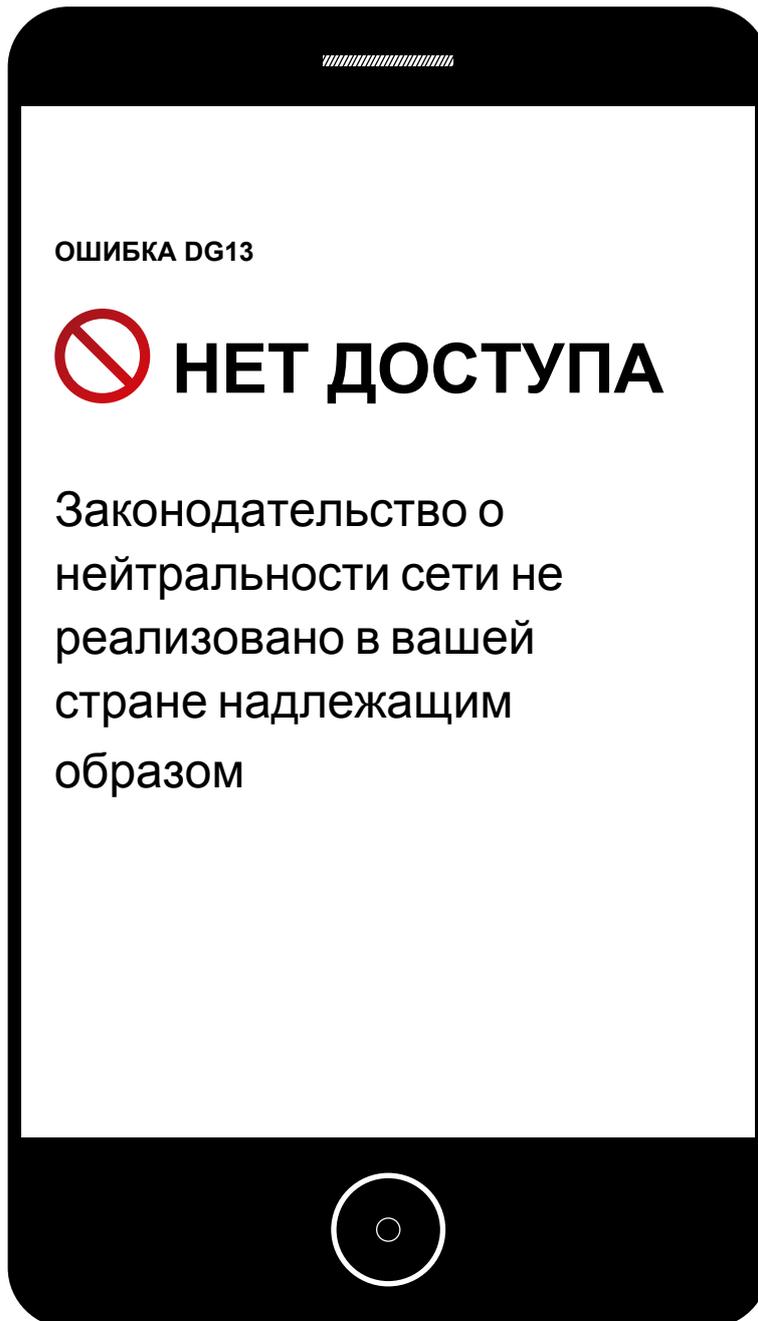


НЕЙТРАЛЬНОСТЬ СЕТИ



Что такое
нейтральность сети?
[СТР 5](#)

10 аргументов в пользу
нейтральности сети
[СТР 10](#)

Заблуждения и
факты
[СТР 13](#)

EUROPEAN
DIGITAL
RIGHTS

Принцип нейтральности сети основан на возможности в любой точке сети установить соединение с любой другой точкой сети, не подвергаясь дискриминации по месту происхождения, месту назначения, либо по типу пересылаемых данных.

Этот принцип - основа успеха интернета. Нейтральность сети – необходимое условие для инноваций, конкуренции и свободного обмена информацией. Более того, нейтральность сети позволяет интернету служить инструментом реализации таких гражданских прав, как право на свободу самовыражения и право получать и передавать информацию.

В этой брошюре мы расскажем о нейтральности сети, о том, почему это важно, почему определенные интернет-провайдеры считают, что им выгодно нарушать этот принцип, и развеем некоторые распространенные заблуждения.

**“Позволить провайдерам
широкополосного доступа контролировать
то, что люди читают, видят или создают
онлайн, - значит нарушить
фундаментальные принципы, сделавшие
интернет таким популярным”.**

- Винтон Серф, отец-основатель интернета⁰¹

- СТР 5** **ЧТО ТАКОЕ НЕЙТРАЛЬНОСТЬ СЕТИ**
СВОБОДА КОММУНИКАЦИЙ В ЦИФРОВУЮ ЭПОХУ
- СТР 8** **ПРИЧИНЫ НАРУШЕНИЯ НЕЙТРАЛЬНОСТИ СЕТИ**
ТРИ ГЛАВНЫЕ ПРИЧИНЫ
- СТР 10** **10 АРГУМЕНТОВ В ПОЛЬЗУ НЕЙТРАЛЬНОСТИ СЕТИ**
- СТР 13** **ЗАБЛУЖДЕНИЯ И ФАКТЫ**
- СТР 16** **СИТУАЦИЯ В ЕВРОПЕЙСКОМ СОЮЗЕ**
В ОЖИДАНИИ НЕЙТРАЛЬНОСТИ СЕТИ
- СТР 20** **ПРИМЕР НИДЕРЛАНДОВ**
КЕЙС-СТАДИ
- СТР 22** **ДЕСЯТЬ ПУНКТОВ ПО ЗАЩИТЕ НЕЙТРАЛЬНОСТИ СЕТИ**
- СТР 23** **ГЛОССАРИЙ**
- СТР 25** **ПРИМЕЧАНИЯ**

