
КОПЕНГАГЕН – Сквозное обсуждение в рамках сообщества с комиссарами по защите данных
Вторник, 13 марта 2017 г. - 15:15 – 16:45 по СЕТ
ICANN58 | Копенгаген, Дания

НАЙДЖЕЛ ХИКСОН (NIGEL HICKSON): Здравствуйте! Добрый день, дамы и господа! Не могли бы... ой. Извините. Добрый день. Мы начнем заседание через несколько минут. Не могли бы мы попросить людей пройти вперед? Мы не кусаемся, поэтому было бы здорово, если бы вы прошли вперед. Давайте работать коллегиально.

ДЖЕЙМС БЛЕЙДЕЛ (JAMES BLADEL): Добрый день. Попрошу всех занять свои места, мы начинаем, и, как сказал Найджел, проходите вперед, не стесняйтесь. Здесь много места и, возможно, мы выбрали слишком большую аудиторию для собравшихся. Но не стесняйтесь, проходите на передние ряды, пожалуйста. Мы начнем примерно через полторы минуты.

Итак, добрый день и добро пожаловать на сквозное обсуждение. Сегодня мы поговорим о конфиденциальности данных, заседание возглавляют GNSO и Правительственный консультативный комитет.

Примечание: Примечание. Следующий документ представляет собой расшифровку аудиофайла в текстовом виде. Хотя расшифровка максимально точная, иногда она может быть неполной или неточной в связи с плохой слышимостью некоторых отрывков и грамматическими исправлениями. Она публикуется как вспомогательный материал к исходному аудиофайлу, но ее не следует рассматривать как аутентичную запись

Для нас большая честь, что в качестве гостей к нам сегодня присоединились эксперты по защите данных из Евросовета. Давайте поприветствуем их от всего сообщества на этом заседании ICANN в Копенгагене.

[аплодисменты]

ДЖЕЙМС БЛЕЙДЕЛ: Тема конфиденциальности данных касается всех заинтересованных сторон, представляющих интересы правительств, реестров или регистраторов доменных имен, миллионов владельцев доменных имен и конечных пользователей здесь, в Европе, и по всему миру.

Почти по всем аспектам защита конфиденциальности данных влияет на работу, которую мы здесь, в ICANN, выполняем, и усложняет ее. Это заседание, в частности, очень своевременное, поскольку мы в GNSO на данный момент участвуем в разработке политики всей будущей системы регистрационных данных, и я надеюсь, что это заседание поможет работе, и наши сегодняшние обсуждения положат начало непрерывному сотрудничеству и постоянному диалогу со всеми вашими организациями.

С учетом сказанного, давайте начнем с того, что, как я полагаю, будет интересным.

Прошу поприветствовать Йоханнеса Кляйсена (Johannes Kleijssen) из Евросовета. Он является

директором информационного сообщества и отдела противодействия преступности, и у него есть несколько вступительных замечаний. Директор Кляйссен.

ЙОХАННЕС КЛЯЙССЕН: Благодарю вас, председатель. Спасибо. Спасибо, Джеймс. Доброго всем дня. Очень благодарен GNSO, GAC и правлению ICANN за то, что они нас приняли, и за то, что поддержали предложение Евросовета о проведении сквозного обсуждения.

Пожалуй, скажу несколько слов о Евросовете, о том, кто мы такие. Обещаю занять всего одну-две минуты.

Евросовет основан в 1949 году, в него входят 47 государств и 5 наблюдателей, штаб-квартира находится в Страсбурге, Франция. Он занимается вопросами прав человека, правовым регулированием и демократизацией, Гражданское общество работает с нами вот уже более 30 лет, и в настоящее время мы также создаем платформу для сотрудничества с бизнес-сообществом, намерены предоставить им официальный статус и место за столом.

Таким образом, Евросовет перестает быть только межправительственной организацией, и становится организацией с участием многих заинтересованных

сторон, мало чем отличающейся от той, о которой мы сегодня говорим.

Те, кто из Европы, конечно, слышали об этом. Представители других стран, возможно, слышали о Европейской конвенции о защите прав человека и Страсбургском суде, который выносит обязательные для исполнения решения по конкретным случаям, касающимся прав человека, а для сотрудников правоохранительных органов, скажу, что у нас есть более 60 международных конвенций по вопросам уголовного права, так что мы работаем по обоим направлениям.

С 2010 года нам присвоен статус наблюдателя в GAC, и на данный момент мы предоставили на обсуждение три отчета, один из которых обсуждается на этой неделе.

Для сегодняшнего заседания особое значение имеет наша конвенция о защите данных, именуемая также Конвенцией 108. В ней участвуют 50 сторон, 50 государств, ратифицировавших конвенцию, и 10 наблюдателей, то есть 60 стран, которые регулярно обсуждают вопросы безопасности, а это значит, что мы объединили половину государств, имеющих законодательство о защите данных, среди которых не только европейские страны.

Аналог конвенции о защите данных — это, пожалуй, конвенция о киберпреступности, известная также как

Будапештская конвенция, которая пока является единственным международно-правовым документом в этой области. Ее также подписали 50 государств, включая, например, США, и мы наращиваем потенциал еще в 125 странах по всему миру.

Что касается сегодняшнего события, мы надеемся, что это обсуждение станет началом процесса, а не разовым мероприятием. Мы убеждены, что обсуждение этого вопроса актуально и необходимо именно сейчас. Я надеюсь, что те из вас, кто все еще настроен скептически, после сегодняшнего обсуждения и после того, как услышат от комиссаров по защите данных и других экспертов, убедятся, что это необходимый диалог.

Правовые обязательства сторон, связанных договорными обязательствами в отношении ICANN, а также национального и международного права, все более противоречивы. Это относится и к самой ICANN. Мы надеемся, что сегодняшняя дискуссия станет началом процесса, который приведет к важным решениям с участием многих заинтересованных сторон. Большое спасибо.

БЕККИ БЕРР (BECKY BURR): Спасибо, и приветствую всех. Многие из вас знают, что моя профессиональная деятельность связана с ICANN, а также законами и политикой в сфере защиты

конфиденциальной информации, а ICANN — это место, где две эти вещи сталкиваются, хотя пока я не присоединилась к Правлению, мне удавалось избегать каждой отдельной проверки WHOIS, которые проходили с тех пор, как мы сюда попали.

И я думаю, многие из вас говорили, что было бы хорошо, если бы представители органов по защите персональных данных присутствовали на наших дискуссиях. Я очень рада, что они сейчас здесь, и я ценю инициативу Евросовета и органов по защите персональных данных, которые принимают участие в нашем диалоге.

Как вы поняли, эта беседа не одного заседания. Она призвана возобновить и укрепить открытый, многосторонний и почти бесконечный диалог по этим вопросам.

Итак, я собираюсь кратко представить участников обсуждения. У меня есть ряд вопросов, с которых мы начнем. Затем перейдем к вопросам от аудитории и от всех, кто участвует дистанционно.

Поэтому для начала я приглашу того, кто не нуждается в представлении и является одним из организаторов, — Томас Шнайдер (Thomas Schneider), председатель GAC и заместитель главы Службы международных отношений, а также координатор международного информационного общества в Швейцарском федеральном управлении

связи. Мне пришлось это прочесть, потому что описание должности действительно длинное. Прошу прощения.

Итак, Томас. Он начнет с ... задаст несколько вопросов.

Также здесь присутствует Джованни Буттарелли (Giovanni Buttarelli), Европейский инспектор по защите данных. Он был назначен на эту должность Европарламентом и Евросоветом в 2014 году на пятилетний срок. Ранее он также работал в этом отделе, а до этого был Генеральным секретарем итальянского управления по защите данных с 1997 года, то есть практически с самого появления вопросов конфиденциальности в интернете.

Уилберт Тоумсен (Wilbert Toomesen) является заместителем председателя комиссии по защите данных в Нидерландах и заместителем председателя рабочей группы по статье 29. Он напомнил мне сегодня, что рабочая группа по статье 29 впервые написала ICANN в 2004 году, и с тех пор мы поддерживаем регулярную переписку. Джо Каннатаки (Joe Cannataci) представляет ООН. Он будет специальным докладчиком по вопросу о праве на неприкосновенность частной жизни. Он возглавляет кафедру информационной политики и управления в Мальтийском университете, а также кафедру европейской информационной политики и технологии на юридическом факультете Гронингского университета. Надеюсь, все я сказала правильно. Ему следовало бы жить в самолете, потому что он ко всему еще

и преподает. Он является адъюнкт-профессором в Университете Эдит Коуэн в Австралии.

Мужайтесь, технари, боящиеся бесконечных дискуссий о политике. Он — дипломированный специалист по вопросам информационных технологий Великобритании и член британского общества вычислительной техники.

Здесь также присутствует Кэролайн Гёманс-Дорни (Caroline Goemans-Dorny), специалист по защите данных из Интерпола. В этой должности она занимается контролем соблюдения требований Интерпола в отношении обработки данных, работает со 190 сотрудниками, ответственными за защиту данных, от каждого из 190 национальных центральных бюро Интерпола.

Наконец, с нами сегодня Гейл Слейтер (Gail Slater), — это Кэролайн, а Гейл вон там. Гейл занимает должность заместителя председателя по законодательной и регуляторной политике организации Internet Association. Ее карьера очень близка моему сердцу. До прихода в Internet Association в 2014 году она более десяти лет работала в Федеральной торговой комиссии США, в том числе в качестве адвоката-советника Джули Брилл. Я полагаю, эксперты по защите данных помнят Джули как человека, настолько приблизившегося к управлению по защите данных, насколько это возможно в Соединенных Штатах.

