

"Территория свободы"

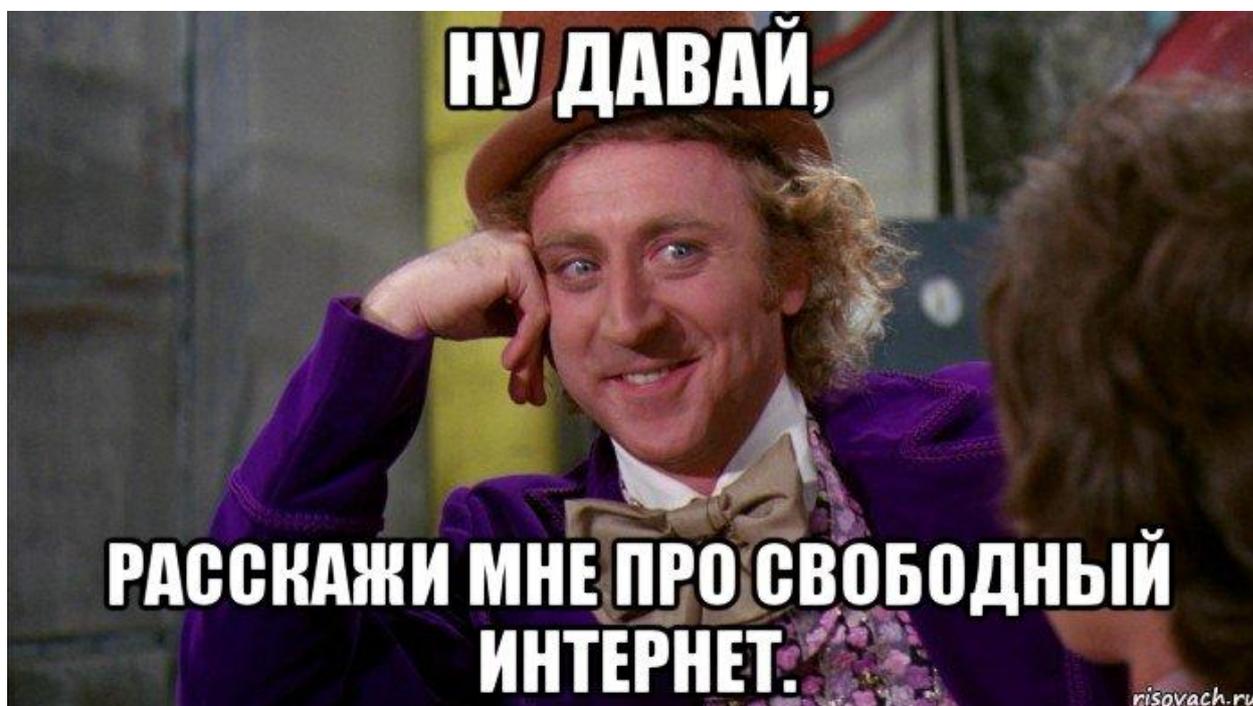
Оглавление:

"Территория свободы"	1
Россиян заставят дорого заплатить за цензуру Кремля	7
Что «Большой брат» знает про каждого пользователя	11

"Территория свободы"

 [colonelcassad](https://colonelcassad.livejournal.com/4774721.html)

13 февраля, 8:37 Источник: <https://colonelcassad.livejournal.com/4774721.html>



Граждане волнуются, что с принятием нового закона "об обособлении рунета", продолжают закручивать гайки в "свободном интернете". Мол, была у нас "территория свободы", а сейчас вот приняли закон и настанет "царство несвободы". На деле, конечно сразу ничего отключать не начнут, но обеспечат условия, когда можно по отмашке опционально закрутить - начиная от ограничения легального трафика извне и заканчивая блокированием тех или иных зарубежных сервисов, которые вступили в конфликт с законодательством, властью или даже лоббистскими группами влияния заинтересованных в продвижении отечественных аналогов цифровой продукции (помянем молчанием мессенджеры, которые должны были прийти на смену Телеграму).

