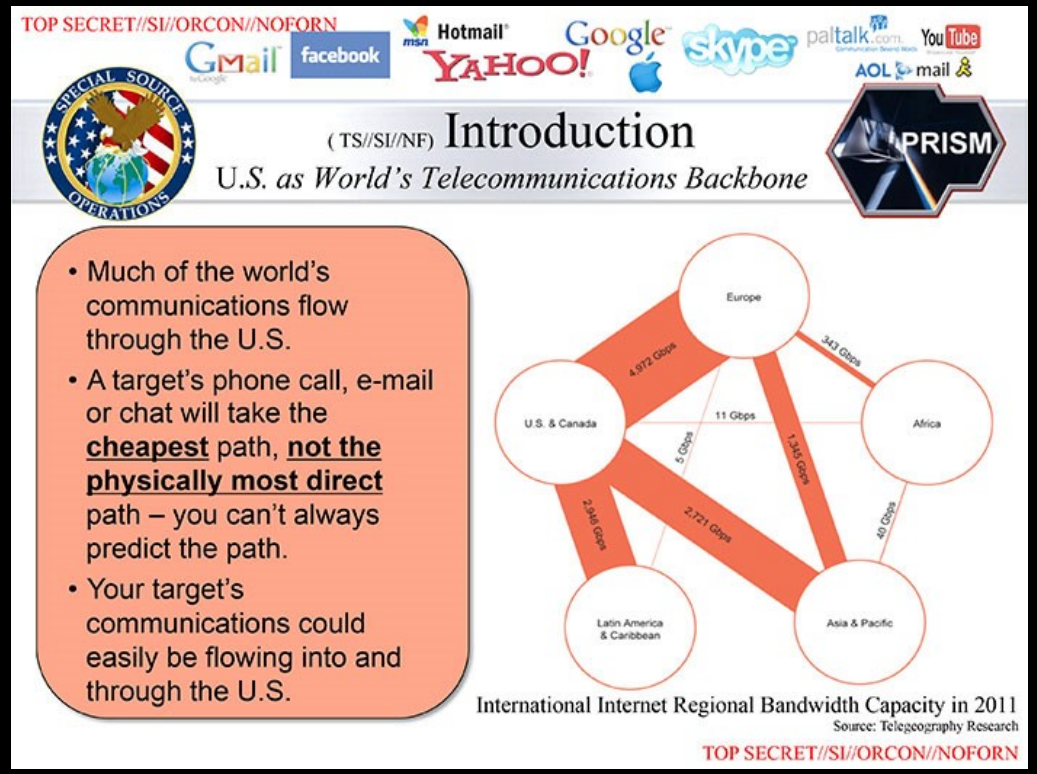
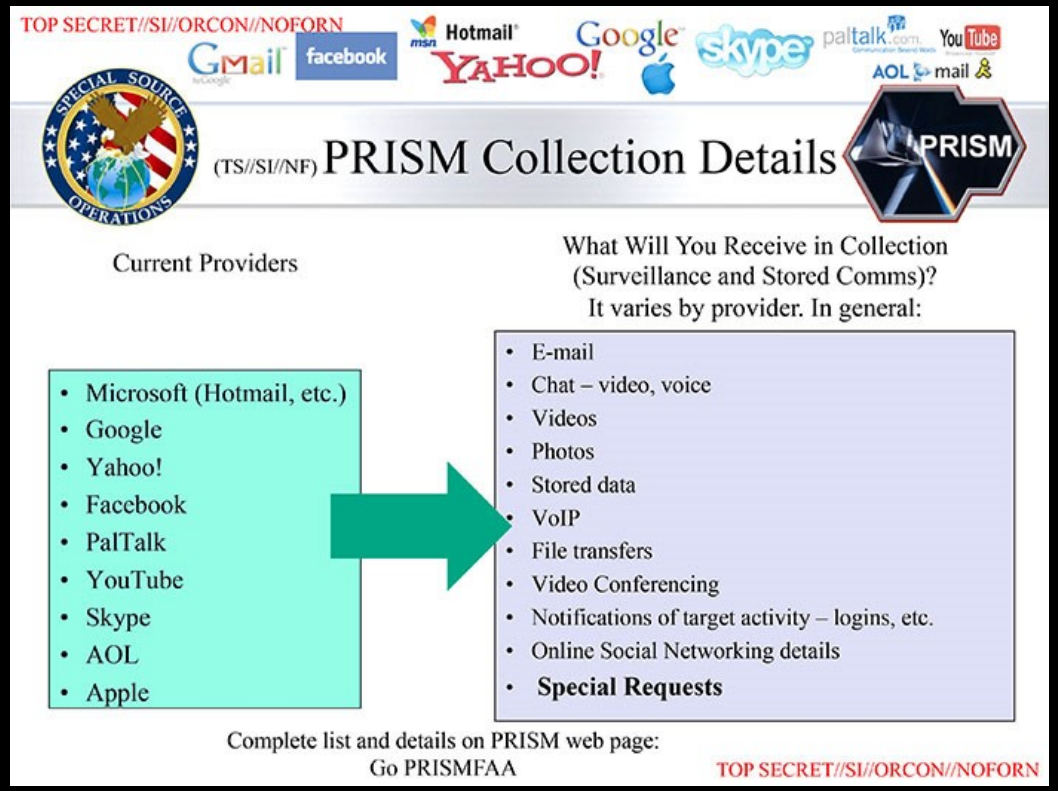
2024

