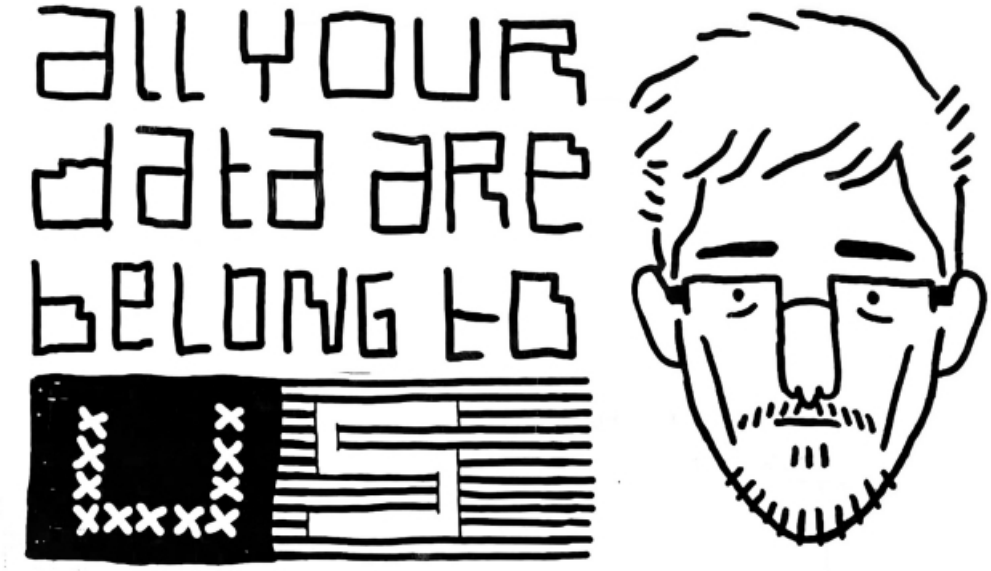
Таймлайн: Прослушка, часть 2

Часть вторая - новейшая история прослушки, в которой мы закрепим навык отличать шпионов от разведчиков, а также, наконец, поймем, почему "четвертая поправка" не мешает ловить шпионов, но защищает разведчиков.



Краткое изложение предыдущей части:

1. Конституция США образца 1787 года не отличалась продуманностью и демократичностью. Например, в этом основном документе полностью отсутствовал раздел, посвященный защите граждан от злоупотребления властью. Поэтому буквально через несколько лет в основной закон была внесена так называемая "четвертая поправка", которая защищает граждан от произвольных обысков и арестов.
2. С развитием телекоммуникационных технологий появилась необходимость защищать граждан также и от незаконного прослушивания. История была трудной и долгой, с громкими судебными процессами и неоднозначными решениями. Но в итоге было решено приравнять прослушку к обыску. И с 1968 года начал действовать "Закон Омнибуса о безопасности на улицах", где был установлен прямой запрет на организацию прослушки граждан без судебных санкций. Но в то же время была введена оговорка что "в целях защиты власти против свержения государственного строя" прослушивать можно и должно. Потом федеральное законодательство было расширено и усовершенствовано Актом "О защите электронных коммуникаций" Electronic Communications Privacy Act of 1986 (ECPA)
3. В США развивается целая индустрия специальных служб, которые занимаются электронной разведкой. Сначала это был проект "Трилистник" (Project SHAMROCK) для записи, хранения и обработки данных, переданных по телеграфу, который после ряда трансформаций организационного и технологического характера вылился в еще более масштабный проект ECHELON, завершившийся международным скандалом и массой расследований действий американских спецслужб и осуждением таковой практики.
4. Глобально отношение к массовой прослушке изменилось 11 сентября 2001 года - в "день, который изменил Мир".

Собственно, вот здесь нужно сделать некоторое отступление в повествовании и прояснить важную вещь: само по себе разумное наблюдение за поведением людей (хотел написать "граждан", но все же здесь более уместно "людей") в телекоммуникационных системах очень важно. Дело в том, что коммуникациями пользуются не только добропорядочные граждане, а совершеннейшие отморзки и злодеи в своих злодейских целях.

