняшнем номере Wall Street Journal, о ЕЦБ и его нежелании раскрыть информацию, в частности, о займах, сделанных Грецией, и финансовой помощи Греции. Я думаю, что такие вещи будут происходить и дальше, но все мы должны быть более бдительными, и, кроме того, должны существовать единые стандарты.

Т. Канделаки:

Здесь присутствует один из менеджеров компании Visa, Элизабет Бьюз. И каждый поймет, почему мой следующий вопрос будет о деньгах. Всем

интересно знать, как можно сберечь свои деньги. Кажется, что сегодня в мире имеется гораздо больше информации по проблемам защиты данных.
Я думаю, что ни одна компания не может гарантировать защиту своих данных. У них есть ощущение того, что миллионы их клиентов начинают все больше испытывать обеспокоенность этим. Можете ли вы как ведущая платежная компания мира что-либо сделать для укрепления этой уверенности? Думаю, что у каждого здесь есть платежная карта, и все испытывают страх в связи с этим. Итак, защищены ваши деньги или нет?

П. Грауэр:

Можно мне сказать два слова? Я считаю, она великолепно выполняет свою работу, Элизабет. Все знают, что когда вам вдруг звонят и спрашивают: «Вы на самом деле ездили в Лас-Вегас и потратили такую-то сумму?», то это они вас так защищают.

Э. Бьюз:

Большое спасибо. Сегодня я встретилась с ним лично впервые. Здорово, правда? Питер, спасибо за это. Да, это правда, у каждого есть карта или платежное электронное средство. А значит, мы всегда должны соблюдать баланс между ростом мировой торговли и безопасностью.
Сначала краткое введение, потому что, как я думаю, не все понимают, что такое Visa. Итак, Visa — это глобальная платежная сеть. Мы работаем в 200 странах мира и осуществляем операции примерно в 175 валютах. Но мы не устанавливаем сборов с торговых организаций или потребителей. Мы не даем кредитов и, как правило, не храним данные потребителей. Они хранятся в банке, выдавшем вашу карту, или в торговой организации, принявшей вашу карту.
Но вот что вызывает у нас беспокойство в этом контексте, поскольку оно связано с операциями по платежным картам: мошенничество. Кто-то

получает мою информацию, он может пойти и сделать покупки на мои деньги. Очень важно осознавать размеры мошенничества. Если посмотреть на систему Visa в мировом масштабе, то в то время как темпы роста платежей исчисляются в двузначных цифрах, уровень мошенничества снижается.

Сегодня мошенничество находится на самом низком в истории уровне: пять центов на каждые сто долларов сделок. А через сеть Visa ежегодно проходит 5 трлн долларов США. Да, проблемы есть, но надо знать, что размеры мошенничества снижаются, и что в его предотвращение все мы вкладываем большие средства.

Одним из примеров является стандарт защиты информации в индустрии платежных карт (PCI DSS). Этот стандарт был принят всей отраслью — финансовыми учреждениями, платежными сетями, торговыми организациями, — и соблюдается во всем мире для обеспечения безопасности данных о потребителях.

Совсем недавно Visa выпустила руководство по передовым технологиям шифрования и токенизации, которые обеспечат еще большую безопасность данных. И, как сказал Питер, мы постоянно инвестируем в нашу сеть на очень высоком уровне, чтобы по мере роста продаж, особенно с применением таких новых методов, как продажа товаров через Интернет и с помощью мобильного телефона, мы могли эффективно решать проблемы мошенничества — ради безопасности наших клиентов.

Сегодня фактически каждая сделка, проходящая через нашу сеть, подвергается динамической оценке рисков и отслеживается на мошенничество. Это происходит с каждой сделкой, каждую секунду, каждодневно. Я хотела бы только добавить, что от всех трех участников дискуссии вы неоднократно слышали три слова: партнерство, баланс и стандарты. Я буду говорить о них в другой последовательности.