ЧТО ТАКОЕ НЕЙТРАЛЬНОСТЬ СЕТИ

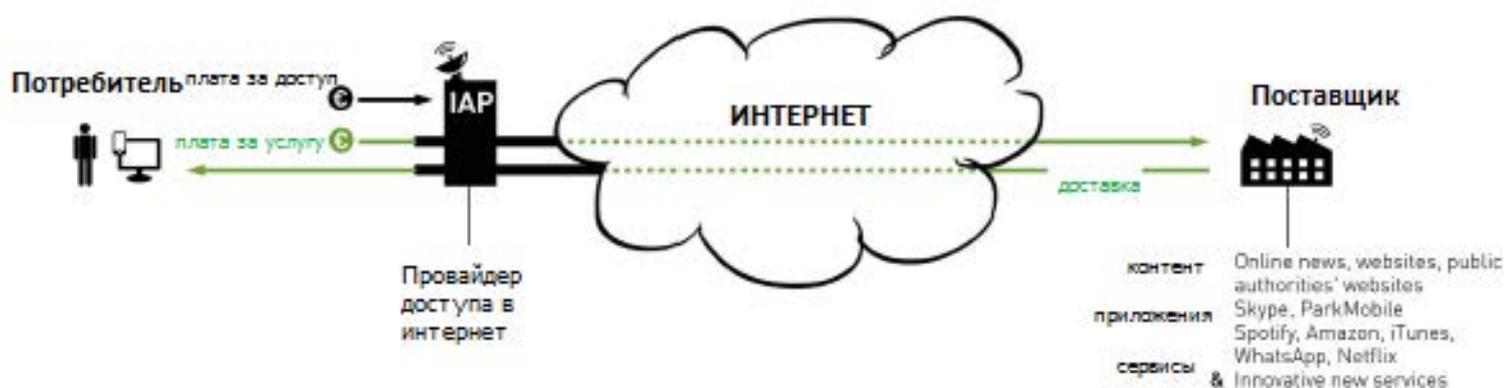


Рис. 1: модель открытого нейтрального доступа

СВОБОДА КОММУНИКАЦИЙ В ЦИФРОВУЮ ЭПОХУ

Интернет – глобальная, децентрализованная, автономная сеть взаимосвязанных компьютеров. Доступ к интернету можно получить через соединения, предоставленные провайдерами интернета.

Эти провайдеры передают информацию, которую мы пересылаем через интернет, так называемыми «пакетами» данных. Способ, которым в интернете передается информация, можно сравнить с почтовой пересылкой страниц книги во множестве разных конвертов⁰².

Почтовое отделение может выслать конверты со страницами по разным маршрутам на один адрес. Когда письма приходят адресату, страницы можно достать из конвертов и разложить в правильном порядке.

Подключаясь к интернету, к каждый из нас становится адресатом этой глобальной сети с возможностью подключиться к любому другому адресату. Неважно, кто этот адресат – компьютер другого пользователя (“peer-to-peer”), вебсайт, электронная почта, видео или что-то еще.

Успех интернета основывается на двух простых, но необходимых компонентах его архитектуры:

1. Каждое подключенное устройство может соединиться с любым другим подключенным устройством.
2. Все службы используют “интернет-протокол”, достаточно гибкий и простой для передачи любого контента (видео, почта, сообщения и т.д.) в отличие от сетей, разработанных для одной цели, например, системы голосовой телефонии.

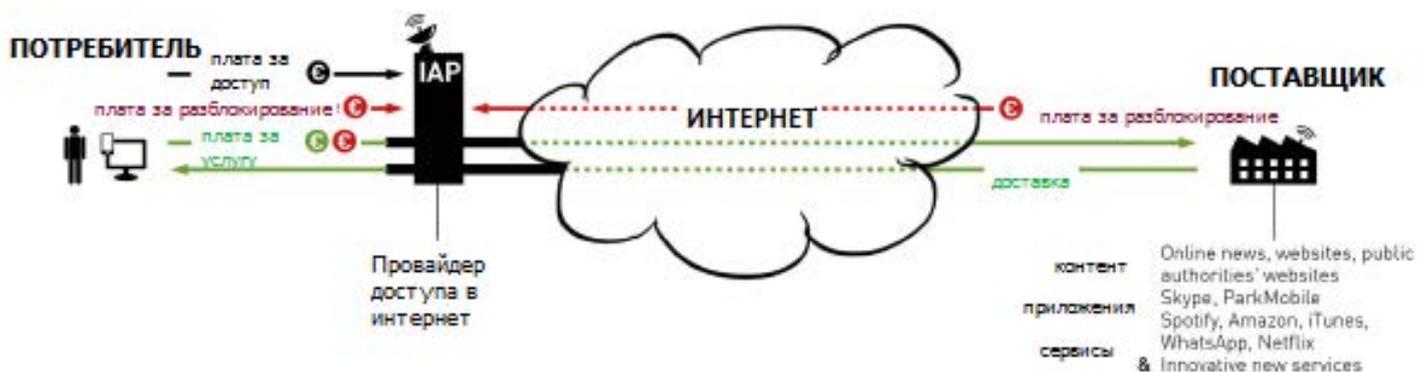


Рис. 2: Модель не-нейтрального доступа

Нейтральность сети чаще всего определяется как принцип, в соответствии с которым пользователи интернета могут подключиться к любой точке сети. Пользователи могут создавать, получать и предоставлять доступ к любому контенту, сервису или приложению, без дискриминации и каких-либо ограничений со стороны тех, кто управляет инфраструктурой.

Провайдеры доступа к интернету позволяют нам общаться, просматривать веб-страницы и передавать файлы через интернет, предоставлять глобальный доступ к нашим веб-сайтам и пользоваться такими сервисами, как электронная почта, социальные медиа или интернет-телефония. Любой человек или организация любого типа и размера могут функционировать по всему миру и в любой роли. Каждый может пользоваться сервисами и предоставлять их.

Предположим, вы хотите посмотреть онлайн-видео: вы подключаетесь к интернету, открываете браузер и идете на ваш любимый видео-сервис. Это возможно благодаря тому, что провайдер не пытается ограничить ваш выбор.

Когда принцип нейтральности сети не соблюдается, вы можете внезапно обнаружить, что скорость подключения к видео-сервису была снижена вашим провайдером настолько, что посмотреть видео невозможно. В то же время скорость подключения к видео-сервису 2 может быть высока, и вы, возможно, сможете увидеть там тот же самый контент. Почему ваш провайдер может так поступать? Есть множество причин. Например, провайдер может а) заключить эксклюзивный договор с видео-сервисом 2 или б) ограничивать доступ к сервису 1, потому что владеет сервисом 2 и хочет привлечь к нему больше пользователей.

Это только часть причин, которые приводят к нарушению принципа нейтральности сети. Такие дискриминационные методы иногда называют «управлением траффиком». Мы подробнее рассмотрим причины нарушений принципа нейтральности сети, в следующей части.

"Я не верю в то, что ограничение выбора потребителей сможет когда-нибудь вызывать рост. Я не считаю, что ограничение доступа к интернету привлечет больше новаторских интернет-компаний. И я не считаю, что ограничение доступа к интернету – правильное решение проблемы ускорения развертывания сетей доступа следующего поколения."