Несколько примеров

Для закрепления навыка отличия шпионов от разведчиков приведем несколько примеров.

Нарковойны

В конце семидесятых и почти все восьмидесятые годы главными злодеями "свободного мира" были колумбийские наркокартели. Это были хорошо организованные, вооруженные группировки, которые поставляли в США и страны западной Европы наркотики на миллиарды долларов. Оборот, например, "Медельинского картеля" во главе с Пабло Эскобаром на пике деятельности составлял десятки

миллиардов долларов, что превышало вообще всю легальную экономику Колумбии и оборот крупнейших корпораций, таких как например, "Дженерал Моторс".

На вооружении у картелей было, в том числе, тяжелое вооружение, зенитные комплексы и даже подводные лодки. И современные средства связи в том числе - для управления "наркоимперией" были необходимы коммуникации и налаженные процессы информационного обмена.



Люди с полным отсутствием какой-либо морали, которые просто убивали людей только за то, что кто-то плохо о них отозвался, получили колоссальную власть и возможности.

Неудивительно, что в конечном итоге властям США все это надоело и к "Управлению по борьбе с накробизнесом" были подключены спецслужбы, занимающиеся технической разведкой и та самая "ужасная АНБ". На контроль и прослушку были взяты вообще все спутниковые терминалы, которые ввозились в Колумбию. Все международные каналы связи. Не удивлюсь, если прослушивались и все местные переговоры, что, впрочем, не так уж и сложно - в восьмидесятых годах XX века телефонизация Колумбии составляла не более 5%, придя к 17% только к 2006 году.

В итоге спецслужбам США, при поддержке собственно властей Колумбии, удалось справиться с наркокартелями только к середине девяностых годов. Пабло Эксобар, благодаря плотной "опеке" со стороны технической разведки был отслежен и уничтожен. О том, как это все произошло, был снят довольно неплохой сериал "Narcos" с очень хорошими оценками в IMDB. Рекомендую. Почти в каждой серии герои сериала, так или иначе, обращаются за помощью к "службам технической разведки", чтобы получить необходимые оперативные сведения.

Как вывод: в целях борьбы с действительно серьезными криминальными угрозами - прослушка и средства электронной разведки необходима. Без вариантов.