Но хочу предупредить Мишель, которая сидит рядом. У Гейл двойное гражданство — Ирландии и США, — и степень магистра по европейскому и сравнительному праву, которую она получила в Оксфорде.

Наконец, Джим Гэлвин (Jim Galvin), который также не нуждается в представлении. Он состоял в обществе Интернета — в консультативном комитете ICANN по безопасности и стабильности с года его основания. Более 20 лет был активным участником IETF, и мне было интересно, вы такой энергичный именно поэтому?

Он также является директором по стратегическим отношениям и техническим стандартам компании Afilias.

Итак, у нас отличный состав. Мы хотим узнать ваше экспертное мнение и какие перспективы вы видите.

Поэтому позвольте сначала задать несколько общих вопросов господину Буттарелли.

Джованни, не могли бы вы кратко рассказать нам о фундаментальных принципах конфиденциальности, которые служат основой для законов о защите данных, включая, в частности, готовящееся положение о защите общих данных?

ДЖОВАННИ БУТТАРЕЛЛИ: Бекки, спасибо за такое вступление, и я приветствую всех собравшихся.

Я выполняю роль своеобразного ледокола, и начать хочу с того, что принципы, которые я попытаюсь кратко перечислить, основаны на принципах Евросоюза, либо содержатся в конвенции 108 Евросовета.

Защита конфиденциальности и данных все больше становится вопросом глобальным. Проведенное недавно исследование показало, что в 120 странах мира уже приняты новые положения о защите конфиденциальности и данных. То есть они значительно отходят от системы саморегулирования, и хотя некоторые принципы имеют различные названия, например, принцип ограничения целей, между ними много общего, при этом ширится сотрудничество надзорных органов на международном уровне.

Прошу вас не думать, что защита данных — это просто административная рутина и скучные требования в отношении управления интернетом. Для ознакомления вы можете взглянуть на полученные в 2014 году и опубликованные на веб-сайте нашей организации результаты анализа, в ходе которого мы пытались определить роль Европы в формировании будущего управления интернетом с точки зрения демократических ценностей и взаимоотношений с заинтересованными

сторонами в построении структуры управления, а также с точки зрения необходимости поддержки единой, целостной сети по всему миру.

Право на конфиденциальность считается во всем мире одним из основополагающих прав, в то время как защита данных как таковая в последнее время рассматривается в лишь Европе и еще в некоторых странах. Но важно то, что защита как конфиденциальности, так и данных во многих законодательствах по всему миру воспринимается как необходимое условие для других основных прав и свобод, включая, например, свободу самовыражения, право на личную индивидуальность и, о чем стали говорить в последнее время, достоинство. Вот почему в следующем году наша организация проведет в Брюсселе международную конференцию комиссии по защите конфиденциальности и данных, что позволит углубиться в вопросы этики новых технологий.

Что же насчет общих принципов?

У нас, разумеется, есть прозрачность, что означает отсутствие путаницы в том, кто и чем занимается, и именно поэтому новые принятые определения, например, как в Европе, касающиеся функций контролера и обработчика, являются ключевыми для определения соответствующей концепции с точки зрения подотчетности.

Необходимо упомянуть правомерность и справедливость. Правомерность — это не только правовые основания для обработки данных, отношения с подрядчиками, юридические обязательства, законные интересы, согласие, жизненно важные интересы контролера третьей стороны, но также логичность и соответствие с другими частями законодательства, в том числе не связанными с защитой данных, такими как, например, авторское право, потребительское право и т.п.

Сейчас, по крайней мере в Европе, конфиденциальность в конкретных случаях и вообще требует соблюдения новых принципов.

Последняя региональная концепция Евросоюза более конкретно направлена на закрепление прав субъекта данных, ужесточение надзорных полномочий компетентных независимых органов, на модернизацию существующей концепции защиты данных с использованием более последовательного подхода, позволяющего контролерам не менять свою политику в зависимости от территории.

Мы хотим, чтобы контролеры следовали принципам подотчетности в большей степени. Это значит, что органы по защите персональных данных должны быть более избирательными. Это значит, что контролеры должны больше заниматься подготовкой и определить

устойчивую политику, решать различные проблемы, определять соответствующие риски, распределять обязанности и соблюдать требования законодательства, и у вас будет соответствующая политика.

Эта правовая концепция должна применяться к физическим лицам. И поэтому понятие «персональные данные» в эпоху Больших Данных является более чем ключевым. Вы должны также определять влияние правовой концепции на персональные данные, относящиеся к физическим лицам, действующим от имени юридических лиц, таких как коммерческие организации и государственные административные органы.

Об ограничении целей я расскажу во втором раунде. Но позвольте сказать, что спустя 13 лет после конференции ICANN в Риме мы хотели бы вернуться к вопросам, которые затронули в отношении точки зрения, принятой нами в 2003 году, когда, говоря кратко, мы задали три вопроса вашему сообществу.

Первый вопрос: Почему регистратура доменного имени должна рассматриваться иначе, чем телекоммуникационные каталоги, когда, например, частное лицо регистрирует доменное имя? Значит, право не должно быть включено в реестр.

Второй вопрос, просто чтобы дать представление о том, как реализуется этот принцип на практике: Существует ли иной, менее агрессивный способ, чем обязательная публикация, который бы отвечал целям каталогов WHOIS, не открывая при этом доступ к данным для всех пользователей?

Третий вопрос относится к массовому доступу для задач прямого маркетинга.

Мы также пытались выйти к вам с предложением относительно доступа третьих сторон, правоохранительных органов. Наш прогноз 13-летней давности — и этот вывод, на мой взгляд, все еще в силе — был таким (быстро процитирую одно предложение, имеющее к этому отношение): «Цель каталогов WHOIS не может быть расширена до других целей, просто потому, что они представляют собой соблазн для некоторых потенциальных пользователей каталогов». Я хочу сказать, что это один пример, который может помочь в определении целей. И мы бы хотели помочь вам реализовать эти принципы на практике.

Это не проблема ЕС в сопоставлении с США. Это глобальный масштаб. Мы поможем укрепить доверие к интернету и принципы конфиденциальности. У нас достаточно гибкости, чтобы эффективно реализовать этот принцип на практике. Мы хотим уйти от формальных

требований. Мы хотим сосредоточиться на эффективных средствах защиты. И я считаю, что в конечном счете мы на одной стороне.

БЕККИ БЕРР: Большое спасибо.

Уилберт, не могли бы остановиться подробнее на принципах подотчетности и ограничения целей? Думаю, эти вопросы крайне важны для нашей дискуссии.

УИЛБЕР ТОУМСЕН: Спасибо, Бекки. Я попытаюсь. Только мне придется немного повторить то, что уже сказал Джованни.

Позвольте мне начать с небольшого признания: более 20... 25 лет я работал государственным прокурором. С тех пор уже более пяти лет я работаю инспектором в области защиты данных. Сочетание этих двух задач означает, что вы до некоторой степени полагаете, что вы все уже видели и все знаете. Поэтому я несколько удивлен размахом и атмосферой этого заседания, то есть я очень благодарен и признателен вам за то, что меня пригласили участвовать в этом важном мероприятии.

За столько лет вы, наверное, заметили — Джованни уже об этом говорил, — что европейские органы по надзору за соблюдением законодательства о защите данных

внимательно следят за дискуссиями об ICANN, например, о публичной доступности данных WHOIS. Мы участвовали в дебатах о последствиях WHOIS для защиты конфиденциальной информации. Но сегодня, насколько я знаю, мы впервые встретились лично, и я с нетерпением жду, когда после вводных речей мы приступим к обсуждению.

Европейцы, дамы и господа, по закону имеют полное право ожидать, что их обработка их персональных данных осуществляется исключительно в законных целях, и что эти данные не будут использоваться или храниться дольше чем необходимо для этих целей. Это означает, что обработка персональных данных должна быть законной, честной, транспарентной. Это основные принципы, уже изложенные в нашей директиве, а год назад в требованиях нашего европейского права. По сути, это означает, что вы, мы и контролеры должны собирать данные исключительно для конкретных, четких законных целей, и не должны заниматься их обработкой в порядке, несовместимом с такими целями, что мы и называем ограничением целей.

Во-вторых, ключевой принцип состоит в том, что данные, которые вы обрабатываете и, к слову, делаете публично доступными, должны быть полноценными, относящимися к делу и должны ограничиваться лишь тем, что необходимо

для целей, в которых эти данные обрабатываются. Это то, что называется минимизацией данных.

Словом, дамы и господа, давайте будем справедливыми, транспарентными и, если можно так сказать, предсказуемыми.

Один мой бывший коллега в этой связи говорил «давайте добиваться удивительной минимизации». Возможно, вот именно это... только вчера мы читали в газетах, что Тим Бернерс-Ли сказал: «Думаю, что мы скоро потеряем контроль над нашими персональными данными». Что касается меня и что касается европейских инспекторов по защите данных, справедливость, транспарентность и предсказуемость, работа в соответствии с законом — один из ответов на это.

Это ключевые принципы, и они не обсуждаются. Должен сказать, что мы, органы по защите персональных данных, никогда не устаем напоминать об этом. И это также относится, должен сказать, к публичной доступности данных WHOIS.