На деле, то что происходит, это часть давней тенденции плавного, но планового закручивая гаек в интернете, где ориентиром может служить китайский вариант государственного контроля в российской lite-версии. Россия в этих вопросах от

Китай традиционно на пару-тройку лет отстает, но идет в том же направлении. Государство к настоящему моменту полностью осознает как угрозы для себя и общества, которые исходят из неконтролируемой сети, так и возможности, которые дает прямой или скрытый контроль над сетью. И это не является сугубо российским поветрием. Стремление установить контроль над своим сегментом интернета достаточно типично для государств стремящихся к субъектности во внутренней и внешней политике и особенно у государств конфликтующих с США, ибо контроль над своей информационной системой, часть процесса высвобождения от *undirect* контроля, который заложен в американскую версию "свободного интернета".

Интернет как таковой вырос из американских военных сетей и в эпоху безоговорочной американской гегемонии, он по сути являлся частью проекта "Глобализации по-американски", где территория информационной свободы подразумевала "свободу" под американским контролем. Там где это было необходимо, "территория свободы" использовалась для развертывания информационного оружия направленного на поддержку интервенций и агрессий, вроде пресловутых "Фейсбук-революций", где социальные сети заменили прежние элементы организации подрывной деятельности или масштабных манипулятивных пропагандистских кампаний, а информационные каналы транслировали один нарратив о победившей американской мечте, которая привела к концу истории.

Когда проект глобализации рухнул и мир вступил в стадию трансформации, фрагментируется не только миропорядок, глобальная экономика и даже "единая Европа". Фрагментируется и глобальная сеть, бывшая детищем глобализации. В эпоху нарастающего экономического протекционизма, правого популизма, блокового мышления и логики Холодной войны, "глобальная территория свободы" рождает внутри себя все новые и новые барьеры в отдельных своих сегментах, а ослабление американской гегемонии выявляет все новые и новые скрытые системы контроля над "свободным интернетом". Все это разумеется происходит не само собой, а рождается в результате идущей борьбы стран и блоков за влияние в быстро меняющемся мире, где свою "базу" пытаются защитить, а позиции противника атаковать. Обвинения в "зажиме свободы", когда из Китая выгоняют очередную корпорацию, в Турции закрывают Твиттер, а в России "блокируют" Телеграм, направлены прежде всего на восстановление полного и безоговорочного доступа для гегемона и его инструментов. С другой стороны, страны-фронтеры усиливая фрагментацию интернета и подрывая базовые механизмы американского непрямого контроля (используя как случайные, так и создаваемые поводы - вроде дела Сноудена, дела Кембридж Аналитики или разоблачений Ассанжа), стремятся обосновать для своего населения и других стран необходимость фрагментации и обособления, так как текущая система несправедлива и должна быть изменена, поскольку в нынешнем формате в ней доминируют США, что представляет угрозу в силу банального неравенства возможностей. Отсюда и проистекает война нарративов - "вы ограничиваете свободу" vs "вы контролируете свободу". Так как предпосылок к окончанию текущей Холодной войны нет, то и эта война нарративов будет продолжаться - от серьезных аналитических материалов и официозных заявлений до матерных комментариев в соц.сетях и несмешных мемов.

В сфере политики интернет все больше представляет из себя площадку для пропаганды дополняющую или вовсе заменяющую устаревающие инструменты манипуляции и контроля над массовым сознанием вроде ТВ, радио или печатных газет. Многие уже начали подмечать, что Ютуб становится все менее отличим от ТВ, что особенно ярко проявилось не так давно, когда люди, которые не смотрят телевизор, "потому что там Киселев", слушали Киселева в гостях у модного либерального блогера. Киселевская пропаганда в трендах Ютуба. Это было весьма иронично.

Перманентные информационные войны, с виртуальными армиями диванных пехотинцев и спецоперациями контролируемых хакеров по взлому правительственных баз данных уже давно сопровождают любую мало-мальски политизированную тему, проявляясь порой даже в темах про котиков и форумах "Яжмать", где никогда не знаешь, не появится ли в теме "Вам нравятся серые или черные котики" случайный человек или бот, который грозно напишет "ПТН-ПНХ", "Порошенко спившийся алкаш", "Гроссмейстер Путин всех переиграл", "Навальный-2018", "Прости нас Государь.." И понеслась...