- Вице-президент Еврокомиссии Вивиан Реддинг, сентябрь 2008¹³

ПРИЧИНЫ НАРУШЕНИЯ НЕЙТРАЛЬНОСТИ СЕТИ

ТРИ ГЛАВНЫЕ ПРИЧИНЫ

Есть много причин, по которым нарушается нейтральность сети. Вот наиболее распространённые:

Провайдеры нарушают сетевую нейтральность ради увеличения прибыли

Некоторые провайдеры требуют права блокировать или замедлять трафик ради коммерческой прибыли. Провайдеры не только контролируют соединение с интернетом, но и предлагают все больше контента, услуг и приложений. Они все активнее ищут возможности стать «привратниками» интернета. Например, голландский провайдер KPN попытался заставить своих клиентов пользоваться мессенджером KPN вместо чат-сервисов, базирующихся в сети, блокируя эти бесплатные сервисы. Другой пример дискриминации -- блокирование T-Mobile сервисов интернет-телефонии (голос по IP, сокращенно VoIP), таких как Skype, чтобы усилить позиции как свои, так и своих партнеров по бизнесу.

Провайдеры нарушают нейтральность сети с целью цензуры.

В Великобритании провайдеры интернет-доступа часто злоупотребляли возможностями блокирования для закрытия доступа к нежелательному контенту. Так, 4 мая 2012 г., сайт противников насилия “Conciliation Resources” был случайно заблокирован фильтрами защиты детей на мобильных сетях Великобритании⁰⁴.

Еще один пример – Virgin Media. Компания предоставляет доступ к интернету и все чаще использует технологию Deep Packet Inspection (DPI – см. таблицу на стр.9). Теперь Virgin использует ту же самую технологию, нарушающую конфиденциальность, чтобы контролировать свою сеть в целях защиты своего музыкального бизнеса⁰⁵

В каждом из этих случаев частные компании контролируют подключения своих пользователей, чтобы цензурировать то, что эти компании считают нежелательным контентом.

Провайдеры нарушают нейтральность сети, следуя законодательству

Правительства все чаще просят провайдеров ограничить определенные типы трафика, чтобы осуществлять контроль и мониторинг интернета в целях усиления власти закона. Десять лет назад, только четыре страны в мире цензурировали и фильтровали интернет – сегодня таких стран больше сорока⁰⁶.

Бельгия, Франция, Италия, Великобритания и Ирландия – лишь некоторые из европейских стран, блокирующих вебсайты. Сайты блокируются по множеству причин, начиная от защиты национальных игровых монополий и заканчивая введением очевидно неэффективных мер по защите интеллектуальной собственности. Некоторые политики призывают как к нейтральности сети, так и к блокированию и фильтрации сайтов и контента. Однако попытки создать для провайдеров законодательные стимулы тратить средства на мониторинг и фильтрацию или блокировку – с одной стороны, и требуя, чтобы они не использовали эти технологии для создания конкурентных преимуществ своего бизнеса, парадоксальны.

Deep Packet Inspection (DPI)

Информация, которую мы посылаем и получаем через интернет, путешествует в так называемых «пакетах», «снаружи» которых есть информация об отправителе и получателе. В отличие от обычного сетевого оборудования, DPI позволяет получить не только информацию об отправителе и получателе, но и о содержании пакета, и может использоваться для блокировки или разрушения пакетов, основываясь на их содержимом.

DPI может использоваться как для безвредных целей (борьбы со спамом или вирусами), так и для наблюдения или цензуры информации. Эта технология позволяет захватывать и анализировать информацию из сетевого трафика в реальном времени. Например, в России, технологии Cisco Deep Packet, по некоторым сведениям, используются правительством для блокирования доступа к определенным сайтам. Инструменты 07 Cisco DPI также используются в Германии компанией T-Mobile 08 для мобильных



В ПОЛЬЗУ

НЕЙТРАЛЬНОСТИ СЕТИ

причина

01

Отсутствие дискриминации

Нейтральность сети - принцип, по которому ко всем типам контента, а также ко всем отправителям и получателям, относятся одинаково. Данный принцип поддерживает право на свободу выражения мнения, включающий, в соответствии со статьей 19.2 Международного пакта о гражданских и политических правах ООН, свободу искать, получать и передавать информацию и идеи любого вида. Без нейтральности сети,

провайдеры доступа в интернет стали бы стражами контента интернета, обладая властью над тем, что мы можем писать и читать, и с кем можем поддерживать коммуникацию.

причина

02

Свобода самовыражения

История интернета четко показывает: нейтральность сети поощряет творческое самовыражение. Способность публиковать контент и выражать мнения онлайн не зависит от финансового или социального

статуса, и не является исключительным правом элиты. Число людей, обменивающихся информацией и опытом онлайн (веб 2.0) непрерывно растет. Это означает, что отдельные люди, мелкие организации, традиционные источники новостей и крупные компании могут создавать контент, доступный всем.

Нейтральность сети позволяет информации распространяться в сети без блокирования или ограничения, создавая среду, благоприятную для новых идей и инноваций.

причина
03

Конфиденциальность

- меры, направленные на подрыв нейтральности сети, могут оказывать прямое влияние на неприкосновенность нашей частной жизни (DPI – см. стр. 9). Не-нейтральный интернет означает, что провайдеры смогут проверять наши коммуникации, чтобы знать, что в них: обмен сообщениями, потоковые мультимедиа, peer-to-peer (P2P), электронная почта и так далее. В соответствии с последним исследованием, некоторые европейские провайдеры уже делают это с помощью Deep Packet Inspection (DPI) в целях получения прибыли⁰⁹. Использование этой технологии правительствами или разведками неизбежно.

"Концепция нейтральности сети основывается на том, что информация в интернете должна передаваться без предвзятости, безотносительно контента, источника или назначения. Собирая информацию об интернет-коммуникациях пользователей, провайдеры могут нарушать существующие правила конфиденциальности коммуникаций - фундаментального права, которое необходимо защищать. Серьезное обсуждение политики нейтральности сети должно обеспечить эффективную защиту конфиденциальности коммуникаций пользователей.

- Европейский Контрольный Орган Защиты Персональных Данных (EDPS) о нейтральности сети.

причина
04

Доступ к информации

- нейтральность сети также служит катализатором создания многообразного и многочисленного онлайн контента. Некоммерческие проекты, такие, как Википедия, блоги и пользовательский контент имеют в целом такие же возможности предоставления доступа и распространения информации в интернете, как и большие, коммерческие компании. Без нейтральности сети нам грозит двухуровневый интернет, где только те, кто платит за информацию, будут иметь доступ к ней.