Думая о принципе, к примеру, ограничения целей, вы лучше меня знаете, что явная цель WHOIS — сделать доступной контактную информацию. Но с тех пор цели WHOIS были расширены, публичный доступ, доступ для правоохранительных органов, правообладателей, представителей служб безопасности.

Но суть в том, дамы и господа, что то, что персональные данные доступны в реестре, не делает законным использование этих данных для других целей просто потому, как мы уже сказали, это удобно. Чтобы ICANN, чтобы вы имели законные основания для публикации персональных данных, такая публикация должна быть действительно необходимой, соразмерной цели. И публикация не перевешивает важность неприкосновенности частной жизни пользователей.

Вам следует знать, что органы по защите персональных данных постоянно получают от людей массу жалоб о публичной доступности их персональных контактных данных через WHOIS. Данные на многих веб-сайтах, которые, к примеру, публикуют старые данные WHOIS, доступны практически любому, для любых целей, хороших и плохих.

Это должно было быть моей первой ремаркой, но позвольте мне сказать это в конце, потому что я считаю это очень важным.

Главнейшая цель, дамы и господа, новых норм, как я уже говорил, это справедливая, транспарентная и предсказуемая обработка персональных данных каждого в этой части света.

Подотчетность в работе контролеров означает способность продемонстрировать нам, органам по

защите персональных данных, соблюдение этих законных требований. Опять же, необходимость обработки данных, ограничения данных, способы информирования субъектов данных о целях и их правах несомненно будут строго оцениваться в каждой стране каждым органом по защите данных в ЕС.

Кстати, органы по защите персональных данных получили значительные полномочия по применению санкций. Но, дамы и господа, на этом я закончу. В то же время, я склонен верить в то, что организации, которые всецело придерживаются общих фундаментальных принципов, тем самым придерживаются и фундаментальных принципов защиты персональных данных, и тем самым завоевывают доверие и уважение своих клиентов. Я уверен, что за такими организациями будущее. Большое спасибо.

БЕККИ БЕРР:

Большое спасибо.

Передаю слово профессору Каннатаки. Джо, не могли бы вы... в контексте WHOIS или временного депонирования данных, к примеру, очень большой проблемой является доступ третьих лиц к персональным данным. Не могли бы вы остановиться поподробнее о доступе третьих лиц?

ДЖОЗЕФ КАННАТАКИ: Да, конечно, Бекки. Опять же, я присоединяюсь к благодарностям организаторам за то, что реализовали то, что, полагаю, уже давно пора было реализовать.

Думаю, будет лучше, если для начала мы разберемся в тех вещах, о которых уже говорил Джованни Буттарелли и другие коллеги. То есть, когда мы говорим о доступе третьих лиц, мы должны помнить о том, как родился закон о неприкосновенности личной жизни и защите персональных данных.

Собственно, если посмотреть на то, как он родился в Соединенных Штатах, и на ранние дискуссии между 1967 и 1973 годами, и на то, как он родился в Европе, то можно увидеть, что суть его в основном заключалась в том, что если вы предоставляете данные для одной цели, то предполагается, что они будут использоваться только для этой цели или для цели, которая очень ей близка. Иными словами, если вы собираете данные, к примеру, для получения кредита в банке, то вы можете их использовать исключительно для этой конкретной цели. А если вы собираете их для получения страхового полиса, то их нельзя применять для цели, отличной от этого страхового полиса, данные о состоянии здоровья и так далее.

Когда мы говорим о доступе третьих лиц, думаю, следует помнить о том, что это контекст, в котором мы должны вести обсуждение.

Во вторых, полагаю, мы все видим, как изменилась ситуация. Если вспомнить мою работу в этой сфере 33 года назад, когда я был занят обсуждениями защиты полицейских данных... нам повезло, что здесь присутствует Кэролайн, специалист по защите данных из Интерпола, которая, возможно, остановится на этом подробнее. Применяется тот же принцип.

Но если вы внимательно ознакомитесь с первыми рекомендациями и постановлениями, которые были приняты Советом Европы, то увидите, что все они были построены на принципе, когда контролер собирает большую часть данных самостоятельно, полиция, службы здравоохранения, медицинские учреждения собирают данные своими силами.

Фактически, на сегодняшний день мы значительно отошли от этой модели, полиции, медицинским учреждениям и фармацевтическим компаниям теперь не обязательно собирать данные самостоятельно, достаточно найти данные, которые кто-то однажды уже собрал. Очень часто данные собираются частными компаниями таким образом, что граждане даже не догадываются, что происходит.

Это особенно важно в ряде случаев, потому что если опросить определенные компании, работающие в интернете, они скажут, что сталкиваются с десятками

тысяч запросов на получение доступа как к метаданным, так и к контент-данным.

И эти запросы приходят не только от правоохранительных или разведывательных органов, хотя два этих аспекта тоже очень важны, поскольку одна компания сталкивается с 17000 запросов, а это огромное давление, не только на компанию, но и на соответствующие правовые системы. У нас сейчас нет времени рассматривать вопрос взаимной юридической помощи. Но если бы вы оказались на месте прокурора или следователя, то могли бы столкнуться с юридической процедурой, проходить которую пришлось бы по старинке, ожидая получения доступа к данным от какой-либо другой страны по 11-13 месяцев.

Итак, доступ третьих лиц — невероятно сложная вещь. Усугубляет проблему то, что ряд правительств, включая европейские правительства, правительство Соединенных Штатов, правительства Австралии и Новой Зеландии и ряд других, заявили, что принцип открытости данных сейчас почти так же свят, как семья и домашний очаг.

30 лет назад, когда я начинал работать в этой сфере, мы думали, что у нас есть гарантии сохранности данных. Мы думали, что это анонимизация или псевдо-анонимизация (это две разные вещи), но мы продвинулись дальше. И теперь, когда вы используете аналитику больших данных

для триангуляции данных из нескольких источников, а затем решаете открыть данные, и в какой-то момент видите, что на самом деле это уже приспособливание данных под другие цели — а зачастую так и происходит — и это приспособливание больших и открытых данных под другие цели означает, что вы предоставляете доступ к данным третьим сторонам, а это уже вопрос изменения общественной политики.

Эти и многие другие темы, напрямую затрагивающие вопрос доступа к данным третьих сторон, полагаю, очень важны в среде ICANN. Потому что это среде ICANN не только помогает предоставлять технологическую инфраструктуру, позволяющую людям связываться с другими людьми, она должна также обеспечивать способ реализации определенных политических решений. И в этом смысле код — это закон. И я должен напомнить вам, что когда дело касается доступа третьих лиц, мы не должны забывать о правовой инфраструктуре и политике всех этих государств, о чем ранее говорил Джованни Буттарелли. У нас более 102... от 102 до 120 государств, большинство из которых следует европейской модели и принципам. Это значит, что когда отступают от этих принципов, доступ третьей стороне можно предоставлять только в особых целях, то есть, в целях защиты государственной или общественной безопасности, финансовых интересов государства или пресечения уголовных преступлений,

остальное будет отхождением от этих принципов. При этом, волей-неволей это должно делаться в рамках закона, и закон должен обеспечивать соответствующие гарантии.

Поэтому, что бы ни обсуждалось в этой аудитории и в ходе процесса, который ICANN будет проводить с людьми, присутствующими здесь или участвующими дистанционно, вопрос этот необходимо решать в таком ключе. Другими словами, мы должны обращать внимание на ожидания людей, а люди ожидают решения проблем. Предприятия ожидают появления возможности ведения бизнеса на международном уровне, граждане ожидают сохранности их персональных данных по всему миру, что, повторюсь, если они работают через интернет без границ, то и ожидают гарантий без границ и решения проблем через границы. И я с нетерпением жду, что по итогу обсуждений в ICANN мы сможем определить пути решения этих проблем и поймем, какие гарантии должны быть технического характера, какие политического или юридического, а какие будут сочетать в себе все эти направления. Спасибо.

БЕККИ БЕРР:

Большое спасибо. Похоже, мы склонны полагать, что в этой дискуссии правоохранительные органы стоят по одну сторону баррикад, а сторонники защиты конфиденциальности — по другую, и компромисса им не найти. Меня поразило, что Йоханнес является главой

информационного сообщества и отдела противодействия преступности, а Уилберт на протяжении многих лет был прокурором. На очереди Кэролайн Гёманс-Дорни, прошу прощения, если неправильно произнесла имя, — специалист по защите данных из Интерпола, и я хотела бы услышать от нее, как правоохранные органы относятся к этой проблеме.

КЭРОЛАЙН ГЁМАНС-ДОРНИ: Да, хорошо. Большое спасибо за этот вопрос, и спасибо, что пригласили меня на это очень содержательное заседание. Как вы, возможно, знаете, Интерпол — это международная организация уголовной полиции, в которой состоят 190 стран-участников, и фактически она действует как международный информационный центр глобальных баз данных полиции. Мы действительно обрабатываем большие объемы информации.

И я могу заявить прямо, что, вероятнее всего, если бы с 1982 года Интерпол не разрабатывал и не применял бы на практике принципы конфиденциальности данных, этой организации сегодня бы не существовало. И это наводит меня на главный вопрос. Зачем нужны все эти принципы? Так вот, они нужны для эффективного сотрудничества полицейских сил. Необходимо, чтобы нам доверяли, нам нужна хорошая репутация, надо устранить пробелы,

особенно это касается работы на международном уровне. И здесь нам на помощь приходят строгие принципы конфиденциальности, реализованные в стандартах защиты данных. Мы в Интерполе убедились на практике, что эти принципы играют роль каркаса, на основе которого может строиться эффективное сотрудничество полицейских сил, как с технической, так и с оперативной точки зрения. По сути, это можно сравнить с закладкой крепкого фундамента, чтобы будущее здание было прочным.