Баланс действительно важен, с этого я начала. Мы должны быть способны содействовать росту, в то же время помня о безопасности. Это и есть баланс, которого мы все должны добиваться. Для его достижения мы должны быть партнерами. Мы должны вступать в партнерство с государствами. Нам нужно широкое партнерство в любой экосистеме — в случае Visa это платежная экосистема — и у нас должны быть стандарты.
Мы говорили о том, что у Интернета нет границ. Если у нас не будет одинаковых стандартов по безопасности, по защите частного пространства, мы не сможем обеспечить рост.

Т. Канделаки:
Я написала пост, до начала нашей панели, о блоггерше из Дамаска, и мне поступает много комментариев, может быть, и от людей, которые находятся в этом зале — не знаю. Один из комментариев мне очень понравился, он был связан с тем, что все-таки страшнее: анонимность или тотальный контроль. И если кто-то из участников панели может ответить — было бы здорово, мы потом перейдем уже к вопросам от аудитории. Собственно говоря, заметьте, как смешно: я вот сейчас смотрю, какие у меня идут комментарии, и я не знаю, эти комментарии, возможно, поступают от людей из зала, а возможно, из какой-нибудь другой точки мира. И вот это как раз очень хорошо демонстрирует то, о чем мы сегодня говорим. В двух словах, если не затруднит, кто-нибудь из участников может ответить на этот вопрос? Ответьте, пожалуйста. Наталья Касперская.

Н. Касперская:
Да. Мне кажется, постановка вопроса вообще неправильна. Это как две крайности — ни одна невозможна, ни другая. Но тотальный контроль в Интернете невозможен, просто чисто технически. Для этого нужно всю систему Интернета полностью поменять, поменять всю серверную

инфраструктуру «железа». Вот сейчас Интернет пытается перейти на следующий стандарт, на следующий, шестой, уровень, но это целая история. Это многолетний, сложный, тяжелый процесс. А поменять всю систему функционирования Интернета — это просто невозможно. С существующей архитектурой Интернета тотальный контроль просто невозможен. Поэтому такая постановка вопроса бессмысленна. Полная анонимность — ее тоже, в общем-то, не существует. Если мы внимательно посмотрим, то люди сами себя регистрируют, люди записываются в какие-то сервисы, они делают покупки, оставляют о себе информацию, этой информации много, эта информация накапливается, как с самого начала говорила Орит — именно об этом. В принципе, о каждом человеке уже много чего есть. Поэтому сказать, что это абсолютно анонимно, невозможно. Даже преступники совершают какие-то действия, а потом выясняется, что он или они присутствуют в социальных сетях, и можно посмотреть, чем они там занимаются. Я думаю, что просто должен соблюдаться какой-то баланс в отношении контроля. Мы должны четко понимать, какие угрозы перед нами стоят, и защищаться именно от этих угроз. Когда предприятие думает, как защититься, оно строит в первую очередь модель угроз. Тут та же самая история. Мы должны построить модель угроз и от этой модели защищаться. На государственном уровне — одна модель, на уровне частном — другая, на уровне компаний — третья. Вот и все.

Т. Канделаки:

Спасибо. Орит, пожалуйста.

О. Гадиш:

Это интересно. Я уже говорил, что должен быть баланс. Я, возможно, первым сказал это, когда только начал. Но это превращается в пустые

слова, особенно когда интернет-провайдеры, поставщики техники и технологий держат вас в неведении.

Последнее из происшествий, например, случилось на Facebook, с технологией распознавания лиц, о чем люди были проинформированы только после случившегося. А затем уже им пришлось сказать, что есть кнопка для отмены этой функции. Это было сделано потому, что Facebook, очевидно, хочет расширяться и зарабатывать больше денег. Такая вот это компания. Вот где идет война на самом деле. И если я хочу защитить себя, то я не буду присоединяться ни к одной социальной сети. Лично меня это не интересует. Я был в одной или двух анонимно, не под своим именем, — просто хотел посмотреть, что там происходит. Интересно оценить это с коммерческой точки зрения. Но война идет не только между странами или людьми, которые хотят совершить преступление, она идет также между людьми, которые разрабатывают технологии, и людьми, которых, как Питера и меня, очень волнуют вопросы частного пространства и которые, возможно, даже не знают, что делается.