причина
05

Демократичность

- нейтральность сети способствует развитию демократии, позволяя интернету оставаться открытым форумом, где все голоса имеют равные права. Нейтральность сети гарантирует, что возможность озвучивать свою точку зрения и размещать контент онлайн не зависит от финансового или социального статуса. Это мощный инструмент усиления демократии, позволяющий выражать мнение и быть услышанными огромному числу самых различных мнений.

причина 06 **Инструмент против цензуры**

операторы сетей могут блокировать не только сервисы,

но и контент. Фундаментальные изменения коммуникационных технологий последних 10 лет помогли революциям и облегчают социальные реформы, обеспечивая прозрачность и свободу информации.

причина 07 **Выбор**

-нейтральность сети обеспечивает доступ к контенту и расширяет выбор, позволяя большему числу игроков выйти на рынок. Это стимулирует темпы роста источников информации онлайн, интеллектуальный и культурный обмен, которые не были бы возможны двадцать лет назад. Без нейтральности провайдеры могут отдавать приоритет контенту, создавая "огороженные сады", и ограничивать выбор.

причина 08 **Инновация и конкуренция**

- нейтральность сети продолжает стимулировать инновации; компании и отдельные люди могут создавать контент и новые услуги для онлайн-аудитории. Каждый может размещать контент без особых затрат. Интернет без ограничений обеспечивает доступ к рынку малым и средним предприятиям, стартапам, которые иначе могут не иметь конкурентных преимуществ перед большими корпорациями. Без нейтральности сети провайдеры могут ограничивать доступ, нужный новаторам, которые пытаются разработать онлайн-сервисы. Рынок, доступный новаторам, будет более узким и менее предсказуемым. Например, стартап не получит доступа к клиентам всех провайдеров, либо же для этого придется платить тысячам провайдеров.

причина 09 **Единый цифровой рынок**

Нейтральность сети - краеугольный камень

единого цифрового рынка, который снимает барьеры и дает пользователям возможность свободно общаться, выражать мнения, получать доступ к информации и участвовать в общественных обсуждениях без ненужного вмешательства со стороны посредников. Не-нейтральный интернет, с другой стороны, способствует фрагментации единого цифрового рынка. Европейский Парламент признал эту опасность, приняв резолюцию по "Созданию единого цифрового рынка" ¹⁰ (2012), и призвав комиссию разработать законодательство по обеспечению нейтральности сети.

причина 10 **Защита глобального интернета**

- Как только провайдеры начнут использовать инструменты по дискриминации трафика и вмешиваться в глобальную коммуникацию в целях повышения коммерческой прибыли, правительства могут захотеть использовать такие же технологии в целях влияния на политическую жизнь - уже сейчас западные правительства все чаще обращаются к провайдерам с просьбами ограничить определенные виды трафика и фильтровать и мониторить интернет с целью соблюдения закона. В других частях мира это привело к созданию "национального интернета", в частности, "Chinternet" в Китае и "халяльный" интернет в Иране. Принцип нейтральности сети позволит сохранить глобальный интернет.

Заблуждения и факты

Дополнение от Access

Миф 1

Нейтральность сети может ухудшить инфраструктуру - кто будет за нее платить?

Фактор, стимулирующий капиталовложения в широкополосный доступ - доступность контента. Доходы от предоставления доступа в интернет зависят от спроса на сетевой контент и приложения. Это было эмпирически доказано исследованием PLUM¹¹, показавшим, что "способность потребителей иметь доступ к контенту, приложениям и сервисам интернета - причина, по которой они платят провайдерам. Провайдеры зависят от этого спроса, если хотят, чтобы их вложения окупились."

Некоторые провайдеры интернета утверждают, что создатели контента и приложений пользуются капиталовложениями в инфраструктуру, сделанными другими, и ничего не платят. Это утверждение безосновательно, т.к. пользователи уже платят за возможность доступа к интернету, что позволяет провайдерам получать прибыль со своих вкладов в сети.

Создатели и распространители контента и услуг тоже платят за доступ к сети. Более того, спрос клиентов на использование P2P и потоковой музыки вызывает спрос на более быстрые подключения к интернету, приносят большую прибыль провайдерам и, в конечном счете, стимулирует развитие инфраструктуры.

Миф 2

Законы о нейтральности сети усложняют контроль за сетями. что приведет к снижению качества доступа

Законы о нейтральности сети не будут мешать провайдерам управлять своими сетями. На самом деле, Transmission Control Protocol ("flow rate fairness"), являющийся инженерным ядром интернета, - один из лучших инструментов, предотвращающих "заторы", который и позволил стать интернету таким популярным. Нейтральность сети устраняет не менеджмент трафика, а ограничения, которые могут ввести провайдеры для получения дополнительной краткосрочной прибыли.

Миф 3

Взимание оплаты с распространителей контента и приложений поможет увеличить капиталовложения в развитие широкополосного доступа

Некоторые провайдеры многократно озвучивали свое желание взимать плату с распространителей контента и приложений – вдобавок к тому, что платят конечные пользователи – утверждая, что это увеличит капиталовложения в сети следующего поколения. Это опасный подход, так как нет гарантий, что провайдеры будут вкладывать доход в инфраструктуру. На самом деле они могут начать вкладывать меньше, так как низкокачественный "базовый" доступ может увеличить спрос на более дорогие "премиум" услуги доступа.

Миф 4

Законы о нейтральности сети не важны, ведь покупатели могут "голосовать рублем"

Еврокомиссия многократно заявляла, что если компания-провайдер ограничивает доступ к интернету, клиенты могут изменить свой выбор в пользу провайдеров, не ставящих таких ограничений. Но если я владелец бельгийского сайта, блокируемого в Польше, Греции и Испании, я не могу ничего сделать, так как не являюсь клиентом зарубежных провайдеров, нарушающих мою свободу.

С точки зрения клиентов, менять провайдера в сфере, где распространены долгосрочные контракты, проблематично, так как возможность сменить провайдера может быть нереализуема.

Конечные пользователи могут, в итоге, иметь ограниченный, низкокачественный и медленный доступ или быстрый доступ с меньшим числом доступных ресурсов, даже не зная об этом.

Миф 5

В регулировании нет нужды, рынок расставит все по местам

Это ложная дилемма. Конкуренция хоть и является необходимым для здорового рынка механизмом, но тем не менее не препятствует провайдерам проводить не-нейтральную политику. Регулирование не может основываться исключительно на прозрачности и конкуренции. Очевидно, что законы конкуренции слишком медленно действуют и не эффективны в решении проблемы. В свете растущего количества попыток провайдеров препятствовать пользователям в доступе к интернету, можно предположить, что свобода рынка приведет к развитию многослойного интернета. А это плохой вариант для граждан.