Социальные сети, которые превратились в дополнительные картотеки спецслужб с полным доступом к учетным записям и закрытой переписке, которая попадает как "товарищу майору" или "мистеру из ЦРУ", а также коммерческим структурам, где ваша личная информация является продуктом, которым торгуете не вы, а левый дядя из "С.А", который, если его за этим поймают, скажет, я не хотел, так получилось, я больше так не буду. А потом выяснится, что этим занималась не только "С.А", да и дядя был не один. Да и чего далеко ходить - телефоны и почтовые адреса, кредитные карточки и прочая приватная информация продаются в промышленных масштабах, как путем добычи этой информации хакерами, так путем утечек из гос.органов.

Прямая и явная корпоративная цензура, зачастую по эффективности и наглости превосходит государственную. Сейчас ничего не стоит по щелчку пальцев заблокировать канал с миллионной аудиторией или удалить десятки тысяч аккаунтов, объявив их причастным к чему угодно, что не нравится хозяевам корпоративных медиа.

Критерий "поддерживал Россию", "поддерживал Иран", "выступал против Хиллари Клинтон", "поддерживал Трампа" - вполне могут быть основанием для прямой карательной цензуры, причем актер цензуры будет скрыт за абстрактной тех.поддержкой сервиса и вы зачастую так и не узнаете, корпорация ли вас забанила или это спецслужбы или правительство "попросили". Есть и более тонкие способы вроде "понижающих коэффициентов", "искусственного ранжирования" и "минимизации поисковой выдачи". Цензоры до-цифровой эпохи могли лишь мечтать о подобных возможностях, когда порой даже не обязательно запрещать, а можно утопить неудобную информацию в безвестности, свалке мусорных новостей или наведенном информационном шуме.

Википедия из склада объективных знаний в сфере политики и истории давно превратилась в площадку борьбы за выгодные трактовки и интерпретации, зачастую просто недостоверные или тенденциозные, но эти трактовки оплачиваются корпорациями или правительствами. Война за правки, это маленькая часть глобальной борьбой за нарратив, где факты и события это ресурс и

инструмент в борьбе за умы, так как значительная часть граждан верит маркетинговым заявлениям, что в Википедии пишут только правды. Грех не воспользоваться, таким количеством простаков, открытых для манипуляции.

Перепродавцы цифрового контента доводят гонку за пиратами до абсурда, когда основой цензуры и ограничения доступа к информации становятся даже не абстрактные государственные интересы, а жажда наживы, чтобы очередной случайный персонаж мог за счет этих ограничений купить замок в Шотландии. Защита прав правообладателей оборачивается тотальным ущемлением прав пользователей мечтавших о мире "свободного цифрового контента". Даже в этой мелочи наглядно проявляется фрагментация текущего миропорядка.

Красивая идея о свободном обмене информацией между свободными индивидами глобального человечества подобного "Титанику" натолкнулась на айсберг реальной политики и несовершенства человеческих сообществ в эпоху капитализма, где интернет это поле боя и инструмент манипуляции сознанием, и именно так его видят правительства и спецслужбы. Отсюда и логичные последствия такого видения для "территории свободы". ЦРУ и АНБ собирают данные через Facebook, ФСБ собирает через ВКонтакте. Apple рассказывает, что АНБ не читает зашифрованную переписку Айфонов, а Дуров рассказывает, что ФСБ не читает закрытые чаты Телеграм. Как представляется - вероятность того и другого стремится к нулю, но в современном мире нарастающего правительственного контроля, информационной слежки и навязанных нарративов, декларируемая приватность может выглядеть удобным маркетинговым ходом, предлагая ищущим приватности своеобразное плацебо, которое призвано поддерживать иллюзию что контроль еще технически ограничен. Хотя на деле, он скорее ограничен возможностями живых контролеров системы, которые просеивают стекающуюся информацию как с помощью автоматизированных систем контроля и наблюдения, что конечно не избавляет от необходимости живого анализа из поставляемых системой выборок. Навязываемая универсализация аккаунтов, когда один аккаунт для всех соц.сетей и сервисов, удобна не только пользователям, но и контролерам, так как один аккаунт на одного человека контролировать проще (с точки зрения затраты человека и машино-часов), чем кучу отдельных аккаунтов с отдельными историями переписки и контактами.