Немалое число таких компаний было вынуждено пойти на попятный под давлением со стороны клиентов, которые были по-настоящему разгневаны и взбешены. Люди, которые доверяли Sony, очевидно, не знали, что там все идет по-другому — не так, как у Питера, который по два раза в неделю заседает со своей службой безопасности. Сейчас мы понимаем, как там все идет. Поэтому вопрос очень сложный. Я имею в виду, что относительно легко сказать: «нужен баланс». Нужен, это ясно. Демократии кое-чего добились за все эти годы: существуют даже особые статьи в уголовных кодексах.

И, конечно, есть, например, Интерпол. Но нельзя создать баланс, когда существует слишком много различных структур, которые хотят слишком многого и фактически воюют между собой.

Форум G8 именно для этого и собирался. Они заседали четыре дня и пришли к выводу, что между ними совершенно нет согласия. Вы все время говорите, что нужен баланс. Единственное, что мне нужно для защиты себя, — это помещать как можно меньше информации о себе. Но даже и тогда нет гарантии, как это обнаружили пользователи Facebook.

Итак, с чего вообще начинать создавать баланс? Где он начинается? На сегодняшний день никто не может дать ответа. Вопрос, как сказал Питер, становится все более острым. Я думаю, что на самом деле компьютерный терроризм является одной из главнейших проблем уже довольно много лет. Это не новая проблема. Но не существует ни одной такой структуры, которая могла бы что-то сделать в приказном порядке. Между многочисленными структурами нет согласия.

Н. Касперская:

Возможно, я могу ответить на этот вопрос, потому что я совсем недавно вернулась с форума по проблемам компьютерной безопасности, организованного Институтом Восток-Запад (West-East Institute). Институт пытается создать площадку, на которой можно начать что-то делать в отношении компьютерной безопасности.

Это был уже второй форум, и он проходил в Лондоне. Первый состоялся в Далласе. Весь его смысл как раз в том, чтобы решать общие угрозы, потому что существует слишком много общих угроз для всех. И необходимо что-то делать с этим. Вы говорили о решении проблем на межгосударственном уровне. Здесь я согласна: интересы у всех разные.

Так Китай, вероятно, не согласился бы с США и с некоторыми другими странами. И Россия тоже с чем-то, может быть, не согласится. Если вы объедините все восемь стран для решения проблем на межгосударственном уровне, ничего, пожалуй, не получится.

С другой стороны, есть общественные организации, есть частные компании, есть частные лица. И правительства должны защищать их всех. Все мы подвергаемся одним и тем же угрозам, от которых нужна защита. Это, например, детская порнография или компьютерный терроризмом, или, скажем, создание ботнет-сетей, или кража данных о кредитных картах, и так далее. Предстоит еще многое сделать. Страны пытаются договориться, эксперты садятся вместе и стараются решать. Кстати, на последнем форуме большая часть времени была посвящена определениям. Они обнаружили, что главная проблема — в разных определениях.

Неизвестно, что следует определить как угрозу. Является ли вот это угрозой? Какого уровня эта угроза? Прошли различные семинары, и были даны различные определения. После создания определений, может быть, наступит следующий этап, когда страны наконец-то придут к соглашению.

По крайней мере, я надеюсь на это, потому что с техническими вопросами все абсолютно ясно. Отразить такое огромное количество атак по всему миру невозможно. Абсолютно невозможно. Поэтому мы должны делать что-то вместе с общественностью, частными лицами и правительством, и особенно важно участие каждого. Нужно просвещать частные компании.

О. Гадиш:

Единственное, что Вы не упомянули, это опять же компании, которые хотят делать деньги на использовании данных. Это, похоже, не является незаконным — мы говорим о частном пространстве — до тех пор, пока люди не начинают протестовать, потому что им до этого ничего не было сказано.