Сноуден

- 2013 год, разглашение данных о массовой слежке, программа PRISM,
- Электронная почта, видеопотоки, HTTP, звонки, метаданные
- Слежка за порядка миллиардом человек, включая граждан США
- Five Eyes – международная программа слежки, через анализ интернет потоков (Австралия, Канада, Новая Зеландия, Великобритания, США)
  - Nine Eyes – более слабы соглашения подписаны и с Францией, Нидерландами, Норвегией и Данией
  - Fourteen Eyes – расширение договорённостей на Бельгию, Италию, Испанию Швецию и Германию

Prism





https://commons.wikimedia.org/wiki/Category:PRISM_(surveillance_program)

https://nsa.gov1.info/dni/prism.html

Принципы массовой слежки

- Смещение акцента от индивидуальной слежки к массовой
  - Нет необходимости снаряжать слежку за отдельными лицами, кода проще следить за всеми
- Использование интернет инфраструктуры
  - Унификация средств сбора информации, нет необходимости, простой доступ к потокам данных, возможность давления на recourse owner’ов
- Производится с использованием средств автоматизации
  - Накопление информации производится поточно, выключая в том числе ту, которая не может быть обработана сразу (включая зашифрованный трафик). В случае надобности делаются выборки по конкретным лицам или группе лиц.

Принципы массовой слежки

- Подготовка законодательной базы
  - Запрет на разглашение сотрудничества с гос органами, серые способы давления на recourse owner’ов
- Отрицание негативных последствий для свободы личности
  - Честным людям нечего скрывать
- Неявное или явное противодействие способам обхода слежки
  - Ограничения на использования криптографии, под предлогом обеспечения безопасности, блокировки, итд.

Мне нечего скрывать

Если вам нечего скрывать, может быть есть что скрывать другим.

“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say”

Не любое скрытие означает скрытие нелегальных действий.

(Использование занавесок не делает вас преступником)

Вопрос обеспечения доступности личных данных это вопрос доверия.

Мне нечего скрывать

Стоит ли доверить тому, кому вы предаёте свои данные?

Модель угроз и оценка рисков

При обеспечении защиты личный информации полезно явно или неявно построить модель угроз и модель противника (нарушителя)

- Выделение защищаемой информации
- Определение уязвимостей
- Определение угроз и их последствий из реализации
- Оценка возможностей противника
- Оценка рисков

Для понимая угроз и их последствий полезно понять, зачем противнику нужна это информация, и что вы потеряете, передав её.

Массовая слежка со стороны гос-ва

- Передача всех своих данных государству в реальном времени
- Усугубляется при увеличении информатизации
- Не известно, какая именно информация собирается и обрабатывается
- Не известна конкретная цель обработки и сбора информации
- Нет прозрачных механизмов контроля
- Возможности злоупотребления
- Безусловное доверие государству?