Конечно, этот контроль всегда объяснят высшим государственным благом, заботой о демократии, защитой от терроризма, борьбой с экстремизмом и т.д. и т.п. Где-то эта аргументация может быть убедительной. где-то нет, но опять же, это уже давно не вопрос убедительности аргументации, чтобы убедить Джона из Детройта или Свету из Иваново, так как вопрос по факту уже решен и мы живем в реальности, где цифровая приватность весьма иллюзорна.

Когда поле боя размечено, цифровые редуты возведены, а средства информационного и кибернападения подготовлены, можно наблюдать трансформацию "территорию свободы" в территорию системной войны, где важны как дела вроде свергнутых правительств, политически и личностно уничтоженных политиков или трансформации курса отдельных государств, но и слова, которые направлены на навязывание массам своего нарратива, будь-то "Россия хуже Эболы или ИГИЛ" или "Все зло в мире от США". "Это мы победили ИГИЛ!". "Нет, это мы победили ИГИЛ".

Британские спецслужбы обвиняют российские в том, что они через соц.сети организовали выход Британии из Евросоюза, а в США на полном серьезе обвиняют ГРУ в том, что несколько тысяч аккаунтов в Твиттере и Фейсбуке помогли выбрать нужного президента США. При этом британские спецслужбы в рамках операции Integrity Initiative не брезгают делать ровно тоже самое, в чем обвиняют российские спецслужбы оказывая скрытое влияние на политику других государств для ее коррекции в своих интересах в тайне от народов этих стран, а США вовсю вмешиваются через цифровые каналы в дела других государств и влияя на их выборы, хотя они совершенно не согласны, когда такой подход может быть применен к ним. Кто следит за этими делами, может убедиться, что вопрос охвата оказывается зачастую более важен вопроса правдоподобности и это уже давно не вопрос содержательной дискуссии между участниками идущей войны.

Разумеется, в подобном "прекрасном новом мире", идея о свободной глобальной сети выглядит утопией и в случае с интернетом, он уже давно определяется не степенью свободы, а скорее степенью несвободы, а также параметрами прямых и непрямых инструментов контроля и подавления, которые применяются в отдельных его сегментах.

В случае с последними инициативами правительства, новый закон конечно направлен на повышение контроля и управляемости российским сегментом интернета, где ограничиваться возможности системы будут не мифическими протестами "свободных индивидов в блогах и на форумах", а качеством технической реализации и затратами на инсталляцию подобной системы. Всегда есть вероятность, что желание закрутить гайки будет сопровождаться ничемным исполнением, как это уже было с попыткой систематизировать всех блогеров через пресловутый "реестр блогеров" (помните еще такой?), запретить Телеграм (когда гос.компании сами рекламируют запрещенный другими гос.органами мессенджер), борьбой с анонимайзерами (когда федеральный канал сам рекламирует способы обхода блокировок) и бесконечная борьба с торрентами в интересах хапуг из РАО (которая к ликвидации пиратских сайтов и пиратского контенте конечно не привела, зато привела к личностному обогащению).

Более вероятной выглядит ситуация, когда развернув "ограничительную систему", РКН и другие гос.структуры могут более деятельно давить на американские компании вроде Facebook, Twitter или Google, добиваясь от них выполнения тех или иных требований, которые они ранее отказывались выполнять или профанировали. Теперь же им будут угрожать реальным "отключением" как это делает Китай, причем у лоббистов системы будет крайне велик соблазн ее задействовать на практике, хотя бы разок, чтобы доказать государству ее полезность и эффективность, чтобы все не выглядело как очередной попил бюджетных средств под красивые слова про "новые технологии безопасности". Разумеется, проверка возможности полного отключения от интернета возможна лишь в маловероятных сценариях полноценной войны с Западом, но с учетом текущей динамики развития отношений с США, сценарий обособления уже нельзя считать совсем невероятным.