Скандал с французскими партнерами

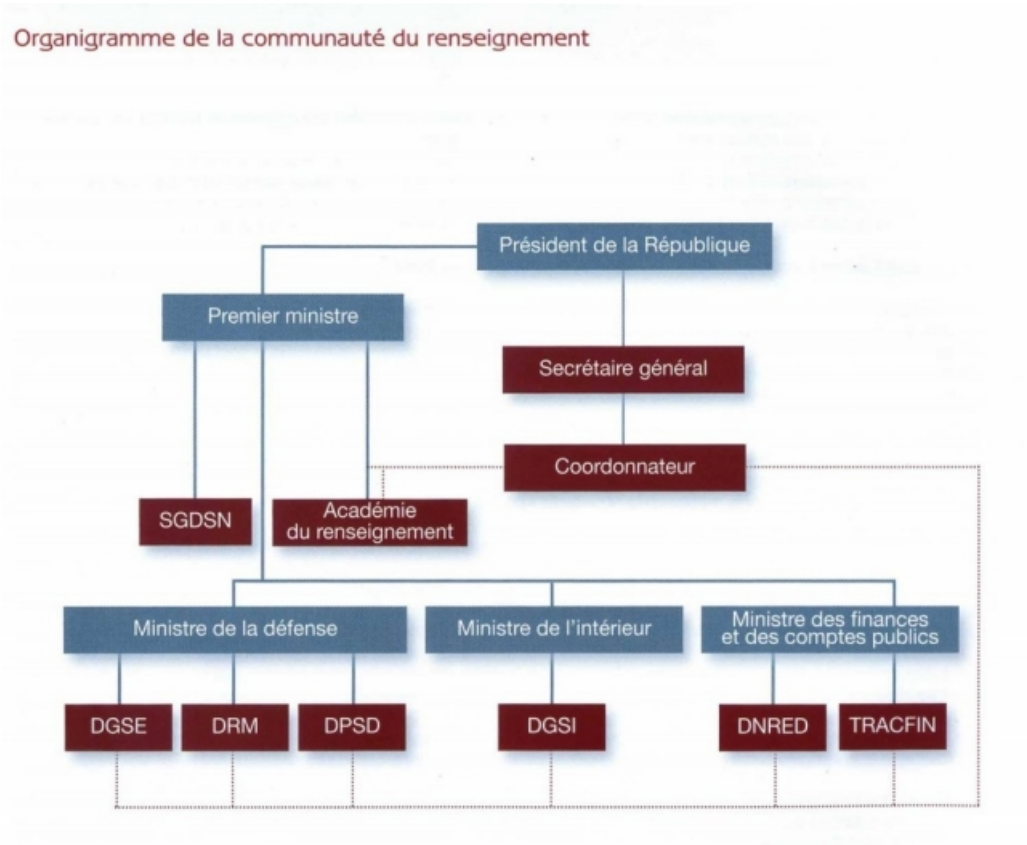
Отрицательных примеров использования технических средств съема информации достаточно много. Например, упоминаемый в прошлой статье скандал "Уотрегейт". И разумеется, это не единственный скандал. Правда, множество подобных раскрытых (никому не известно о нераскрытых - думается, что их много больше) случаев шпионажа были связаны с противостоянием между блоками в "Холодной войне". Но вот раскрытых случаев с "дружественным шпионажем" не так уж и много. Один из самых громких - промышленный шпионаж французских компаний против американских военных корпораций описан в 1993-ем году в газете "Нью-Йорк Таймз".

Разумеется, в газете мы не увидим всех технических подробностей, хотя в Сети наверняка можно найти больше подробностей. Ну, например, есть вот такой отчет в виде кейс-стади (учебный материал), который в коротком пересказе повествует о том, что французские компании, пользуясь техническими возможностями собственного оборудования, установленными на спутниках связи в рамках международного сотрудничества, снимали информацию научно-технического плана, чтобы успешно конкурировать с американскими компаниями в различных международных тендерах.

Жертвами промышленного шпионажа стали корпорации IBM, Boeing Corp., McDonnell Douglas Corporation, the Lockheed Corporation и General Dynamics Corporation.

Скандал был урегулирован дипломатическими службами, но, как говорится, осадочек остался.

Организационная структура разведывательных служб Франции. Без подробностей. Цель - показать, что разведка существует не только в США.



Трудно определить в этом эпизоде правых и виноватых. С одной стороны, французские власти поступали достаточно некорректно по отношению к американским партнерам. С другой стороны - напомню, что как раз в это же время бушевал скандал с ECHELON, где в подобных действиях обвинялись уже власти США. Отличить шпионов от разведчиков в такой обстановке крайне непросто. Точнее - проще простого. Все зависит от точки зрения наблюдателя. Если шпион "работает" в пользу стороны наблюдателя, то он никакой не шпион, а вовсе даже и разведчик, который стремится принести максимально пользы своей стороне.

Ликвидация Джохара Дудаева

Для полноты картины необходимо описать и одну из самых успешных операций российских спецслужб в "Первой чеченской войне" - ликвидация лидера банд-формирований Дудаева.

Все материалы по этому делу до сих пор засекречены, и мы можем судить об операции только по сообщениям прессы и официальных источников. Итак, что достоверно известно: 21 апреля 1996 года российские спецслужбы запеленговали сигнал от спутникового телефона Дудаева в районе села Гехи-чу, в 30 км от Грозного. В воздух были подняты два штурмовика Су-25 с самонаводящимися ракетами. Предположительно, Дудаев был уничтожен ударом ракеты прямо во время разговора по телефону с депутатом Госдумы Константином Боровым. Сам Боровой подтверждает факт разговора и его внезапное разъединение.