Миф 6

Цены растут из-за роста объема данных

Это неверно как для стационарного, так и мобильного доступа. Для стационарного доступа, затраты, относящиеся к трафику, являются небольшим процентом от дохода, так как принцип "одна линия доступа для одного домашнего хозяйства" обеспечивает рост трафика без роста затрат. Для кабельных и мобильных сетей проблема в другом, так как кабельные и радиосети делятся между пользователями, и затраты на дополнительную

пропускную способность значительно выше, чем для стационарных сетей. Тем не менее, переход от 2G к 3G и 4G для мобильных и от EuroDOCSIS X к 2.0 (и скоро к 3.1) для кабельных сетей привел к значительному уменьшению затрат на передачу трафика. Это значит, что несмотря на более высокую стоимость мобильного доступа, затраты на единицу уменьшаются. В таком случае, рост трафика приводит не только к увеличению рентабельности для провайдеров, но и потенциально к меньшим затратам на пользователя сети.

Миф 7

Нейтральность сети повредит инновациям

То, что нейтральность сети может повредить инновациям, неверно. В реальности, верно обратное: отказ от принципа нейтральности сети ограничит свободу вести бизнес для распространителей контента и приложений. Как сказано в части 3, отсутствие нейтральности повредит инновационности контента, так как стартапы и мелкие компании вынуждены будут преодолевать барьеры для выхода на рынок, не говоря уж о возможности возникновения все новых барьеров. Это ограничит защищаемую Хартией Европейского союза по правам человека свободу новаторов распространять информацию и вести бизнес.

Миф 8

Наша сеть, что хотим, то и делаем.

Интернет в самом деле "по-настоящему публичное пространство,

открывающее новые горизонты свободы и служащее инструментами для защиты этой свободы"¹² Граждане привыкли полагаться на стабильный, открытый и надежный интернет для защиты своих фундаментальных прав, включая право на самовыражение, доступ к информации и свободу ассоциаций. Эти права подтверждаются ООН, признающей ответственность корпораций за соблюдение прав человека. Кроме того, делегация ЕС на 7 Международном форуме о вопросах управления интернетом (IGF) в 2012 г. заявила, что "интернет не просто технология или цифровой рынок".

Миф 9

Нейтральность сети - проблема США, а не Европы

Существует множество доказательств того, что европейские провайдеры, особенно провайдеры мобильного доступа, используют технические средства для манипуляции доступом конечных пользователей к интернету в целях продвижения своих коммерческих интересов.

К примеру, последние находки BEREC (Совета европейских регуляторов в области электронных коммуникаций) показывают, что такая проблема в Европе есть. Все больше и больше провайдеров ограничивают доступ к контенту (сайтам P2P), сервисам (VoIP), и ухудшают качество доступа к интернету. Кроме того, доказательства, собранные такими гражданскими платформами, как Glasnost¹³ и Respect My Net¹⁴ дают ясную картину многочисленных и вредных нарушений нейтральности сети в Европе.

СИТУАЦИЯ В ЕВРОПЕЙСКОМ СОЮЗЕ

В ОЖИДАНИИ НЕЙТРАЛЬНОСТИ СЕТИ

В пользу нейтральности сети есть множество аргументов, так что же сейчас происходит в Европе?

В конце 2009г. европейские законодатели решили не вводить в действие законодательную защиту нейтральности сети в рамках "Телекоммуникационного пакета". Этот пакт обязывает провайдеров информировать конечных пользователей о менеджменте траффика, осуществляемом в сетях, и обеспечивать "честные, разумные и равные условия" для распространителей контента и приложений в их сетях¹⁵. Более того, в соответствии с этими законами, национальные регулирующие органы должны обеспечить пользователям возможность получать и распространять информацию и пользоваться услугами и приложениями по своему желанию. Тем не менее, как показал опыт, телекоммуникационный пакт оказался недостаточен для защиты нейтральности сети¹⁶.

Когда Нели Крос заняла должность Комиссара по цифровым технологиям в 2010г., она заявила,

что нейтральность сети будет центральной темой ее повестки дня, и назначила первые слушания по этой проблеме. Тем не менее, она ушла от темы нейтральности сети, проводя совещания вместо реальных действий по обеспечению нейтральности сети в Европе.

В 2011г., Европейская инспекция по защите персональных данных вынесла предупреждение о том, что нарушения нейтральности сети могут вызвать "серьезные последствия" для прав конечных пользователей на конфиденциальность и защиту персональных данных. EDPS заявила, что "определенные методы проверки, используемые провайдерами, действительно могут нарушать неприкосновенность частной жизни, если собирается информация о частной интернет-переписке, полученных и высланных письмах, посещенных сайтах и скачанных файлах"¹⁷.

В мае 2012г., после серии консультаций, Совет европейских регуляторов в области электронных коммуникаций (BEREC) опубликовал свои результаты анализа управления траффиком и других практик, ведущих к ограничению открытого интернета в Европе. Данные исследования

показали тенденцию к ограничению доступа к сервисам и приложениям со стороны провайдеров. 15 октября 2012г., официально завершилась последняя совещательная сессия по нейтральности сети. Это было шестым совещанием европейского уровня на тему нейтральность сети с тех пор, как Нели Крос заняла свою должность. Только через две недели Европейский Парламент потребовал изменения подхода "поживем-увидим" и призвал Комиссию разработать законопроект, обеспечивающий нейтральность сети¹⁸

Осенью 2012г. была проведена дополнительная неофициальная сессия, в период подготовки учреждений и стран-членов ЕС к участию во Всемирной конференции по международной электросвязи 2012 (WCIT12)¹⁹, организованной Международным союзом электросвязи (ITU). Целью конференции был пересмотр Международного регламента электросвязи (ITRs) -договора глобального уровня, имеющего обязательную силу для телефонных, телевизионных и радиосетей. Европейская ассоциация операторов телекоммуникационных сетей (ETNO) предложила включить управление интернетом в ITRs и вынесла на обсуждение поправку, которая позволила бы операторам предоставлять услуги доступа разного качества

а также создавать бизнес-модели типа "платит отправитель"²⁰. Данное предложение забыть о принципах нейтральности сети и "непрерывной цепи" не были приняты участниками конференции.

стр. 18/19: Обсуждение нейтральности сети в Европе за последние три года.