Телеметрия

Телеметрия – сбор метаданных о функционировании какой либо системы.

В целом – добрая штука, помогающая разработчикам систем отслеживать их поведение и ошибки, с целью их доработки.

В реальности – беспрерывная передача произвольной информации приложением или устройством, с целью сбора информации и пользователе.

Телеметрия… зачем?

Зачем собирать не анонимную телеметрию на пользователей?

Создание «персонализированных предложении» (слежка + классификация для последующей перепродажи явно или неявно), сбор статистики.(К слову об анонимности – использование идентификатора вместо имени – не есть анонимность.)

Телеметрия не нужна пользователю. Она нужна для разработчику и только ему.

Пример – WiFi в метро

https://******.io/feature/2018/10/24/proshli-mimo-kafe-a-vam-tut-zhe-pokazali-ego-reklamu-eto-ne-paranoyya

Отслеживающие cookie и прочие веб-штуки

- Отслеживающие cookie – cookie файлы, устанавливаемые владельцами ресурсов через сторонних провайдеров («сервисы аналитики»).
- При визите на сайт, он делает запрос на сайт стронного провайдера, к которому прикладывается отслеживающая cookie. Провайдер определяет пользователя по данным в cookie, и зная сайт, с которого переправили пользователя, дополняет информацию о нём.
- Провайдер затем сообщает владельцу сайта статистику посещений пользователя, оставляя себе всю остальную информацию

Отслеживающие cookie и прочие веб-штуки

- Сам же провайдер также использует эту информацию – явно продавая её, или обеспечивает «сервисный доступ» к ней, т.е. использует её при работе со своими клиентами (например – «рекламные предложения».
- Могут использоваться не только как услуга для сторонних сайтов, но и внутри собственных сервисов.

- Пример – поискали бесперебойники на яндекс маркете – получили рекламу в mail.ru
- Пример – загуглили название игры, получили рекомендации на youtube с роликами про неё.

Телеметрия и cookie, ну и что?

- Ну и пусть показывают рекламу. Мне то что?
- Во первых стоит понять – провайдеры отслеживания обладают большой информацией. И пользоваться они ей могут произвольно. Доверяете ли вы им все свои данные?
- Во вторых – задача провайдеров – заработок денег на основе информации. Они не хотят показывать вам «интересную» рекламу, или помочь с поиском. Им нужно больше денег, извлекаемой из вашей деятельности. Что бы они не говорили. «Мы уважаем вашу приватность, но будем использовать ваши данные чтоб впарить товары от наших партнёров»
- В третьих – отрицательные эффекты: эффект поискового пузыря, влияние на предпочтения через отображение результатов поиска итд.

Биометрия, камеры и прочите технические штуки

«Ну и как тебе поможет твой Tor против камер»?

Камеры ,биометрия и прочие датчики – возможность создания путей перемещения пользователя, получения статистики и извлечение метаданных. Главный виновник – система распознания лиц.

Слежка с использованием wifi MAC устройства

Сложно защититься от слежки.

Биометрия, как способ аутентификации

Биометрия не пригодна в качестве основного способа аутентификации.

- Нет механизмов финальных стадий срока жизни фактора аутентификации (уничтожение)
- Нет механизмов отзыва фактора
- Неотрекаемость фактора (сложно доказать подделку)
- Носит вероятностную природу (нейронки)
- Легко подделать (https://habr.com/ru/post/356612/)
- Легко обосновать слежу (смотри камеры у турникетов метро)