Таким образом, успех операции сильно зависел от работы служб технической разведки - очевидно, что для однозначного определения координат бандита нужно было точно знать, что данный телефон находится у него в руках. Поскольку Дудаев был далеко не дурак, и вполне себе представлял все риски использования средств связи, то очевидно, что велась очень сложная оперативная игра, было задействовано большое количество технических специалистов, которые, скорее всего, перехватывали и прослушивали все телефонные разговоры в данном регионе.



Возможно, это было нарушение "Закона о связи" (хотя он появился только в 1997 году). Возможно, это прямое нарушение п.2 ст. 23 Конституции РФ. И даже могу допустить, что никакого судебного решения в отношении прослушки всех телефонных разговоров не было - суд по логике обстоятельств не мог выдать такого решения.

Но факт остается фактом - бандит был уничтожен, что, возможно, спасло тысячи жизней мирных граждан.

Попробуйте порассуждать по этой теме.

Кажется, что результат превосходит все те неудобства граждан, связанные с нарушением их конституционных прав, и вполне может оправдывать действия текущей власти в законотворчестве. НО!

Но перейдем все же к изучению новейшей истории "Прослушки" в США.

Таймлайн

2001 год

В предыдущем Таймлайне уже упоминался Patriotic Act. Вокруг этого законодательного акта ведутся, пожалуй, самые ожесточенные споры, а в русскоязычной прессе не так много материалов, которые в полной мере бы раскрывали этот документ. В основном домыслы. Особенно официальных.

На самом деле, это очень объемный документ, который затрагивает достаточно много различных сфер жизни и состоит из десяти разделов. Коротко перечислим:

- Раздел I: Укрепление внутренней безопасности по борьбе с терроризмом
- Раздел II: Процедуры слежки и наблюдения (это как раз по нашей теме)
- Раздел III: Борьба с отмыванием денег для предотвращения терроризма
- Раздел IV: Безопасность границ
- Раздел V: Устранение препятствий к исследованию причин терроризма
- Раздел VI: Жертвы и семьи жертв терроризма
- Раздел VII: Межведомственный обмен информацией для защиты критической инфраструктуры
- Раздел VIII: Уголовное право в области терроризма
- Раздел IX: Расширение полномочий разведывательных служб (тоже наше)
- Раздел X: Другое

Как видите, "Патриотический Акт" - это не только про слежку и разведку. Но в нашем случае это именно то, что нужно разобрать.

Второй раздел дополняет уже работающие законодательные инициативы, которые мы уже разбирали - это FISA (Акт о негласном наблюдении в целях внешней разведки) и ECPA (Закон о защите электронных коммуникаций).

Расширение полномочий связано с несколькими достаточно спорными вещами, вокруг которых, отмечу особо, в американских судах всех инстанций идут непрекращающиеся процессы. С того самого 2001 года - не прекращаются.

Спорные моменты:

1. Sneak and peek warrant - "секретный ордер", который назвали "подкрасться и подсмотреть". Это такой специальный документ, когда суд разрешает органам правопорядка проводить "тайный обыск". Иногда такой "обыск" связан и со взломом физических помещений, не говоря уже о взломе информационных систем.
2. Roving wiretap - "особая прослушка". Как уже несколько раз упоминалось, Четвертая поправка прямо запрещает любой обыск без санкции судебных органов. Но в случае сложившейся практики использования средств телекоммуникаций, иногда очень трудно уследить за "перемещающейся целью". Например, если объект слежки использует одноразовые телефоны или пользуется услугами публичных средств коммуникаций. Каждый раз получать ордер на новый номер одноразового телефона - долго и неэффективно. Злодей может ускользнуть. Поэтому в "Патриотическом акте" имеется пункт об "особой прослушке", когда полиция может прослушивать фактически любого без ордера на основании каких-то подозрений. Но таки нужен ордер именно на "Roving wiretap".
3. Ability of the FBI to gain access - ссылки на отдельную статью в Википедии даже на английском нет. Если коротко, то это право спецслужб (ФБР) получить доступ к любому документу по требованию, включая доступ к документам, охраняемым другими законодательными актами. Например, к досье у адвокатов или медицинским данным пациентов. Очень спорное право, вокруг которого споры особенно ожесточенные.