<http://www.tiki-toki.com/timeline/entry/108784/Net-neutrality-in-Europe/>

СОБЫТИЕ

НЕЛИ КРОС ЗАЯВЛЯЕТ:

22 декабря 2009

"Мы также должны обеспечить (...) надежность, открытость и нейтральность сетей"

2010

СОБЫТИЕ

НЕЛИ КРОС ЗАЯВЛЯЕТ:

14 января 2010

"(...) нейтральность сети абсолютно необходима. Для меня и для Комиссии крайне важно сохранить открытость и нейтральность сети."

НАРУШЕНИЕ

T-MOBILE БЛОКИРУЕТ SKYPE

3 апреля 2010

Deutsche Telekom, родительская компания T-Mobile, сообщила о планах блокировать Skype для iPhone в Германии.

НАРУШЕНИЕ

BT БЛОКИРУЕТ BBC IPLAYER

1 июня 2010

BT Broadband срезает скорость доступа пользователей к таким видеосервисам, как BBC iPlayer и YouTube в часы пик.

СОБЫТИЕ

НЕЛИ КРОС ЗАЯВЛЯЕТ:

11 ноября 2010

"При соблюдении духа нейтральности сети любой контент и приложения должны иметь равный статус." - "Любой легальный контент или приложение, не вызывающее заторов или другого вреда пользователям или сети, должно быть полностью доступным"

КОНСУЛЬТАЦИЯ

**ЗАПУЩЕНА ПЕРВАЯ КОНСУЛЬТАЦИЯ
ЕВРОКОМИССИИ 30 июня 2010**

2011

СОБЫТИЕ

EDPS ПРИНИМАЕТ ТОЧКУ ЗРЕНИЯ

7 октября 2011

EDPS дало несколько рекомендаций, включающих: создание законных практик проверки, необходимых для обеспечения бесперебойной передачи трафика или в целях безопасности; определение случаев, когда мониторинг требует согласия пользователей (фильтрация, нацеленная на ограничение доступа к услуге, например р2р); и, в таких случаях, необходимость инструкций по применению мер по защите информации (предотвращение злоупотреблений и т.д.).

НАРУШЕНИЕ

KPN ОБЪЯВЛЯЕТ ОБ ИСПОЛЬЗОВАНИИ DPI

22 апреля 2011

Голландский провайдер KPN заявляет о намерении взимать отдельную плату за использование voice-over-IP (VoIP) сервисов (Skype), мессенджеров и потокового видео.

НАРУШЕНИЕ

**ФРАНЦУЗСКИЙ ПРОВАЙДЕР
ОГРАНИЧИВАЕТ YOUTUBE**

3 мая 2011

КОНСУЛЬТАЦИЯ

10Е СОВЕЩАНИЕ BEREC

15 октября 2011

BEREC начинает совещание по указаниям для нейтральности сети и прозрачности.

ПАРЛАМЕНТ ЕС

1АЯ РЕЗОЛЮЦИЯ ПАРЛАМЕНТА ЕС

26 октября 2011

"Призывает Комиссию предотвратить блокирование, дискриминацию, помехи возможности любого пользователя получать, использовать, предлагать, отправлять любой контент, приложение или услугу по своему выбору вне зависимости от источника или цели."

СОБЫТИЕ

НЕЛИ КРОС ЗАЯВЛЯЕТ:

9 ноября 2011

она слышала "голословные заявления, что провайдеры ограничивают доступ к сервисам"

КОНСУЛЬТАЦИЯ

2, 3 & 4 СОВЕЩАНИЯ BEREC

23 февраля 2012

BEREC начинает совещания - три гайдлайна по Качеству Услуг (BoR 32), IP-взаимосвязи (BoR 33) и практике дифференциации (BoR 31)

2012

НАРУШЕНИЕ

**ЕВРОНАБЛЮДАТЕЛИ: TELCOS
ОГРАНИЧИВАЕТ ТРАФИК VOIP И P2P**

15 марта 2012

СОБЫТИЕ**ГОЛЛАНДИЯ ПРИНИМАЕТ ЗАКОНЫ**

8 мая 2012

Реагируя на анти-нейтральные планы KPN, подавляющее большинство членов голландского парламента проголосовали за законопроект о защите открытого интернета в Голландии

СОБЫТИЕ**НЕЛИ КРОС ЗАЯВЛЯЕТ:**

29 мая 2012

"потребители должны знать, получают они шампанское или игристое вино (...) Я не предлагаю принуждать всех операторов к предоставлению доступа ко всему интернету."

ПАРЛАМЕНТ ЕС**ЕВРОПАРЛАМЕНТ ВНОВЬ ТРЕБУЕТ НЕЙТРАЛЬНОСТИ СЕТИ - 15 декабря 2012**

Европарламент требует усилить защиту нейтральности сети - резолюция "Стратегия Цифровой Свободы во Внешней Политике ЕС" подчеркивает, что Европарламент "поддерживает принцип нейтральности сети, в частности, отсутствие дискриминации или каких-либо препятствий, включая ценовые, со стороны провайдеров в отношении способности любого человека использовать доступ к интернету для распространения, рассылки, получения любого контента, приложения или услуги, вне зависимости от источника или цели" и "призывает Комиссию и Совет поддерживать высокие стандарты цифровой свободы ЕС, в частности, кодифицируя принцип нейтральности сети".

ИССЛЕДОВАНИЕ**BEREC публикует находки**

29 мая 2012

"Как минимум 20% пользователей мобильного интернета в Европе подвергаются ограничениям доступа к услугам VoIP (...)"

КОНСУЛЬТАЦИЯ**НАЧАЛОСЬ ВТОРОЕ СОВЕЩАНИЕ КОМИССИИ**

23 июля 2012

Работа над новыми законами откладывается в связи с новым совещанием ЕС на тему нейтральности сети.

ПАРЛАМЕНТ ЕС**ЕВРОПАРЛАМЕНТ ТРЕБУЕТ ЗАКОНОДАТЕЛЬСТВА О НЕЙТРАЛЬНОСТИ СЕТИ - 26 октября 2012**

"81. Призывает Комиссию выдвинуть законопроект по защите нейтральности сети"

СОБЫТИЕ**СЛОВЕНИЯ ОДОБРЯЕТ ЗАКОНОПРОЕКТ**

20 декабря 2012

2013**НАРУШЕНИЕ****ORANGE ВЫНУЖДАЕТ GOOGLE ПЛАТИТЬ ЗА ТРАФИК 16 января 2013****НАРУШЕНИЕ****VODAFONE БЛОКИРУЕТ VIBER - 26 февраля 2013****ИССЛЕДОВАНИЕ****ПОДГРУППА КОМИССИИ ВЫДВИГАЕТ ЗАКОНОПРОЕКТ 23 января 2013**

"Каналы или механизмы, с помощью которых информация СМИ доставляется пользователю, должны быть нейтральны в работе с этой информацией. In the case of digital networks, Net Neutrality and the end-to-end principle should be enshrined within EU law."