Так что это не только проблема межгосударственных решений. Насчет детской порнографии: думаю, все в большинстве своем согласны, что это нехорошо. Но сейчас разные люди и структуры делают такие деньги, которые раньше невозможно было делать, устанавливая такие связи,

которые опять же раньше никто не мог устанавливать. И их за это не наказывают, потому что это ненаказуемо.

Н. Касперская:

Я думаю, что существует множество угроз. Например, если говорить только о существующих ныне вирусах, насчитывается более 50 их типов. Поэтому пытаться найти защиту от всего — это невыполнимая задача. Сперва нужно определить области, где мы можем сделать что-то вместе, и попытаться защитить эти области. Вы совершенно правы насчет частного пространства и компаний, которым нужны ваши деньги. Может быть, стоит отложить эту проблему на некоторое время, потому что есть много других вопросов, которые нужно решать. И надо начать решать какие-то проблемы, потому что имеется огромное количество проблем, которые требуют решения. Я верю, что шаг за шагом мы постепенно улучшим ситуацию.

Т. Канделаки:

Спасибо, Наталья.

Э. Бьюз:

Я только хотела сделать одно короткое замечание. Я считаю очень важным то, о чем говорил Орит: ясно, что потребители ожидают защиты персональных данных, и — думаю, мы все с этим согласны, — полагают, что имеют право на защиту персональных данных. И даже если эти данные используются надлежащим образом, я думаю, потребители имеют право знать, что их данные находятся у того-то. И они должны иметь право выбора относительно того, как эти данные будут использоваться. Это возвращает нас к случаю с Facebook. Потребителей следует спросить и дать возможность ответить «нет».

Т. Канделаки:

Спасибо, Элизабет. Теперь, если есть вопросы из зала, то у нас осталось время только на два. Извините, что так вышло.

Из зала:

Это вопрос для Орита, для Элизабет, и, возможно, для Натальи Касперской. Итак, вкратце: я работаю в области высоких технологий, и постоянно сталкиваюсь с атаками хакеров. На самом деле они хотят проникнуть в системы не с определенной целью, не потому, что они, допустим, террористы. Они делают это просто из любопытства.

Мой вопрос с предпринимательской точки зрения: вы никогда не думали о создании фонда, который даст этим людям право и возможность основывать компании, способные обеспечить вам новый уровень безопасности?

О. Гадиш:

На самом деле это уже делается. Я имею в виду, что многие из этих людей — это хакеры, произведенные в предприниматели, чтобы помочь нам разобраться в проблеме. Это делается уже давно, хотя здесь есть эксперты, которые знают об этом больше меня.

Э. Бьюз:

Одно короткое добавление. Если вы видите, как компании открывают пограничный сегмент своей сети, то, естественно, это делается под контролем, например, как это делал центр разработок в Apple. Мы в Visa открыли пограничный сегмент нашей сети и стимулировали разработку как приложений, облегчающих работу для клиентов, так и приложений, обеспечивающих безопасность данных.

П. Грауэр:

Выскажу свое мнение. Любая компания, которая серьезно думает об этих проблемах, привлекает внешние фирмы для постоянного тестирования на проникновение различными способами через брандмауэры в свои сети, чтобы посмотреть, к чему это приведет, удастся проникновение или нет. Думаю, что существуют целые группы людей, которые этим занимаются.

Т. Канделаки:

Пожалуйста, Фриц Морген, известный российский блоггер.

Ф. Морген:

У меня вопрос к Наталье Касперской. Скажите, если бы у вас была техническая возможность щелкнуть пальцами и ликвидировать анонимность, ну, ради всеобщей безопасности, допустим — Вы бы сделали это?