В остальном же - новый закон ведет к тому, что не прямое гос.регулирование в рунете возрастет, хотя для обычного пользователя вряд ли что-то поменяется, так

как у РКН и ФСБ были и до этого все возможности, чтобы надавить на провайдера, ознакомиться с перепиской, заблокировать сайт или страницу в соц.сетях, а то и довести дело до суда (где лишь недавно смягчили наказание за репосты). Напрямую "новшество" коснется обычного пользователя в том случае, когда он обнаружит, что в результате каких-то кулуарных решений или конфликтов, его любимая соц.сеть перестала работать без VPN, а любимый поисковик перестал выдавать ссылки на очередное зеркало любимого пиратского кинотеатра. Но пока это лишь возможные отложенные последствия.

Новый закон скорее направлен против "крупной рыбы" - информационных конгломератов, социальных сетей и IT компаний, которым придется учитывать в своих действиях наличие "большой красной кнопки ВЫКЛ", с поправкой на то, что в силу качества исполнения, она может работать не столь эффективно, как мечталось заказчику.

Возрастает именно общий контроль, который свидетельствует о готовности государства и далее, при необходимости, идти по пути фрагментации глобальной информационной системы и усиления гос.регулирования российской части уже давно не свободной "территории свободы".

Несомненно, что не за горами тот день, когда в интернет начнут пускать по паспорту. В Китае обязательную идентификацию ввели в 2017-м. В 2020-2021 ждем в России.

<https://youtu.be/1k-JkIDZ9LE>

Метки: [Китай](#), [Россия](#), [США](#), [интернет](#), [информационная война](#), [капитализм](#), [корпоратократия](#), [манипуляция сознанием](#), [социальные сети](#), [цензура](#)

Россиян заставят дорого заплатить за цензуру Кремля Наживутся на введении «суверенного рунета» вполне конкретные олигархи

Источник: <https://svpressa.ru/society/article/224284/>



[Антон Чаблин](#)



Фото: YAY/TASS

Материал комментируют:



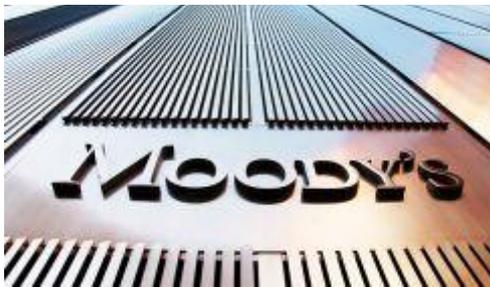
[Саркис Дарбинян](#)

Российский сегмент интернета готовится окончательно «отрезать» от глобальной паутины, несмотря на тихие протесты Счетной палаты и даже самого Минкомсвязи. Происходит это на фоне колоссального роста интернет-цензуры. Правда, даже у самых одиозных цензурных инициатив есть не только политическая... но и сугубо коррупционная первопричина.

«ВКонтакте»: служит или прислуживает?!

Правозащитная ассоциация «Агора» пятый год подряд ведет мониторинг интернет-цензуры в России. По итогам 2018 года число подобных фактов, по подсчетам экспертов, выросло в разы — со 116 до 663 тысяч! Абсолютное большинство таких случаев связаны с ограничением доступа к интернет-сайтам и сервисам, а также запретом на распространение информации (по самым различным основаниям). Причем все чаще власти используют практику «тройного давления». К примеру, пользователь может быть привлечен к уголовной ответственности за публикацию в блоге, опубликованный им текст — признан запрещенным к распространению, а сам сайт — включен в «черный список» Роскомнадзора.

ЧИТАЙТЕ ТАКЖЕ



[Хозяева довольны: Запад похвалил Россию за пенсионную реформу](#) Агентство Moody's повысило рейтинг РФ с мусорного за «позитивную госполитику»

За прошлый год, подсчитали в «Агоре», в России были вынесены 45 приговоров по фактам распространения информации в Интернете (годом ранее — 48). Самый массовый инструмент уголовно-правового давления — это, конечно, обвинения в экстремизме. Но помимо этого еще 28 человек осуждены за клевету.