Таким образом, долгосрочное инвестирование в защиту данных и уверенность в ее необходимости — это позиция, занимаемая Интерполом с давних пор. Не случайно первый регламент Интерпола в отношении защиты данных, основанный на положениях Конвенции 108, был установлен сразу же после ее принятия Евросоветом.

И это еще не конец истории. Принципы конфиденциальности разрабатывались на протяжении многих лет и были реализованы в виде подробного кодекса, содержащего 136 положений. С 1982 года он 11 раз обновлялся. То есть приблизительно каждые три года происходило обновление стандартов защиты данных.

Таким образом, защита данных — это действительно динамичный процесс. Стандарты полезны только в том случае, если они по-настоящему гибкие. И я считаю, что для Интерпола иметь гибкий регламент, который мог бы

отвечать поставленным целям — это действительно достояние. И это, конечно, постоянная проблема. Последнее обновление правил было в тысяча девятьсот... в 2016 году, в ноябре. Оно касалось укрепления роли надзорных органов, а уже сейчас мы продумываем следующее обновление, которое в частности будет затрагивать вопрос сотрудничества с частным бизнесом. Естественно, все постоянно развивается, и концепция должна соответствовать целям.

И здесь я перехожу ко второму пункту, к вопросу о репутации. Как упоминалось ранее, речь идет не только о праве на конфиденциальность или о фундаментальных правах, которые затрагиваются для эффективной работы полиции. Речь также идет о праве на свободу выражения. И Конституция Интерпола напрямую ссылается на Всеобщую декларацию прав человека. Кроме того, речь идет об принципе нейтралитета организаций, который фактически означает, что организациям запрещается вмешиваться в военные, религиозные, политические и расовые вопросы. И эти основополагающие правила также были отражены в стандартах обработки данных. В связи с этим я думаю, что дополнительное преимущество Интерпола заключается в том, что он может играть роль центра обмена информацией. Существует группа междисциплинарных аналитиков, юристов, сотрудников и офицеров полиции, которые работают днем и ночью, обрабатывая в месяц по

3000 запросов, полученных от стран-участников, сотрудничающих с Интерполом в конкретном регионе или добивающихся ареста разыскиваемых лиц.

Качество и правомерность этих запросов проверяется вручную. А также инструментами автоматизации, такими как, например, поиск по определенным словам. И кроме того, с помощью задания конкретных критериев и параметров. Роль информационной службы очень важна для Интерпола, таким образом он может гарантировать определенное качество информации и повысить эффективность сотрудничества полицейских сил.

И, наконец, третий пункт: я действительно считаю, что сила глобальных принципов конфиденциальности заключается в их универсальности и в том, что они закрывают пробелы. Пробелы из-за различий в законодательстве, в бизнес-процессах. Они обеспечивают функциональную совместимость, благодаря которой система начинает работать. Не только с технической стороны. Эти стандарты опираются на несколько основных положений, позволяющих эффективно их реализовать. Хорошо, когда имеются стандарты, но если они неизвестны, непонятны и не применяются, в них нет смысла. Итак, это эффективная реализация, потенциальные перспективы, возможность обучения, эффективный надзор и защита граждан. Стандарты Интерпола были утверждены 190 странами-участниками. И каждый находит в них себя. Сотрудничество

через Интерпол добровольное, но если вы решили сотрудничать, то кодекс становится обязательным к исполнению, существуют корректирующие меры и санкции, которые могут применяться.

В заключение скажу, что фактически, если вдуматься, принципы конфиденциальности и основанные на них принципы защиты данных на самом деле являются принципами рационального управления. Зачем вы обрабатываете? Цель. Что вы обрабатываете? Точность. На каком основании вы обрабатываете? Легитимность. Как вы обрабатываете? Транспарентность. Насколько обработка данных соответствует требованиям? Механизм надзора. Вот и все принципы рационального управления, и организации, соблюдающие эти принципы, ведут успешную деловую деятельность. Закончу на том же, с чего начала. Думаю, мы можем не волноваться о юридических стандартах только тогда, когда реализуем принципы конфиденциальности. Это непрерывный, целостный процесс — это регулирование, политика, бизнес-процессы, правильные технологии. Это, конечно, очень сложно.

И наконец, не будем забывать об очень важном аспекте — об этике. Потому что она оправдывает себя. Регламент указывает на то, что вы можете делать, а чего не можете, а этика — что вы должны делать, а чего не должны, и это очень важно в интернете. Спасибо.

БЕККИ БЕРР: Спасибо, Кэролайн.

Томас, GAC принимал участие в этих бесконечных дискуссиях и обсуждениях, я мне хотелось бы узнать ваше мнение с точки зрения GAC, когда мы перейдем к новому витку диалога.

ТОМАС ШНАЙДЕР: Спасибо, Бекки, и я приветствую всех присутствующих.

Прежде всего, мы благодарим Совет Европы за эту инициативу, которую мы полностью поддерживаем и приветствуем, потому что считаем, что эта дискуссия в Копенгагене очень своевременна и актуальна, ведь мы, как и все остальные, все больше и больше осознаем, что защита данных, конфиденциальность, а также политика в отношении данных в более широком смысле, выходящая за рамки защиты частной жизни, — это один из ключевых вопросов для наших граждан, бизнеса, правительств, институтов, международных институтов, которые наделены такими функциями, как ICANN, и они не обязательно ориентированы на конфиденциальность, но конфиденциальность становится все большей проблемой для всех, кто имеет дело с данными, а сейчас с данными работают все.

Ключевой момент заключается в том, что данные и использование данных становится основным ресурсом для инноваций, для экономических инноваций. Это инструмент, который позволяет нам делать нашу жизнь более комфортной и безопасной, и у него есть огромный потенциал для инноваций.

В то же время, конечно, существуют огромные риски злоумышленного, несанкционированного использования данных, риски потери контроля. Люди чувствуют, что теряют контроль над своими данными. Таким образом, мы сталкиваемся с ключевыми проблемами, касающимися всех нас.

И одна из таких проблем, не только для нас — правительств, — но и для граждан, и особенно для предприятий, состоит в том, что у нас разные юрисдикции и разные нормы, разные законодательства, и внутри страны тоже есть разные сегменты правительств с различными функциями. Предполагается, что одни должны защищать права своих граждан, другие должны ловить преступников, а предприятия зажаты между этими двумя, скажем так, партнерами в рамках одной и той же правительственной администрации, как на национальном уровне, так и на более глобальных уровнях.

И иногда — или часто — мы сталкиваемся с противоречивыми ожиданиями со стороны правительств

и потребителей, которые, с одной стороны, требуют защиты данных и конфиденциальности, а с другой — хотят пользоваться услугами, которые подразумевают максимальное распространение их данных и информации по всему миру, и мы понимаем, что для отрасли, для тех, кто предлагает услуги, понять, что делать в таком случае — это отдельная проблема.

Я более 10 лет представляю свою страну в Евросовете, и не колеблясь могу подтвердить слова Йоханнеса Кляйссена о том, что Евросовет превращается в организацию с участием многих заинтересованных сторон. Все большее и большее участие в нем принимают предприятия, гражданское общество, другие эксперты. Например, когда я в качестве председателя группы экспертов участвовал в разработке принципов защиты прав человека для поставщиков интернет-услуг, Совет Европы занимался этим вопросом в сотрудничестве с поставщиками интернет-услуг, гражданским обществом и экспертами по правам человека. Самое забавное, что когда мы над этим работали, мы узнали, что в том же самом учреждении — что тоже связано с должностью Йоханнеса — отдел борьбы с киберпреступностью разрабатывал для поставщиков интернет-услуг принципы обеспечения правопорядка, и нам потребовалось некоторое время, чтобы выяснить, что происходит, и как только мы поняли, то конечно собрались и обсудили все с ними, попытались

убедиться, что эти руководящие принципы для отрасли поставщиков интернет-услуг Европы не будут конфликтовать друг с другом, и нам действительно пришлось разрешить некоторые конфликты, прежде чем мы смогли опубликовать нашу работу.

Это всего лишь один пример того, насколько важно, чтобы люди собирались вместе, разрешали конфликты, и я думаю, что комиссары по защите данных впервые вышли на диалог с представителями отрасли доменных имен и других отраслей. Возможно, контакты были налажены лучше, и поэтому я очень рад, что этот диалог теперь ведется и с представителями отрасли доменных имен по всему миру, что ICANN может больше узнать о том, как осуществляется регулирование конфиденциальности в различных регионах, и люди, занимающиеся разработкой концепции новых gTLD или других служб, где есть такая проблема, могут решать ее максимально эффективно. Мы полагаем, что это возможно, наряду с существующими и разрабатывающимися регламентами. Таким образом организациям и пользователям не придется выбирать, что лучше нарушить: регламент ICANN или регламент своего государства, что, как мы знаем, происходит последние годы.

И я хочу сделать личное замечание.