СОБЫТИЕ**НЕЛИ КРОС ЗАЯВЛЯЕТ:**

20 марта 2013

"Мне надоело слышать о том, что люди не могут законно получить доступ к музыке и фильмам; что артисты не могут выйти на свои аудитории; что ученые не могут использовать современные исследовательские методы."

НАРУШЕНИЕ**ФРАНЦИЯ: SFR НАРУШАЕТ НЕЙТРАЛЬНОСТЬ СЕТИ - 30 марта 2013**

SFR нарушает нейтральность сети, изменяя HTML-контент на мобильном интернете.

СОБЫТИЕ**УТЕЧКА: ПРОЕКТ ПРАВИЛ ДЛЯ "ЕДИНОГО РЫНКА ТЕЛЕКОММУНИКАЦИЙ"**

11 июля 2013

Правила, в Статье 20, нацелены на запрет антиконкурентной блокировки и снижения скорости, НО в то же время разрешает соглашения по приоритезации трафика между провайдерами доступа и контента во имя нейтральности сети.

СОБЫТИЕ**НЕЛИ КРОС ЗАЯВЛЯЕТ:**

11 июля 2013

"Я буду гарантировать нейтральность сети. (...) Позволяя использование новых премиум-услуг, на которые полагается столько новых сервисов"

ПРИМЕР ИДЕРЛАНДОВ: КЕЙС-СТАДИ

Дополнение Bits of Freedom

КЕЙС-СТАДИ

В 2011г. бывший голландский телекоммуникационный монополист KPN заявил, что планирует взимать отдельную плату за трафик, используемый некоторыми сторонними приложениями, например, WhatsApp и Skype, чтобы создать преимущество для собственных услуг звонков и текстовых сообщений KPN. В мае 2011г. KPN сообщил, что использовал Deep Packet Inspection (DPI – см. стр. 9) для установления использования определенных приложений клиентами своего мобильного интернета²¹.

Годом позже, 8 мая 2012г., Нидерланды приняли важный законопроект по защите открытого и безопасного интернета, включая защиту положений нейтральности сети²². Нидерланды стали первой европейской страной (и второй страной в мире), законодательно закрепившей принципы нейтральности сети. Пример Нидерландов доказывает, что возможно создать законопроект по нейтральности сети, защищающий интересы пользователей и провайдеров услуг и доступа, а также свободу выбора и конфиденциальность.

Закон нацелен на укрепление свободы выбора и выражения в интернете и запрещает препятствование или нарушение работы сервисов и приложений в интернете. Только в определенных ограниченных случаях, когда это необходимо, допускается нарушить этот принцип. Исключения следует интерпретировать узко, базируясь на пропорциональности и критериях, установленных в контексте применения Европейской Конвенции прав человека.

Первое исключение нацелено на то, что срочному трафику (например, VoIP) может отдаваться приоритет в случае нехватки пропускной способности канала, и что в таких случаях другой трафик может быть задержан. Провайдеры должны избегать ограничений пропускной способности канала путем достаточных инвестиций. Тем не менее, в случае проблем с пропускной способностью, меры, указанные в данном исключении, должны обеспечить пользователям сохранение максимально полного доступа к информации и сервисам. Использование данных мер должно быть прекращено при первой возможности.

Второе исключение направлено на блокировку трафика, подрывающего безопасность или целостность сети либо устройства доступа конечного пользователя. Таким трафиком может быть трафик бот-сети, используемый для DDoS-атаки. Принятые меры должны быть пропорциональны, то есть влиять только на трафик, угрожающий целостности и безопасности, и не должны использоваться дольше, чем необходимо.

Третье исключение разработано для блокирования ненадлежащих комментариев и спама.

Наконец, последнее исключение описывает ситуацию, в которой провайдеры обязаны блокировать или замедлить трафик в соответствии с решением суда или законодательством.

Вдобавок к этому, провайдерам доступа запрещено менять стоимость услуг доступа к интернету в зависимости от услуг и приложений, используемых или предлагаемых пользователями.

“Экономический успех интернета - во многом следствие его архитектуры.”

- Лоуренс Лессиг, профессор права Гарвардского университета²³

ДЕСЯТЬ ПУНКТОВ ДЛЯ ЗАЩИТЫ НЕЙТРАЛЬНОСТИ СЕТИ

- 1** Интернет должен быть нейтральным и открытым.
- 2** Доступ без ограничений между всеми точками подключения к интернету должен сохраняться.
- 3** Все формы дискриминационного управления трафиком, например, блокирование или снижение скорости, должны быть запрещены, если в них нет объективной необходимости.
- 4** Управление трафиком может разрешаться только как отклонение от правила в узких рамках. Оно должно быть либо необходимым, целесообразным и требуемым по закону, либо решать временную проблему управления сетью, нерешаемую иначе.
- 5** Должна быть установлена правовая ясность по вопросу того, в каких обстоятельствах управление трафиком законно.
- 6** Провайдеры доступа должны указывать в контрактах минимальную гарантированную ширину канала, максимальное время ожидания и индикаторы качества подключения (чтобы пользователи знали, может ли подключение использоваться, например, для Skype). Провайдеры должны обеспечивать инструменты для подтверждения этих стандартов. Стандарты должны быть определены статистически и доступны публично.
- 7** Необходимо установить четкий набор обязанностей провайдеров в отношении нейтральности сети и максимальных усилий по обеспечению качественного широкополосного доступа с одной стороны, и для специализированных услуг, не использующих интернет, с другой.
- 8** По умолчанию, только информация разметки пакета должна использоваться для управления трафиком. Использование DPI должно быть проверено национальной инспекцией защиты персональных данных (DPAs) для оценки соответствия фундаментальным правам и принципам защиты данных ЕС.
- 9** Конечный пользователь должен иметь возможность сообщить о нарушениях вышеуказанных пунктов органу, определенному правительством. Данный орган должен иметь достаточно ресурсов для обеспечения соблюдения вышеуказанных условий защиты нейтральности сети.
- 10** Законодательство ЕС о нейтральности сети должно включать финансовые санкции, достаточные для предотвращения нарушения нейтральности сети.

ГЛОССАРИЙ

Лучшее из возможного. Интернет действует по принципу "лучшее из возможного" в отличие от гарантированного качества услуги телефонной цепи. Это происходит из-за того, что цифровой трафик дискретен и идет "вспышками", при этом попытка зарезервировать ресурсы для такого трафика будет крайне нерациональна. Вдобавок к этому интернет состоит из слишком большого числа сетей, что не позволяет создать прямые контрактные отношения, гарантирующие фиксированное качество услуги. См. также пиринг.