Общая же характеристика изменений "Патриотического Акта" - они относятся только и исключительно к борьбе с терроризмом и все же соответствуют духу "Четвертой поправки". Ордер таки получать надо. Пусть и более широкого действия и иногда задним числом, но ордер судебных инстанций необходим. Более того, если в рамках расследования террористической деятельности вскроются факты совершения преступлений другого плана, то, скорее всего, они не будут приняты в судах. Хотя и могут быть использованы в оперативной работе.

Что касается расширения полномочий в рамках FISA (Внешняя разведка), то там все еще более сложно и запутано. Но именно расширение полномочий спецслужб в области "негласного наблюдения" позволило, например, найти и обезвредить террориста №1 - Усаму Бен Ладена.

2002 год

Создание National Joint Terrorist Task Force (NJTTF) - "Объединенных национальных сил по борьбе с терроризмом. Это такое "суперагентство", которое возникло из "Патриотического Акта" - Раздел VII.

"Объединение" создано на базе ФБР, но включает в себя группы из других силовых ведомств - таможни, иммиграционной службы, военных всех мастей и даже железнодорожной полиции. Очевидно, что такая группа должна быть сильно эффективнее, поскольку получает доступ к информации и навыки офицеров из многих источников. Но пока эта группа подвергается безжалостной публичной критике и особо себя не проявила. Впрочем, при существующем уровне секретности, общественность может и не знать...

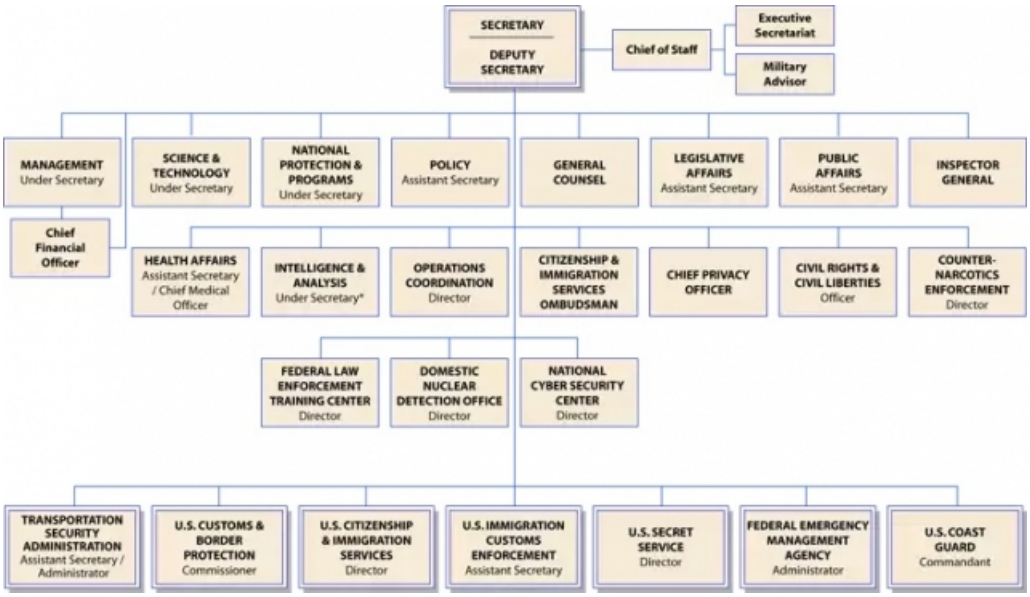
2003 год

Был принят следующий достаточно спорный законодательный акт, о котором почему-то в русскоязычных источниках еще меньше информации, чем о "Патриотическом Акте" - Homeland Security Act (HSA) - "Закон о национальной безопасности".