У меня на родине также ведется обсуждение политики защиты данных и ее перспектив, и я думаю, все больше людей приходит к выводу, что понятие защиты данных с точки зрения запрета на использование данных — это не самый прогрессивный способ реализации наших прав в отношении конфиденциальности, потому что существуют причины, по которым данные необходимо использовать для решения проблем, чтобы сделать нашу жизнь лучше и комфортнее, если цель в этом, но речь, скорее, идет о переходе от запрета на использование данных к усилению контроля со стороны граждан, их самостоятельности, чтобы пользователи могли решать, кто может использовать их данные и в каких целях. Мы думаем о том, как можно извлечь выгоду из потенциального развития больших данных, Интернета вещей и прочего, и мы пытаемся работать в этом направлении, чтобы создать такую политику данных, которая может быть действительно полезной в 21 веке.

И эта дискуссия — часть этого обсуждения, и я надеюсь, что у нас будет еще интерактивная часть, где представители бизнеса смогут задать конкретные вопросы и поговорить о конкретных случаях. Хорошо, что это обсуждение сейчас имеет место. Разумеется, оно продолжится, будет рассмотрен ряд других вопросов на Форуме по управлению Интернетом, который мы с

удовольствием проведем в этом году с 18 по 21 декабря в Женеве. Спасибо.

БЕККИ БЕРР:

Спасибо, Томас.

Скоро мы перейдем к вопросам от аудитории. У нас есть еще две темы для краткого обсуждения.

Гейл, любые изменения контента или доступности данных WHOIS окажут влияние на предприятия, и поскольку мы пытаемся прийти к согласию, скажите, что еще нужно предприятиям, помимо тех вещей, которые мы сейчас обсуждаем?

ЭБИГЕЙЛ СЛЕЙТЕР (ABIGAIL SLATER): Огромное спасибо, Бекки.

Еще раз представляюсь, меня зовут Гейл Слейтер, я работаю в организации Internet Association. Мы находимся в Вашингтоне, округ Колумбия, и представляем более 40 международных компаний, работающих через интернет.

Мы не встречались с ICANN с момента передачи координирующей роли в исполнении функций IANA, но для нас было честью принять участие в этой работе, в частности, мы состояли в группе из 14 различных организаций, среди которых было и гражданское

общество, которое в Техасе предоставило нам экспертное заключение в отношении NTIA, и к счастью мы добились успеха, это хорошо для международного интернет-сообщества.

Итак, я постараюсь говорить кратко. Я хочу поговорить о трех вещах, и думаю, у меня около трех минут, поскольку главное для меня сегодня — это узнать ваше мнение.

Итак, с точки зрения бизнеса, я полагаю, прежде чем задумываться о том, что нужно бизнесу, очень важно сделать шаг назад, достичь в конечном счете правовой определенности, и говорить об этом в очень специфическом контексте ICANN.

Мы в ICANN. Основа и миссия ICANN — я прочту — «поддерживать операционную стабильность, надежность, безопасность, глобальную функциональную совместимость, отказоустойчивость и открытость DNS». И я думаю, веское тому доказательство заключается в том, что база данных WHOIS играет ключевое значение для этой миссии, поэтому когда мы говорим о принципах конфиденциальности, очень важно говорить о них в контексте WHOIS и понятия, которое администрация Обамы обычно называла «конкурентное равновесие». А что такое «конкурентное равновесие» с точки зрения WHOIS — вы и так знаете, я просто перечислю — это вопросы контроля товарных знаков, конфиденциальности, что,

безусловно, очень важно, защиты потребителей, предотвращения спама и мошенничества, обеспечения правопорядка. Некоторые из них связаны с конфиденциальностью, другие находятся с ней в разных плоскостях, но они создают конкурентное равновесие.

Очень важно помнить об этом.

Об этом говорилось в моем исследовании сообщества ICANN. Вспомните отчет SSAC от 2012 года, у него было замечательное название, хорошо иллюстрирующее ситуацию. Он назывался «WHOIS: Слепой и слон». Это отсылка к индийской притче о трех слепых. Их попросили потрогать слона. Каждый из них ощупывал определенную часть тела слона, а затем они сравнивали свои ощущения и не смогли прийти к одному выводу относительно того, что это за животное, что оно делает и как выглядит. Я думаю, это очень уместная аналогия, когда мы говорим о конкурентном равновесии в контексте WHOIS. Еще я должна сказать о том, что было принято в европейских законах о защите конфиденциальной информации. Несмотря на то, что конфиденциальность — это очень важный принцип в системе Евросоюза, мы получили от судебной системы Евросоюза подтверждение, что конфиденциальность должна обеспечивать справедливое равновесие между соблюдением фундаментального права на неприкосновенность частной жизни с одной стороны и, что важно в этом контексте, требованием о свободном

перемещении персональных данных с другой, и это равновесие имеет большое значение для бизнеса.

Я также отмечу, что новое европейское право, которое вступит в силу через 18 месяцев, признает этот принцип в статье 6.

Наконец, я перейду к пункту 3, который наиболее конкретно отвечает на вопрос Бекки.

Компаниям необходима правовая определенность, и прямо сейчас, как я говорила, в нашей системе есть конкурентное равновесие. Эти принципы еще не устоялись. Но бизнесу нужна правовая определенность, и если мы хотим, чтобы ЕС перешел на международный режим конфиденциальности, то в первую очередь я хотела бы задать вопрос: Правильный ли это режим? Необходимо ли нам проводить обсуждение оптимальной политики ICANN в этом отношении?

Если это так, то хочется подчеркнуть, что этот режим плохо изучен, и на сегодняшний день не поднимается вопрос о том, будет ли он применяться ко всей базе данных WHOIS или к готовящимся RDS.

Например, опять же по данным исследования, более 40% записей в базе данных WHOIS фактически внесены юридическими лицами, а не физическими лицами, а режим конфиденциальности ЕС применяется только к

физическим лицам. Для предприятий очень важно, будет ли он применяться в контексте ICANN.

Еще один критический вопрос: На какие типы данных распространяются нормы конфиденциальности, схожие с нормами режима ЕС, в контексте WHOIS?

В системе ЕС существует стандарт, который применяется к информации, позволяющей установить личность. Это вещи, которые могут быть связаны с человеком. Значительную долю базы данных WHOIS занимает техническая информация. Не персональная. Это не конфиденциальная личная информация. Опять же, для предприятий было бы очень полезно понять, на что именно распространяется стандарт конфиденциальности в контексте WHOIS, на какую информацию распространяется, на какую нет, что это за информация.

Все эти вопросы очень важны. Я благодарю вас за этот диалог, GNSO и бизнес-сообщество с нетерпением ждет его продолжения.

БЕККИ БЕРР:

Спасибо, Гейл. И последний докладчик, доктор Гэлвин.

Джим, изменение стандартов напрямую затронет отрасль доменных имен. О каких технических проблемах мы должны помнить, знать и размышлять, ведя этот диалог?

ДЖИМ ГЭЛВИН:

Бекки, спасибо за этот вопрос.

Когда я думаю о принципе конфиденциальности как таковом, и о том, как он повлияет на сообщество и какие решения необходимо реализовать, чтобы обеспечить конфиденциальность, меня беспокоят две проблемы.

Первая - это управление данными.

В каждой отрасли есть собственные внутренние технологии получения данных из одного места, копирования в другое место для хранения, резервного копирования в третье место, службы оперативного онлайн-резервирования, еще какие-либо альтернативные и вспомогательные службы, службы отчетности или каталогов, такие как WHOIS или его грядущая замена RDAP.

И конфиденциальность окажет влияние на эти возможности, на процесс перемещения данных и места их хранения. Нам необходимо подумать о сложностях, связанных с этим перемещением, о том, каким образом нам, возможно, придется изменить архитектуру или внутренние процессы, чтобы удовлетворить эту потребность.

Некоторые из этих решений будут эффективней других с точки зрения затрат, будут оказывать огромное влияние на то, что и когда можно делать, а чего нельзя.

Поэтому размышляя о политике, которую мы собираемся разрабатывать, чтобы удовлетворить требования конфиденциальности, необходимо также подумать о том, что делать с данными при их перемещении и хранении в разных местах.

Итак, это первая проблема. Управление данными.

Вторая проблема, которая меня беспокоит — это доступ к данным.

Сейчас у нас относительно открытая система, так? Каждый может получить доступ ко всем данным в любое время. По сути, система WHOIS — это то, что мы имеем на сегодняшний день в сфере служб каталогов.

Другой крайностью будет полный запрет на получение данных в любое время.

Но, полагаю, мы все осознаем, что движемся по пути создания дифференцированной системы доступа. Нам нужно разработать политику, которая распределит роли и установит, кому будет разрешен доступ, и каким образом этот доступ будет осуществляться. Мы, в сущности, создаем систему управления учетными данными, в которой нам придется определить группу людей, предоставить им учетные данные, а потом определить другую группу, которая будет использовать эти учетные

данные, чтобы каким-то образом подтвердить, что вам разрешен доступ к определенному набору данных.

Системы управления учетными данными сильно разнятся по стоимости, от дешевых до более дорогих, и в них могут происходить сбои, и, как вы знаете, на решение проблем с такими сбоями тратится очень много времени.

Например, для ознакомления, предлагаю рассмотреть следующие идеи и подумать о том, какие решения по управлению учетными данными на сегодняшний день мы имеем в сообществе.

То есть сейчас мы работаем с довольно объемными инфраструктурами DNS, многие из нас задействованы в довольно устойчивой системе, которая обеспечивает постоянный доступ к данным в реальном времени и отличается стопроцентной работоспособностью и доступна вам. В эту инфраструктуру вложены довольно крупные инвестиции.