Одно из самых известных — дело в отношении 25-летней жительницы Барнаула **Марии Мотузной**, которая несколько лет назад сохранила в альбом на своей страничке «ВКонтакте» картинки, позднее признанные оскорбляющими чувства верующих.

Кстати, свою страничку Мотузная удалила еще два года назад, но администрация «ВКонтакте» услужливо предоставила данные кэша правоохранителям.

В отношении Мотузной возбудили уголовное дело по ст. 282 УК РФ («Возбуждение ненависти или вражды»), а сама она эмигрировала сначала на Украину, а затем в Литву.

Настя Рыбка как «лицо» цензуры

Дело Марии Мотузной прогремело на всю страну. Выяснилось, что сотрудники ФСБ и Центров по противодействию экстремизму (ЦПЭ) по всей стране пачками «штампуют» подобные уголовные дела. В итоге даже сам президент **Владимир Путин** во время «Прямой линии» заявил: борясь с экстремизмом, «не нужно доводить всё до маразма и до абсурда».

После этого пресловутая 282-я статья Уголовного кодекса (благодаря наличию которой и возбуждались уголовные «дела за лайки и репосты») была декриминализована. Впрочем, это стало единственным административным послаблением — на фоне непрекращающегося наступления на свободу слова в интернете.

«Агора» в своем докладе отмечает, что на фоне отмены 282-й статьи Уголовного кодекса резко выросло число дел по «смежным» ст. 205.2 УК РФ («Публичные призывы к осуществлению террористической деятельности») и ст. 280 УК РФ («Публичные призывы к осуществлению экстремистской деятельности»).

Расширяется практика блокировки сайтов, где размещена «неудобная» информация. Примеры — блокировка расследования **Алексея Навального** (а также написанных на его основе журналистских статей)

о времяпровождении олигарха **Олега Дерипаски** и вице-премьера **Сергея Приходько** на яхте в присутствии белорусской дамочки сомнительных занятий **Насты Рыбки**.

Также по требованию банка ВБТ были заблокированы материалы, в которых в негативном свете фигурировал председатель правления **Андрей Костин**.

Но это все «цветочки» на фоне новых инициатив законодателей. Сенатор-единоросс **Андрей Клишас** в конце 2018 года разродился целой серией подобных законопроектов — о наказании за распространение fake news и оскорбление органов власти.

Ну и, безусловно, самый скандальный — о тотальном отключении рунета от глобальной паутины. Он предусматривает введение жесткого централизованного контроля надо всем трафиком, который будет осуществлять всеильный Роскомнадзор.

Коррупциогенная подоплека

«Свободная пресса» обсудила драконовские законодательные инициативы российских депутатов с ведущим юристом общественного проекта «Роскомсвобода», руководителем Центра цифровых прав Саркисом Дарбиняном.

«СП»: — Саркис Симонович, на днях автор законопроекта о создании «суверенного Интернета» Андрей Клишас заявил, что на его реализацию выделяю 20 миллиардов рублей. Откуда такие суммы?! Да и вообще, неужто больше не на что бюджетные средства потратить?!

— В финансово-экономическом обосновании к законопроекту авторы забыли определить источники и порядок исполнения нового вида расходных обязательств. Сами авторы позже обозначили цифру в 20 млрд. рублей, но эксперты в один голос твердят, что стоимость его реализации обойдется на самом деле в сотни миллиардов рублей!

Это, очевидно, скажется на удорожании услуг связи и конечно никого ни от чего не защитит, потому что предлагаемые в проекте технические средства противодействия угрозам абсолютно не предназначены «для обеспечения устойчивости и безопасности интернета».

Стоит также отметить высокую коррупциогенность законопроекта! Уже называют некоторых бенефициаров, которые могут существенно заработать на нем. И это будет покруче СОРМов и «пакета Яровой», которое уже обязывает операторов за собственный счет покупать дорогостоящие программно-аппаратные комплексы, сертифицированные ФСБ и российскими властями.

«СП»: — А на что конкретно должны пойти деньги?