Н. Касперская:

Нет, конечно. Уничтожение анонимности приведет к проблемам другого рода. Мы, собственно, здесь и говорим о том, что потеря приватности — страшная вещь. Теперь представим себе, что анонимности нет: человек уже выложил о себе много чего, и о нем вообще все известно: куда зашел, что там сделал. Я даже знаю случаи, когда общение в социальных сетях приводило к совершенно ужасным последствиям. Поэтому я думаю, что Интернет таков, каким создался. Есть плюсы и минусы, но давайте жить с тем, что есть.

Т. Канделаки:

Вот мы сейчас говорим, и у меня впервые появились такие мысли: насколько вообще появление Интернета — к слову, о статистике, —

простимулировало повышение уровня преступности? Ведь раньше люди все-таки были ограничены не только нравственными нормами, но и отчасти законом, пониманием того, какое наказание они понесут за преступление. Сегодня Интернет дает возможность людям выплескивать свою агрессию: ты можешь сказать, что хочешь и кому хочешь, нанести какой хочешь ущерб, и никто ничего тебе не может сделать. Я думаю, что разговор об этом невозможно уложить в одну панель. Об этом можно говорить долго и бесконечно, потому что с каждым днем, с каждой минутой, с каждой секундой появляются новые возможности для все большей и большей коммуникации между людьми во всем мире, а, соответственно — чем ближе мы становимся к друг другу, тем, как выясняется, мы становимся уязвимее. Вот он — этот глобальный мир, о котором мы так много говорили, к которому мы так стремились. Мы хотели жить в глобальном мире — пожалуйста. В любую секунду мы сейчас можем по Skype связаться, с кем угодно. Но что это нам принесет — другой вопрос.

Большое спасибо всем участникам панели, большое спасибо вам, дорогие гости. Я бы хотела сказать несколько слов. Ну, во-первых, понятно, что дух российских хакеров, абсолютно очевидно, был сегодня среди нас. И я абсолютно уверена в том, что сегодня вы отсюда ушли чуть менее защищенными и чуть более уязвимыми. Но такова жизнь, вы выбрали эту панель, поэтому — ничего не поделаешь — придется за это заплатить. Так как я много лет работала на телевидении, не могу не вспомнить одну банальность: когда телевидение только появилось, многие упрекали его в том, что оно оказывает давление на людей, заставляет их делать выбор, который они не собирались делать. Мы хотели бы выбирать одно, но телевидение нас убеждает в том, чтобы сделать другое. Но что телевидение? Сегодня Интернет дает нам возможность оказывать влияние на людей, и мы даже не знаем о том, что делаем это преднамеренно. В этом принципиальная разница. Мы на телевидении знаем, что адресуем

вам и чего хотим от вас. А вот в Интернете, когда мы кому-то что-то адресуем, если это не крупные компании, которые должны делать деньги, если это именно частная коммуникация, — никто не знает, к чему приведет эта коммуникация. Знаете хорошую фразу: this spy camera never sleeps? Поэтому когда ты слышишь, например, о том, что Интернет — это tool of Satan, ты понимаешь, что таких людей становится все меньше и меньше, потому что противостоять этому невозможно. Просто нужно учиться в этом жить. Это самое главное. Поэтому я уверена, что человечество найдет механизм регуляции. История помнит случаи, когда от болезни умирали целые народы, но, тем не менее, потом что-то восстанавливалось, механизм восстанавливался, человечество самосохранялось. Механизм самосохранения слишком развит в человеке, для того чтобы не использовать эту потрясающую возможность, которая за 45 лет дала нам то, чего не дала ни эпоха пророков, ни эпоха возникновения письменности. Все исчисляется тысячелетиями. Интернет исчисляется десятками лет. Благодаря Питеру Брауэру, не могу не отметить то, что все подняли руки, когда он спросил, кто зарегистрирован, вы все честно сказали, что да, они зарегистрировались. Поэтому, Питер, если Вы не против, я позволю себе попросить всех, кто поднял руки, обязательно зафолловить меня в твиттере, и я надеюсь, что Вы это тоже сделаете, потому что я на новости Bloomberg подписана.

Большое спасибо.