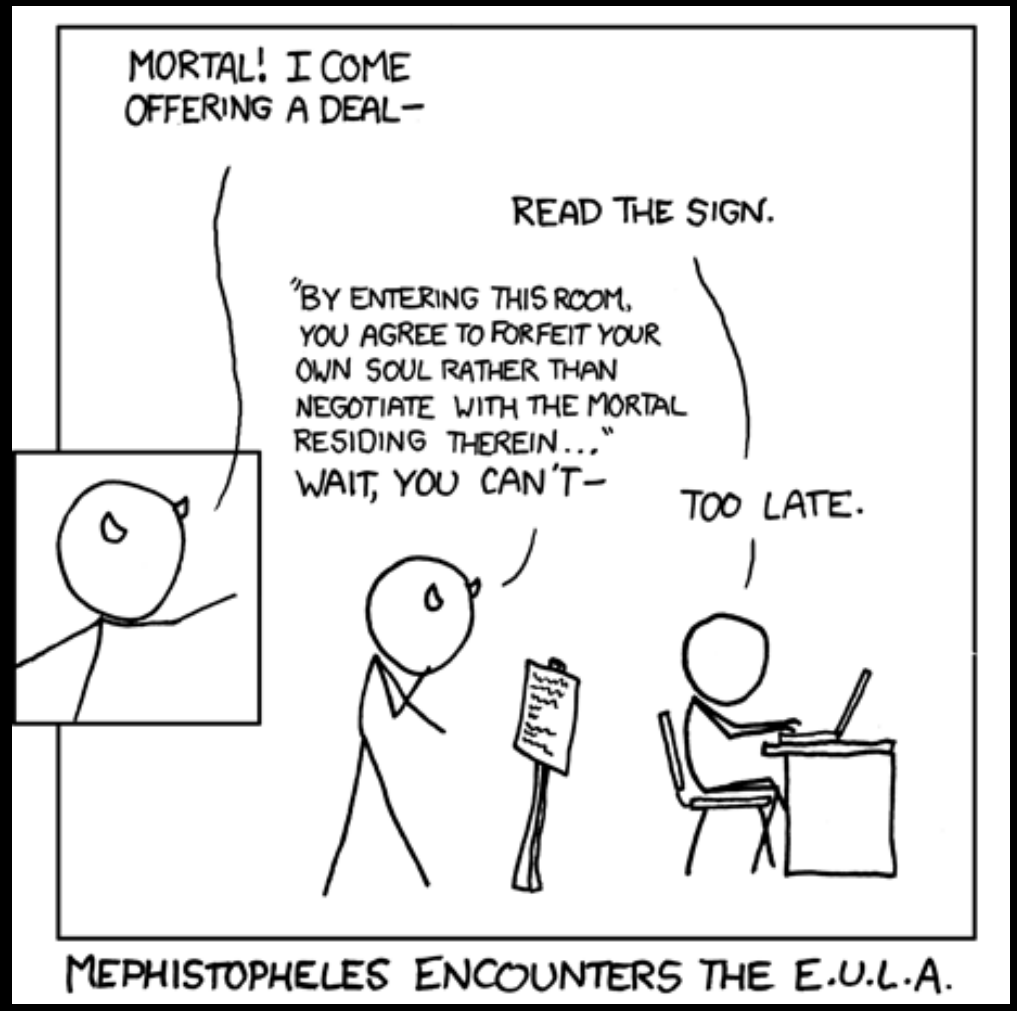
Рекламная компания массовой слежки

- Персонализированные рекомендации!
- Релевантная реклама!
- Используйте один логин на всех устройствах\сайтах!
- Необходимо создать учётную запись, для вашего же удобства!
- Нам обязательно нужен ваш email и телефон для идентификации … и вашей безопасности!
- Все ваши данные надёжно зашифрованы (но мы их расшифровываем и читаем каждый день)

EULA aka пользовательское соглашение

Как уговорить пользователя на всё – не разрешать пользоваться услугой или программой, пока он на всё не согласится.

Отдельное развлечение - читать соглашения. Многие составлены в стиле «Вы отказываетесь от всех претензий, мы собираем всю информацию какую можем, а взамен мы дадим вам временных неэксклюзивный доступ к нашей информации, которой вы не будете владеть. И мы можем менять наше соглашение и не обязаны вам об этом сообщать»



Двойственность информации в авторском праве

- С одной стороны информация приравнивается к физическим объектам, когда речь идёт об правообладателях. Спиратили и раздали софт 1000 раз? Потери равны 1000 * стоимость софта.
- С другой стороны при приобретении информации, она престаёт считаться объектом и вы являетесь максимально бесправным, и можете использовать её только определённым образом.
  - Доходит до того, что вы не имеете право взламывать защиту приобретённой программы, извлекать информацию и как либо её обрабатывать.
  - Аналогия – вы **купили** топор для рубки деревьев левой рукой, но как только вы начинаете рубить им правой – вас сажают в тюрьму за неправильно использование своего топора.