— Авторы законопроекта предполагают проведение целого ряда мероприятий — надо сказать, мало обоснованных. Во-первых, это контроль над трансграничными точками обмена Интернет-трафиком, обязательное оснащение операторов связи дорогостоящей технологией Deep packet inspection (DPI) для более «внимательного» определения вида трафика, создание альтернативных корневых DNS-серверов.

Во-вторых, это плановые учения органов власти, операторов связи и владельцев технологических сетей по выявлению угроз и отработке мер по восстановлению работоспособности российского сегмента сети Интернет.

ЧИТАЙТЕ ТАКЖЕ



[По росту инфляции Россия обгонит Украину, дойдя до двузначных цифр](#)
[Повышение НДС и нацпроекты для олигархов совсем обесценят наши деньги в 2019-м](#)

Ну и, наконец, существенное расширение полномочий Роскомнадзора.

«СП»: — Клишас с соавторами уверен, что таким образом удастся «обезопасить» Россию от внешних кибернетических угроз, в первую очередь, американских и европейских хакерских атак.

— В логике проекта перевернуто все с ног на голову. И хоть в пояснительной записке говорится, что необходимость его принятия продиктована возможностью отключения России от интернета в условиях изоляции, сами механизмы, заложенные в документ все же говорят немного о другом - о том, как изолировать Рунет от внешней Сети изнутри, якобы в целях госбезопасности.

Отрицая всю логику и факты того, что в мировой практике не известно случаев отключения кого-либо от глобального интернета и корневых серверов, кабинет министров в целом одобрил предлагаемую концепцию.

«СП»: — Насколько, на ваш взгляд, велика вероятность принятия закона, учитывая, что против него выступили даже Минкосвязи и Счетная палата?

— Вероятность достаточно велика. В таком случае, блокировки веб-сайтов и сервисов вроде Telegram в России станут чуть более эффективной, а сам отцензурированный и «поломанный» «российскими властями интернет — сильно дороже.

Пока еще есть немного времени, что отбить очередную сомнительную инициативу, которая способна существенно ограничить цифровые права российских пользователей интернета и задушить телекоммуникационные компании. Они и без того уже работают не в самых простых условиях, но все еще стараются развивать свои сервисы в нашей стране.

Что «Большой брат» знает про каждого пользователя

15:56 20.11.2018 Источник: <http://www.km.ru/science-tech/2018/11/20/833999-что-болшой-brat-znaet-pro-kazhdogo-polzovatelya>

Многие подозревают, что в современном мире о человеке собирается множество самой разной информации. И это действительно так



Изображение с сайта pixabay.com

Сбор информации происходит при самых разных устройствах, например, смартфоны, компьютеры и ноутбуки, планшетные компьютеры, браузеры, новомодные гаджеты.

Разумеется данная информация может оказаться доступна не только спецслужбам, но злоумышленникам.

По мнению большинства пользователей, данные, которые известны о каждом, выглядит так:

Microsoft	Amazon	Twitter	Apple	Facebook	Google	Icon	Label
Microsoft	Amazon	X	Apple	Facebook	Google	Person with umbrella	Name
Microsoft	X	X	X	Facebook	Google	Person	Gender
Microsoft	X	X	X	Facebook	Google	Calendar	Birthday
Microsoft	Amazon	Twitter	Apple	Facebook	Google	Phone	Phone Number
Microsoft	Amazon	Twitter	Apple	Facebook	Google	Email	Email Address
Microsoft	Amazon	Twitter	Apple	Facebook	Google	Location pin	Location
X	X	Only you time zone	X	Facebook	X	Relationship	Relationship Status

Изображение с сайта securitybaron.com

И это мало кому кажется опасным, но вот как все обстоит на самом деле.