Что касается системы управления учетными данными, если вы хотите получить подтверждение для работы с данными, получить доступ к данным, необходимо предоставить учетные данные, должна быть уверенность, что если я дам вам учетные данные, то получу доступ и могу рассчитывать на систему со стопроцентной работоспособностью, которая позволит проверить эти учетные данные и убедиться, что они существуют.

Таким образом, здесь есть над чем подумать. Мы действительно хотим пойти этим путем? А если нет, то кто будет отвечать за сбои? Какую позицию мы займем как сообщество? Какой политики мы будем придерживаться для устранения этих сбоев?

Я предлагаю подумать о еще одной технологии, с которой многие хорошо знакомы. Подумайте о существующей в мире инфраструктуре центров сертификации.

Мы наблюдали несколько довольно крупных проблем в этой отрасли. Нам следует думать о нашей политике и о том, что для нас означают эти проблемы. Как мы будем их решать? Хотим ли мы свести к минимуму риск таких проблем или собираемся признать, что они могут произойти, и как мы собираемся применять правила, которые позволяют признать их и справиться с ними, вместо того, чтобы предотвратить их изначально?

Это довольно существенные технические проблемы, одна из которых — управление данными, а вторая — доступ к данным, и чтобы удовлетворить потребности конфиденциальности, мы должны продумать решения, как это будет работать, каким образом будет осуществляться доступность, и чего мы хотим этим добиться. Спасибо.

БЕККИ БЕРР: Великолепно, спасибо. Наше время ограничено, поэтому перейдем к вопросам от аудитории, и если кто-то хочет задать вопрос, вот микрофон.

Пока люди подходят, скажу: я думаю, неважно, какой подход в отношении конфиденциальности вы принимаете. Мы слышали, что обработка персональных данных должна быть легитимной, и чтобы соответствовать стандартам прозрачности, необходимо доказывать правомерность цели. Использование данных должно соответствовать цели, нельзя, чтобы оно нарушало права на конфиденциальность частных лиц. Надо бороться за это.

Джо, я видела, что вы подняли руку, прошу.

ДЖОЗЕФ КАННАТАКИ: Небольшой комментарий, я просто подчеркну то, о чем говорили другие докладчики.

Гейл постоянно говорит о ЕС. Это можно понять, потому что ЕС только что завершил GDPR (Общий регламент по защите данных).

Но я считаю, нельзя забывать, что главное соглашение о защите данных берет свое начало в другой Европе, в Европейском Совете Это Конвенция 108. Конвенцию 108 может подписать любая страна. Уругвай подписал. Тунис подписал. Еще десять стран заняли позицию

наблюдателей. И именно эта конвенция фактически сформировала стандарт, который приняли более ста стран по всему миру.

Я говорю это, потому что считаю, что это было бы более правильно. Я не хочу быть слишком педантичным, мы можем относиться к нему как к европейскому стандарту, а не как к стандарту Евросоюза. Это не означает, что GDPR не будет оказывать колоссального влияния. Он будет оказывать огромное влияние, его требования и рекомендации, например, в отношении конфиденциальности как таковой и т. д., значительно повлияют на весь мир. Но большинство других принципов сходны с европейскими стандартами, вытекающими из Конвенции 108. Спасибо.

БЕККИ БЕРР: Большое спасибо.

Да. Просьба ко всем, пожалуйста, называйте свое имя, когда выходите к микрофону.

ЛУТЦ ДОННЕРХАКЕ (LUTZ DONNERHACKE): Лутц Доннерхаке из EURALO (Европейская региональная организация At-Large). Я был членом группы проверки WHOIS, и мы обсуждали расширенный и сокращенный вариант записи данных WHOIS. И я хочу подчеркнуть тот факт, что расширенный

вариант записи данных WHOIS предполагает, что у нас есть международная, общая, понятная правовая система. То есть у нас нет проблем с избытком или вводом данных.

С другой стороны, сокращенный вариант записи данных WHOIS распределяет данные по местам, где их собирают регистраторы. Единственная информация, которую мы имеем в сокращенном варианте записи данных WHOIS, — это информация о том, кто будет следующей ответственной стороной, как это происходит сейчас в WHOIS IANA. Если задать серверу IANA вопрос о конкретном доменном имени, они ответят: «мы не несем за него ответственности, но заключили контракт со следующей регистратурой. Спросите у них».

Если используется сокращенный или ультра-сокращенный вариант записи данных WHOIS, мы получим следующий ответ от регистратуры: «Мы продали его следующему регистратору. Спросите у него».

И если у регистратора есть данные, полученные непосредственно от конечного пользователя, который может предоставить серверу WHOIS свой местный, подчиняющийся местным законам домен, то вся собранная или предоставленная WHOIS информация никогда не покидает место, где этот закон применим.

Поэтому я призываю вас подумать о том, является ли расширенный вариант записи данных WHOIS

действительно правильным способом ведения дел.
Спасибо.

БЕККИ БЕРР:

Спасибо.

Хочу кое-что добавить, прежде чем передать слово. Насколько я понимаю, я могу найти название домена .COM, владелец которого проживает в Европе, которое будет использовать сокращенный вариант записи данных WHOIS. Но я получу доступ к регулярным данным WHOIS, сидя за своим столом в Вашингтоне. И, как я понимаю, закон о защите данных позволяет мне получить данные, не выходя из дома, что, вероятно, является перемещением данных из Европы с соблюдением этих стандартов.

Поэтому я не уверена, что мы решим проблему с помощью различия между сокращенным и расширенным вариантом записи данных.

Есть какие-либо комментарии к этому?

ДЖОВАННИ БУТТАРЕЛЛИ: Мы внимательно следим за дебатами о сокращенном и расширенном варианте записи данных. Но прежде чем дать вам рекомендацию, позвольте сказать, что, честно говоря, до сих пор не ясны цели сообщества защиты данных.

Поэтому, прежде чем решать вопросы о количестве данных, централизованной и децентрализованной системе и правах доступа — я имею в виду, исходя из законных интересов (я сейчас не говорю о правоохранительной деятельности), — я думаю, нам следует собраться и определить цели. Потому что для нас, откровенно говоря, спустя годы после того, как в 2003 году была принята наша точка зрения, все еще неясно, почему эти данные должны собираться и публиковаться именно таким образом, поэтому мы хотели бы понять, в чем цель.

Необходимо ли, чтобы контактное лицо было идентифицируемым? Нужно ли, чтобы контактным лицом был идентифицируемый человек? И правильно ли они информированы о публикации этих данных? Есть ли у вас хорошая политика в отношении вторичных целей, особенно в отношении прямого маркетинга?

Я думаю, что если мы сначала ответим на этот вопрос, то на остальные будет ответить легче.

БЕККИ БЕРР:

Спасибо.

Джеймс, прошу вас, а затем я передам слово Джиму. У вас обоих есть замечания по этому вопросу.

ДЖЕЙМС БЛЕЙДЕЛ: Надо просто принять ваше предложение о том, чтобы собраться и обсудить цели. Я знаю, что это на самом деле одно из основных направлений разработки политики RDS, о которых мы говорили выше. Я знаю, что это было проблематично для конкретно этой рабочей группы, но хорошо то, что мы намерены убедиться, что эта работа является частью предварительной подготовительной работы, которую нужно выполнить, чтобы решить некоторые из этих проблем.

ДЖИМ ГЭЛВИН: Спасибо. Я хочу подчеркнуть, что когда я говорил о существовании различных решений, которые необходимо учитывать в контексте требований конфиденциальности, вы выделили различия между существующими на сегодняшний день двумя видами решений. Это расширенный и сокращенный вариант записи данных WHOIS. И нам действительно нужно сделать шаг назад и подумать о том, какой из этих вариантов может быть более подходящим для реализации наших решений в будущем. И этот вопрос нам нужно пересмотреть, определив свою цель. Спасибо.

БЕККИ БЕРР: Спасибо.

Прошу вас.

ВИТТОРИО БЕРТОЛА (VITTORIO BERTOLA): Спасибо. Меня зовут Витторио Бертола, я представляю компанию Open-Xchange. И у меня есть пара вопросов. Для начала скажу о том, что меня разочаровало. Я не посещал заседания ICANN последние восемь лет, но до этого на протяжении десяти лет я был с ICANN, даже был членом Правления, председателем ALAC и работал в ряде других подразделений.

И мне очень неприятно, вернувшись через восемь лет, обнаружить, что за 15 лет мы не сдвинулись с места. Господин Буттарелли любезно...

[аплодисменты]

Он любезно напомнил, что эти же вопросы задавались на заседании ICANN в Риме 13 лет назад. И ICANN до сих пор не может представить убедительные аргументы в пользу того, почему эти данные необходимо собирать в первую очередь.

И немного печально, что мы все еще слышим те же самые аргументы. Я имею в виду противопоставление конфиденциальности и обеспечения правопорядка. В действительности конфиденциальность не противопоставляется охране правопорядка. Леди из Интерпола правильно высказалась об этом. Я не знаю ни одного преступника, который предоставил бы свои

достоверные данные при регистрации доменного имени для совершения преступления.

И дело не в равновесии между договорными обязательствами и законом, потому что законы важнее договорных обязательств. Извините. Дело не в том, что ICANN может заставить красть ноутбуки у своих клиентов, она не может заставить регистратуры красть данные клиентов.