Интеллектуальная собственность и авторские права

- В целом современное авторское право защищает не автора или покупателя, а владельца информационных ресурсов.
- В настоящий момент уже и информацию нельзя купить. Продают доступ к ней (подписки).
  - Steam не продаёт игры. Почитайте соглашения. Они вам не принадлежат. Вы их не покупали. Вы перечислили деньги за право временного использования сервиса.
  - Нельзя уже даже сохранять информацию. Платя за подписку вы не имеете никаких «физических прав»
  - Доступ к подписке может быть отозван, удалены отдельные элементы итд. Невозможно резервирование.

Интеллектуальная собственность и авторские права

Корпорации пытались распространить это и на физические вещи.

- Пример – можно ли заправлять принтер в неофициальных сервисных центрах? Производитель утверждал что приобретённые картриджи не принадлежат пользователям, и заправляя их он нарушает соглашения.

- Благо логика восторжествовала, но не быстро.

- https://habr.com/ru/post/370603/

Как с этим бороться

- Не пользоваться поисковиками, отключить js, cookie, уйти в подполье? – мало реалистично и очень неудобно
- Для начало достаточно простого осознания. Для каждого случая отслеживания быстро построить модель угроз, и прикинуть, какие есть риски для вашей информации. Не забыть учитывать уровень доверия к сервису. Задуматься, почему мы доверяем google больше, чем одногруппникам и коллегам.
- По возможности переставать пользоваться не жизненно важными сервисами, нарушающими приватность и анонимность. В оставшихся сервисах по максимуму отключить все отслеживания.

Как с этим бороться

- Понимать, что крупные компании не заинтересованы в вашей приватности и конфиденциальности. В этом заинтересованы только вы. Их ограничивает только законодательство (и то далеко не всегда)
- Распространять информацию о способах защиты
- Использовать шапочку из фольги или титановую пластину в черепе для предотвращения сканирования мыслей

Ссылки

- https://www.eff.org/issues/privacy
- https://ssd.eff.org/
- https://www.privacyguides.org/en/ *
- https://www.nytimes.com/2019/12/24/opinion/location-privacy.html

* - замена оригинального https://www.privacytools.io/classic/, который сейчас содержит много аффилированных ссылок и рекомендаций.

Управление цифровыми личностями

Один из способов достижения анонимности в интернете – использование **независимых** цифровых личностей (digital identities).

Основные правила:

- Короткий срок жизни
- Отсутствие периодического использования или других наводящих метаданных
- Одна идентичность – для одной цели
- Не оставлять следов использования, надёжное уничтожение

Управление цифровыми личностями

Основные правила (продолжение):

- Независимое использование личностей. Зная все действия личности должно быть невозможно восстановить другие личности или реальную личности. Не должно быть общей информации между личностями.
- Невозможность компрометации реальной личности при компрометации цифровой
- Невозможность компрометации цифровой личности, при компрометации реальной
- Сложность компрометации (в том числе криптографической)

«Ты помнишь, что я буду жить вечно, а ты умрешь лет через шестьдесят?»

Сервис "На всякий случай"

Сервис "На всякий случай" позволяет уведомить выбранного вами человека или открыть ему доступ к определенным данным из вашего аккаунта, если вы перестанете им пользоваться. Чтобы выбрать действия, перейдите на страницу сервиса и нажмите **Начать**.

Как мы понимаем, что аккаунт активен

На это указывают определенные признаки. Среди них ваши входы в аккаунт, недавние действия, записанные в разделе Мои действия, работа с почтой Gmail (например, в мобильном приложении) и отметки в Google Картах на Android.

Что происходит после удаления аккаунта

Удаление аккаунта Google отразится на всех связанных с ним сервисах (например, Blogger, AdSense или Gmail), но по-разному. Проверить данные, связанные с вашим аккаунтом, можно в Личном кабинете. Если вы пользуетесь почтой Gmail, после удаления аккаунта вы потеряете к ней доступ. Вы также *не сможете повторно зарегистрировать то же имя пользователя Gmail.*