THE DATA BIG TECH COMPANIES HAVE ON YOU

THE TYPES OF DATA MAJOR TECH COMPANIES ADMIT TO COLLECTING IN THEIR PRIVACY POLICIES

	Google	Facebook	Apple	Twitter	Amazon	Microsoft
Name	✓	✓	✓	✗	✓	✓
Gender	✓	✓	✗	✗	✗	✓
Birthday	✓	✓	✗	✗	✗	✓
Phone Number	✓	✓	✓	✓	✓	✓
Email Address	✓	✓	✓	✓	✓	✓
Location	✓	✓	✓	✓	✓	✓
Relationship Status	✗	✓	✗	Only your time zone	✗	✗
Work	✗	✓	✗	✗	✗	✗
Income Level	✗	✓	✗	✗	✗	✗
Education	✗	✓	✗	✗	✗	✗
Race/Ethnicity	✗	✓	✗	✗	✗	✗
Religious Views	✗	✓	✗	✗	✗	✗
Physical Address	✗	✓	✓	✗	✗	✓
Facial Recognition Data	✗	✓	✗	✗	✗	✓
Political Views	✗	✓	✗	✗	✗	✗
Credit Cards	✗	If you've made purchases on Facebook	✓	✓	✓	✓
Government IDs (Such as Social Security and Driver's License Numbers)	✗	✗	Only the IP address used to open the Apple ID account	✗	✓	✗
IP Addresses	✓	✓	✓	✓	✓	✓
Your Emails	✗	Including followers, following, friend requests, pending friend requests, removed friends, friends, the friends tagged as family members, and groups	✗	✗	✗	✓
Your Contacts	✗	✗	✗	After you've given Twitter permission	✗	✓
Your Phone Calls	✗	✗	Only the meta data on when the phone calls were made	Only the meta data on when the text messages (in Messages) were made	✗	✓
Your Chat Conversations/ Messages	✗	✗	✗	✗	✓	✓
Calendar Events	✗	Including both what you've joined AND what you've been invited to	✗	✗	✗	✓
Search History	✓	✓	✗	✗	✓	✓
Videos Watched	✗	✗	✗	Including live broadcasts	✓	✓
Websites Visited	✓	✗	✗	✗	✓	✓
Browser Information	✓	✓	✗	✗	✓	✓
Video Uploads	✗	✗	✗	✗	Including a personal photograph in your profile	✓
Photo Uploads	✓	Including photo metadata	✗	✗	✓	✓
Status Updates/Posts	✗	✓	✗	✗	Including discussion boards, community features, and reviews	✗
Likes	✗	✓	✗	✗	✗	✓
Your Documents	✗	✗	Only Apple device purchases and maintenance	✗	Including documents you store in the cloud	✓
Your Purchase History	✗	✗	✓	✗	✓	✓
Your Games	✗	✗	Only meta information on gaming sessions with Game Center	✗	✗	✓
Your Books	✗	✗	✗	✗	✗	✓
Your Music	✗	Including iTunes downloads as well as iTunes Match uploads and downloads	✗	✗	✗	✓
Your Fitness/Health Data	✗	✗	✗	✗	HealthVault data such as heart rate and daily steps taken	✓
Ads You Click	✓	✓	✗	✗	✓	✓
What you've hidden from newsfeed	✗	✓	✗	✗	✗	✗
The Devices You Use	✓	✓	✓	✓	✓	✓
Information About the Things Near Your Device (WiFi, Bluetooth, etc.)	✗	✗	Only Apple device purchases and maintenance	✗	✗	✓
Voice Data	✗	✗	✗	✗	✓	✓
Gaming Interactive Data	✗	✗	✗	✗	✗	Including skeletal tracking data and buttons pressed while using Xbox Live

Изображение с сайта securitybaron.com

Как можно видеть, из полученных данных, а скорее всего их даже больше, чем показано на картинке, можно составить подробный психологический портрет пользователя, оценить интеллектуальный и финансовый уровень, выявить круг общения, связи, предпочтения, установить повседневный маршрут и текущее местонахождение. Также можно узнать его внешность, голос, физические кондиции и многое другое. Некоторую часть собираемых данных можно удалить и даже запретить собирать, но именно часть. В остальном же «Большой брат» продолжает следить за поведением всех пользователей.

Темы: [Антивирусы и обеспечение безопасности компьютера](#), [Компьютерная безопасность](#), [Хакеры и проблема безопасности компьютерных сетей](#)