DOCSIS - международный стандарт телекоммуникаций, позволяющий добавить высокоскоростную передачу данных к существующей кабельной ТВ-сети.

Принцип непрерывной цепи - фундаментальная часть архитектуры интернета. Этот принцип постулирует, что интернет-коммуникация должна контролироваться в крайних точках, а не в самой цепи. "Передающая труба" не дискриминирует получателя, отправителя или содержимое, передаваемое по сети.

Фильтрация. Блокировка конкретных пакетов данных во время их перемещения по сетям, основанная на predetermined критериях. Она может быть использована для создания брандмауэра в целях безопасности, но также и для цензуры коммуникаций.

IP (интернет-протокол) - стандарт коммуникаций, позволяющий компьютерам передавать пакеты данных друг другу. Интернет-протокол - базовая технология коммуникации в интернете.

IP-адрес - численный адрес, назначаемый каждому подключенному к интернету устройству. Домашние или офисные роутеры могут показывать один IP-адрес для всех подключенных к нему, поэтому IP-адрес может идентифицировать не только одного человека, но и группу людей.

Провайдер доступа к интернету - компания, предлагающая доступ к интернету, работающая со стационарной/мобильной инфраструктурой, или обеспечивающая доступ к инфраструктуре.

ISP (интернет-провайдер) - общее обозначение компаний и организаций, обеспечивающих доступ к интернету и связанным с ним услугам. Есть много типов ISP, например, провайдер доступа, хостинга и т.д.

Пиринг. Множество сетей в интернете обмениваются трафиком между "равными" без оплаты. Это сложный ответ запутанному окружению. Отчетности, биллинг и даже составление контрактов означают затраты для любой организации. В простейшем варианте сеть провайдера доступа оплачивается из кармана абонентов. Такая сеть может впоследствии приобрести доступ к остальному интернету. Но если сеть может потом обмениваться трафиком между участниками, то это выигрышный для всех вариант. Нелогично будет платить другому участнику, если ему придется просто платить эти же деньги вам - и вдобавок в такой ситуации вам придется оплачивать издержки транзакций.

Peer to peer (P2P). Децентрализованная система, где пользователи ("peer") подключены друг к другу напрямую с помощью интернета.

Shaping намеренное замедление провайдером доступа к услугам, приложениям или контенту.

Протокол TCP - протокол, отвечающий за проверку успешной доставки данных, и "следящий" за пакетами данных. TCP помогает найти ошибки и вызвать ретрансмиссию, пока все пакеты не будут правильно и полностью приняты.

Архитектура TCP/IP. TCP и IP - самые распространенные и старейшие стандарты интернет-коммуникации. Поскольку основная масса переданных данных использует TCP и IP, название TCP/IP используется для обозначения всей группы протоколов, используемых в интернете. Эти протоколы определяют правила, которым должны следовать компьютеры для связи между собой и отправки данных правильному адресату.

Управление трафиком ISP всегда использовали прикладные механизмы контроля за потоками трафика для сохранения безопасности сети или предотвращения замедления доступа. Если ISP осуществляют управление трафика вдобавок к существующему контролю TCP/IP, это называется "управление трафиком".

VoIP (Voice over IP) Набор технологий и протоколов передачи данных, позволяющих передавать голос по интернету или отдельным сетям, использующим ИП.

Примечания

- 01 <http://www.commerce.senate.gov/pdf/cerf-020706.pdf>
- 02 EDRi booklet: How the Internet works http://www.edri.org/files/2012EDRiPapers/how_the_internet_works.pdf
- 03 http://europa.eu/rapid/press-release_SPEECH-08-473_en.htm
- 04 Open Rights Group: <http://www.openrightsgroup.org/blog/2012/peace-advocates-blocked-as-porn>
- 05 BBC: Virgin defends file-sharing campaign http://news.bbc.co.uk/newsbeat/hi/technology/newsid_7486000/7486836.stm and Virgin Media and Cview to rifle through your packets: <http://crave.cnet.co.uk/software/virgin-media-and-cview-to-rifle-through-your-packets-49304424/>
- 06 Open Net Initiative, West Censoring East <https://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011>
- 07 Wired, The Kremlin's New Internet Surveillance Plan, 1 November 2012: <http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/>
- 08 Thomas Grob, Deutsche Telekom, at the Netz-für-alle-Konferenz: <https://www.youtube.com/watch?v=HQBwiZ5hloo#t=20m28s>
- 09 BEREC report on traffic management, 2012: "When blocking/throttling is implemented in the network, it is typically done through deep packet inspection (DPI)" https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf
- 10 European Parliament resolution, 26/10/2012 <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2012-0341&language=EN>
- 11 PLUM study 2011 http://skypeblogs.files.wordpress.com/2011/10/plum_october2011_the_open_internet_-_a_platform_for_growth.pdf
- 12 Joint Statement of the EU Delegation to the 7th International Governance Forum (IGF) in Baku http://europa.eu/rapid/press-release_MEMO-12-852_en.htm
- 13 Glasnost data visualised in a Net Neutrality map <http://netneutralitymap.org/>
- 14 Respect my net: <http://respectmynet.eu/list/>
- 15 Directive 2002/19/19 (Access Directive): <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:EN:HTML>
- 16 See BEREC study May 2012 http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf
- 17 EDPS Opinion on Net Neutrality, traffic management and the protection of privacy https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-10-Net-neutrality_EN.pdf
- 18 EU Parliament resolution on completing the Digital Single Market, 26 October 2012: <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2012-0341&language=EN>
- 19 See WCIT resources: <http://wcitleaks.org/resources/>
- 20 ENDitorial: The ETNO's WCIT Proposals are not as bad as some say <http://www.edri.org/edriagram/number10.19/wcit-etno-proposals-not-so-bad>
- 21 Web wereld: KPN luistert abonnees af met Deep Packet Inspection <http://webwereld.nl/beveiliging/53691-kpn-luistert-abonnees-af-met-deep-packet-inspection>
- 22 The translated provisions can be found on the website of Bits of Freedom: <https://www.bof.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/>
- 23 <http://www.nytimes.com/roomfordebate/2010/8/9/who-gets-priority-on-the-web/a-deregulation-debacle-for-the-internet>



EDRI.ORG/PAPERS



With financial support
from the EU's
Fundamental Rights and
Citizenship Programme.

This document is distributed under a Creative Commons 3.0 Licence
<http://creativecommons.org/licenses/by-nc-sa/3.0/>