Вопрос касался того, о чем говорил господин Буттарелли, что, с точки зрения информированного согласия, действительно изменится для европейских властей и для властей 120 стран, имеющих схожие законы, со вступлением GDPR в силу?

Мы действительно не видели, чтобы закон о конфиденциальности WHOIS за последние 15 лет применялся. И эти власти, я бы сказал, очень терпеливы. Но рано или поздно надо предпринять какой-то реальный шаг, чтобы применить закон.

Поэтому мне было интересно, изменится ли что-то с новым GDPR, в любом случае необходимо то сделать.

Другой вопрос адресован ICANN. Хотя я не знаю, кто на самом деле может на него ответить. Но когда европейские органы защиты по защите персональных данных направят письмо всем европейским регистратурам и регистраторам

и скажут, что им нужно прекратить сбор или публикацию определенных данных, действительно ли ICANN приостановит действие этих регистратур или регистраторов? Что будет делать ICANN? Потому что они просто исполняют закон. Спасибо.

[аплодисменты]

ДЖОВАННИ БУТТАРЕЛЛИ: Витторио, мы здесь решаем проблемы, а не ищем их, и не берем на себя роль исполнительных органов. Хотя всем нам через 14 месяцев придется перейти к исполнению. А сейчас, в отличие от того, как было 20 лет назад, за неисполнение предусмотрены серьезные штрафы.

Поэтому вопрос заключается в том, как подготовиться к первому дню, назначенному на 25 мая 2018 года. Какое это имеет отношение к остальному миру? Поскольку региональный GDPR будет применяться по всему миру, ко всем, кто предлагает товары, а в данном случае услуги, в ЕС. И, следовательно, мы не будем заботиться о серверах, о разработке и о локализации определенных услуг. Важно то, где предлагаются эти услуги. Как мы можем помочь?

Поэтому я думаю, начинать необходимо со стратегически важных вещей. На мой взгляд, стратегически важным здесь является принцип ограничения цели, это не только принцип ЕС, не только Конвенция 108. О нем говорится в конвенции

ОЭСР. В проекте первых десяти поправок к конституции США говорится о разумных ожиданиях в отношении содержания. Вы найдете его в новом японском законодательстве. Найдете его в новой судебной практике Европейского суда по правам человека. Это глобальный и стабильный элемент, я имею в виду, во всем мире. Это основа, которая требует определения цели.

Нам не нужны очень подробные цели. Но люди регистрируются. Люди, предоставляющие данные, должны понимать контекст с момента предоставления данных. Так что цели должны быть указаны. Цели должны быть ясны. Они должны быть достаточно однозначными. Четко выраженными. И я, как субъект данных, регистрирующий данные, я как контактное лицо, имею право заранее знать, куда пойдут мои данные.

Знать, что цели законны. Мы говорили об этом 15 лет назад. Поэтому мы осознаем необходимость обеспечения уровня прозрачности.

И мы просим вас, определив цели, понять пропорциональность соответствующих методов. И два вопроса, которые мы задали 13 лет назад: Вам действительно нужны расширенный и сокращенный варианты записи данных, чтобы разом сделать эти данные общедоступными? Есть ли более

пропорциональная альтернатива достижения этой цели, достижения всех целей?

Я считаю, это крайне важно. И если у нас есть проблема интерпретации принципов, мы можем помочь решить ее до реализации, потому что я уверен сразу после событий в мае 2018 года органы защиты данных станут ответственными за обеспечение соблюдения требований в этих и во многих других областях, это может случиться в июне, сентябре, декабре 2018 года. Но этот день придет. И поэтому мы хотели бы помочь вам заранее.

БЕККИ БЕРР:

Спасибо.

На очереди Гейл, Джо и Уилбер. Скоро мы закроем очередь, потому что у нас мало времени.

Итак, Гейл.

ЭБИГЕЙЛ СЛЕЙТЕР:

Спасибо. Просто краткий ответ. Я думаю, причина, по которой дебаты заняли столько времени, кроется в конкурентном равновесии, о котором я говорила ранее. То есть, я действительно думаю, что оно зависит от того, с кем вы ведете диалог внутри ICANN. И я думаю, что равновесие найдено. Я не вижу ни одной составляющей, которая бы противоречила другой в рамках системы ICANN.

Единственный руководящий принцип — Устав, а в Уставе говорится о сохранении отказоустойчивости, надежности DNS. Я не вижу ничего, противоречащего Уставу. Думаю, это важный момент, на который снова стоит обратить внимание.

Что касается данных WHOIS и их соответствия грядущему GDPR, санкций и штрафов и тому подобных вещей, то отмечу, что даже в рамках собственной правовой системы ЕС — и именно поэтому компаниям, опять-таки, нужны определенные указания — в директиве об электронной коммерции, распространяющейся на все участвующие компании, говорится о конкурентных обязательствах. В соответствии с этими обязательствами, элементы должны быть публично доступными, что очень похоже на запись данных в базу WHOIS. Будем ли мы нарушать директиву об электронной коммерции? Будем ли мы нарушать GDPR? Это очень важные для предприятий вопросы, и они сложны. Опять же, это вопрос руководства.

БЕККИ БЕРР:

Спасибо. Попрошу докладчиков быть краткими.

Джо. Нет? Ладно. Уилберт.

УИЛБЕР ТОУМСЕН: Я постараюсь быть кратким. Я могу повторить слова Джованни.

Когда я разговариваю с контролерами, для меня важен следующий вопрос: Зачем я обрабатываю эти данные? Нужно ли это и можно ли это сделать другим, менее агрессивным способом? И если речь идет о подотчетности, еще одном принципе нового и будущего европейского права, законодательства ЕС, подотчетность для меня означает уверенность в том, что вы ответили на вопросы «почему», «зачем» и «каким образом» я защищаю ваши данные. Это то, что мы требуем от контролеров. Убедите меня, что вы преследуете именно эту цель.

Я занимался этим всю жизнь. Поэтому для меня это вопрос о честном и транспарентном соблюдении требований. И в конце концов, да, нам придется их соблюдать. Возможно, даже принудительно. Но я бы предпочел быть уверенным, что контролеры данных задумываются о том, почему я это делаю. А я делаю это, соблюдая все новые принципы. Спасибо.

БЕККИ БЕРР: Спасибо. Витторио. Я знаю, что вы ждете моего ответа. Конечно, вы правы, ICANN не может принуждать регистратуры и регистраторов выбирать между своими

обязательствами по соблюдению применимого законодательства и соблюдением договора.

Да, прошу вас.

МАРИЯ ФРЕДЕНСЛУНД (MARIA FREDENSLUND): Спасибо. Меня зовут Мария Фреденслунд. Я директор организации «Датский правозащитный альянс» (Danish Rights Alliance). Это неправительственная организация по борьбе с преступлениями в сфере интеллектуальной собственности в Дании. Мы ежедневно работаем над пресечением преступной деятельности, связанной с продуктами, защищенными правом на интеллектуальную собственность. Мы также работаем с общественностью.

И мы видим, что продукты, защищенные правом на интеллектуальную собственность, фильмы или литература, все чаще используются преступниками для привлечения пользователей, чтобы взламывать их компьютеры. Так, например, веб-сайты, зарегистрированные в других странах, привлекают пользователей, обманным путем убеждают их установить вредоносное ПО, позволяющее совершать другие виды экономических киберпреступлений.

Таким образом, продукты, защищенные правом на интеллектуальную собственность, используются в

качестве способа привлечения трафика к этим веб-сайтам.

Население Дании — около 6 миллионов человек. За прошлый год было зарегистрировано более 200 миллионов посещений таких запрещенных веб-сайтов с датских IP-адресов. Это очень много. Это растущая проблема.

В интернете так много преступников именно потому, что они могут действовать анонимно. Я могу анонимно создать веб-сайт на внешнем домене и вести с этого сайта преступную деятельность, и полиция или другие организации не смогут ее пресечь. Это действительно большая проблема.

Я хочу сказать, что нам, естественно, необходимо иметь возможность осуществлять деятельность в интернете с сохранением правильного соотношения между основными правами, такими как право на конфиденциальность и другие принципы. Но проблема в том, что сейчас нарушить закон не составляет труда. На сегодняшний день у нас нет никакого способа помешать преступнику, ни в качестве правообладателя, ни в качестве полицейского органа. И одна из причин этого заключается в том, что в интернете слишком легко оставаться анонимным.

Спасибо.

БЕККИ БЕРР: Спасибо.

ДЖОВАННИ БУТТАРЕЛЛИ: Скажу как член судебных органов, хоть и связанный с сообществом по защите данных, основываясь на своем опыте в сфере уголовного права, я полностью разделяю вашу точку зрения — ни один из принципов защиты данных не предотвращает... То есть, правоохранительные органы имеют доступ к данным на законных основаниях. И, как правило, положения этих принципов препятствуют доступности системы WHOIS.

Одной из проблем является также точность данных. Точность, как правило, рассматривается как мера защиты набора данных. Это также актуально для организаций, имеющих локальный доступ к данным.

Поэтому поддерживаю ваш комментарий. Я не вижу большой проблемы.

Если проблема заключается в беспрепятственном доступе по всему миру, то это вопрос международного сотрудничества. И, опять же, принципы защиты данных — это не проблема.

ЭЛЛИОТ НОСС (ELLIOT NOSS): Здравствуйте, меня зовут Эллиот Носс, я представляю компанию Tucows. Это регистратор, который работает в данной сфере с самого начала истории ICANN. Начну с того, что я очень рад, что это заседание состоялось. Это, наверное, самое позитивное и оптимистичное заседание, на котором я присутствовал за последние пять-десять лет.

[аплодисменты]

И это потому, что сейчас в ICANN образовался дисбаланс, вы и ваше сообщество нужны нам, чтобы поддерживать нашу активность. Возвращаясь к комментариям Томаса о том, что предприятия зажаты конкурирующими интересами, скажу, что ICANN на сегодняшний день не зажата, а подвержена давлению только с одной стороны, и это интеллектуальная собственность и обеспечение правопорядка. Посмотрели бы мы, как нас зажмут.

У меня есть две просьбы. Во-первых, и это касается каждого, надо становиться более активными. Я надеюсь, что это не разовое заседание. Что это начало постоянных встреч внутри сообщества ICANN для людей, занимающихся вопросами конфиденциальности, таких как вы. И я призываю вас, в интересах всех членов GAC, присутствовать и прикладывать усилия там, где это необходимо сегодня членам GAC, преимущественно в

вопросах охраны правопорядка. Опять же, я не завидую ни сотрудникам правоохранительных органов, ни членам GAC с точки зрения их нынешней позиции, но они не зажаты.

Во-вторых, я считаю, что ICANN необходимо учредить подразделение, отвечающее за конфиденциальность, укомплектованное специалистами в сфере конфиденциальности, которым предоставлены реальные полномочия. Поскольку потребности этого сообщества глобальны. Они должны учитывать национальные интересы, но существуют уникальные международные элементы, с которыми мы сталкиваемся на уровне юрисдикции, с точки зрения конкретных механизмов и конкретных подходов. И только если ICANN предпримет этот шаг, мы действительно сможем получить международные гарантии и международные средства защиты. Спасибо.

[аплодисменты]

БЕККИ БЕРР:

Спасибо. Думаю, мы... мы это обсудим. На самом деле GDPR может потребовать, чтобы у нас был сотрудник, отвечающий за конфиденциальность. Матье.

МАТЬЕ ВЕЙЛ (MATHIEU WEILL): Большое спасибо, Бекки, и благодарю вас всех присутствующих. Меня зовут Матье Вейл. Я

исполнительный директор организации AFNIC, которая является менеджером ccTLD во Франции, а также поставщиком регистратур для ряда gTLD в Европе.

Это еще одна перспектива отрасли. Я, как и Эллиот, думаю, что будущее намного ярче, чем прошлое. И мой комментарий — это ответ на слова Джеймса, очень уважаемого во всем мире специалиста данной отрасли. Мы, как ccTLD, очень обеспокоены этим регламентом. Мы всегда относились очень серьезно ко всему, что связано с конфиденциальностью. И я думаю, при ближайшем рассмотрении, проблемы, о которых говорил Джеймс, слишком преувеличены. Это не такой пробел, чтобы, будучи человеком, работающим в доменной отрасли, изучать различные принципы, лежащие в основе GDPR. И я думаю, это действительно важно. Мы открыты для обсуждения в отрасли, в GNSO. Мы также проводим эти обсуждения среди европейских ccTLD. Необходимо обмениваться информацией, чтобы точно понять проблемы с точки зрения практикующего специалиста отрасли. Нам нужны не только органы защиты данных. Надо начать с себя, проанализировать свои процессы и понять, что именно означает «следовать принципам этого регламента». И мы, такие как Эллиот, поддерживаем эти принципы. Мы живем ими, когда думаем об интернете как о равном уважительном отношении к людям и сообществам людей.

И поэтому нам нужно научиться говорить: «Так, этот регламент был нам навязан, поэтому он неизбежно плох», и хорошо, что это подталкивает нас в правильном направлении. И, безусловно, проблемы существуют, особенно для специалистов, работающих на международном уровне, но их можно решить, если обратиться для обсуждения, без борьбы, если попытаться найти правильные решения. Потому что эти решения существуют уже давно. И мы можем их найти. Я снова призываю ICANN и всех остальных, в первую очередь надо упорядочить эти процессы, чтобы помочь регистратурам и регистраторам, исполняющим требования регламентов, чтобы они не утаивали от ICANN получение разрешений на отступление от требований или другие процессы. Думаю, что это первоочередная задача, наряду с сотрудничеством и укреплением позиций в отрасли.

ДЖЕЙМС БЛЕЙДЕЛ: Спасибо, Матье. Уточню, вы имели в виду Джеймса Гэлвина?

МАТЬЕ ВЕЙЛ: Да, конечно.

ДЖЕЙМС БЛЕЙДЕЛ: Думаю, он хочет ответить, очень кратко. Спасибо.

ДЖИМ ГЭЛВИН: Да, спасибо. Я хочу сказать, что я согласен с вами. Не в том, что проблемы преувеличены, а в том, что решение начинается с нас, что мы, как сообщество, должны собраться провести эти обсуждения. Я вижу, что мы создаем новую систему управления учетными данными, — и может быть надо провести это обсуждение в живую, провести много обсуждений, потратить много времени, чтобы разобраться в этом вопросе — система управления учетными данными в глобальном масштабе — это то, чего мы не могли достичь ни в какой отрасли. У нас нет системы управления учетными данными глобального масштаба, которая бы занималась проверкой подлинности, как в отношении работы с учетными данными, так и в отношении доступа в режиме реального времени к проверке учетных данных как таковых, и другой работы такого рода. Это мое наблюдение. Думаю, что по мере продвижения в этом направлении мы столкнемся с реальными проблемами, с которыми никто из нас вообще никогда не сталкивался прежде. Мне бы хотелось продолжить обсуждение по этим вопросам.

МАТЬЕ ВЕЙЛ: Спасибо.

БЕККИ БЕРР: Спасибо. В 17:00 здесь будет проводиться общественный форум. Я прошу оставшихся говорить как можно более кратко. Мы выслушаем все ваши вопросы, а затем постараемся очень быстро ответить.

ВИКТОРИЯ ШЕКЛЕР (VICTORIA SHECKLER): Спасибо. Меня зовут Вики Шеклер. Я представляю рабочую группу RDS, и у меня есть вопрос из двух частей, я его прочту. Извините за это. Что касается соответствия субъектов ЕС требованиям GDPR, было бы достаточно правомерно, если бы в согласованной политике ICANN были определены новые RDS, которые позволяют контролировать доступ к регистрационным данным, не запрашивая официального согласия субъекта данных для каждого типа использования — для целей использования, например, для пресечения уголовных или гражданских правонарушений? С другой стороны, многочисленные заинтересованные стороны в ICANN предложили, чтобы конечные пользователи или владельцы домена, получающие выгоду, запрашивали разрешение на дальнейшее использование регистрационных данных, что позволило бы разрешить спор по поводу конфиденциальности регистрационных данных,

доступных через WHOIS, например, для целей исполнения уголовного или гражданского права.

Каково ваше мнение по обоим этим вопросам, в контексте процесса согласования PDP как определения пропорциональности, и использования данных третьими сторонами или использования согласия как механизма для легитимных, соразмерных закону целей. Спасибо.

БЕККИ БЕРР:

Спасибо. Это очень хорошие вопросы. У нас мало времени, поэтому я предлагаю ответить на них в автономном режиме. Кит.

КИТ ДРАЗЕК (KEITH DRAZEK): Спасибо, Бекки. Всем привет. Кит Дразек. Я представляю компанию VeriSign. Я не собирался сегодня задавать вопросов, но не смог оставить без внимания обсуждение расширенного и сокращенного варианта записи данных. Для тех, кто не очень внимательно следил за этим процессом, в 2014 году была принята политика в отношении расширенного варианта записи данных WHOIS, которая фактически требует, чтобы регистратуры .COM and .NET компании VeriSign перешли с сокращенного на расширенный вариант записи данных, что позволит эффективно собирать данные WHOIS для 142 миллионов записей доменных имен от наших

регистраторов. Многие из них находятся в Соединенных Штатах, а многие другие — нет. И в свете нового регламента, в свете изменившихся с 2014 года, когда была принята политика ICANN, обстоятельств, мне интересно, что вы думаете о последствиях передачи массы записей 142 миллионов доменных имен для наших регистраторов с точки зрения юрисдикции? И в частности, учитывая грядущие события 2018 года с новыми правилами и возможностью внедрения новой RDS? На этом я остановлюсь и с удовольствием выслушаю ваши ответы, сейчас или позже. Спасибо.

БЕККИ БЕРР:

Спасибо. Это тоже очень хорошие вопросы, но, вероятно, они требуют большего времени, чем у нас осталось. Сюзан, у вас есть вопрос?

СЮЗАН КАВАГУЧИ:

Нет, это один из вопросов (неразборчиво).

БЕККИ БЕРР:

Это не разовое заседание. Это начало диалога. Я выражаю большую благодарность Совету Европы за то, что он привлек к этому обсуждению новых замечательных экспертов и специалистов, и благодарю всех вас за то, что посетили это обсуждение. И да, Найджел, я иду.

[аплодисменты]

НАЙДЖЕЛ ХИКСОН: Большое спасибо, Бекки. Это было отличное заседание, а сейчас нам надо покинуть аудиторию, потому что через девять минут здесь начнется общественный форум.

[КОНЕЦ СТЕНОГРАММЫ]