Этот закон еще больше расширяет границы "Патриотического Акта" и на основании него созданы правительственные организации с весьма широкими полномочиями. Например, создан United States Department of Homeland Security (DHS) - "Департамент национальной безопасности Соединенных Штатов". Фактически он был создан ранее - в 2002-ом. Но на "проектную мощность" вышел в 2003-ем.

"Департамент национальной безопасности" имеет астрономический бюджет (в 2011 году оценивался в 98,8 миллиардов долларов) и включает 240 тысяч (!) служащих.

Структура организации, если верить английской Википедии, примерно такая:



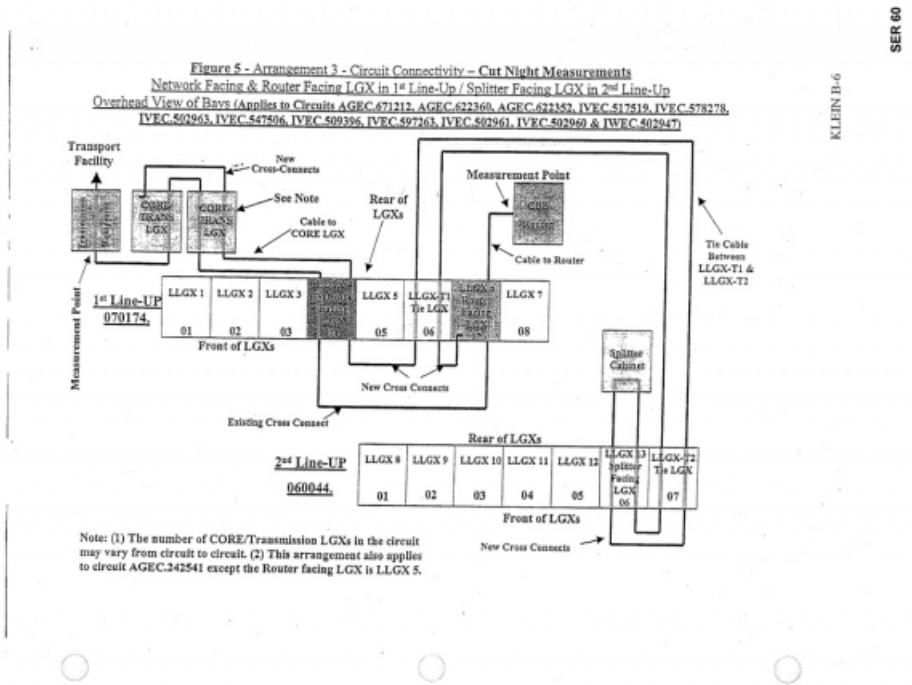
Фактически это была самая масштабная реогранизация всех силовых ведомств США со времен Войны за независимость.

А еще, в 2003-ем году разгорелся первый скандал, связанный с негласным наблюдением: техник корпорации AT&T Марк Клейн (Mark Klein) случайно обнаруживает секретную комнату (black room известной в прессе под номером 641A) в ЦОДе в Сан-Франциско. Позже он свидетельствует об этом, в федеральном судебном процессе против АНБ, возбужденной общественной организацией Electronic Frontier Foundation. По его показаниям получается, что комната была создана для функций "пылесоса" - сбора данных и негласному наблюдению за миллионами ничего не подозревающих американских пользователей Интернета. Причем, сбор данных осуществлялся не только за абонентами корпорации AT&T, но и, пользуясь положением корпорации, и за другими операторами. Вот документ.

Вот эта знаменитая комната:



Схема организации "отводов от оптических кабелей" из документов по незаконной слежке АНБ:



2005 год

Скандалы с незаконной прослушкой коммуникаций граждан США набирает обороты. В "Нью-Йорк Таймз" опубликована обличительная статья и выдвинуто общественное требование по аудиту деятельности спецслужб в области электронного шпионажа.

2006 год

Президент Джордж Буш (мл.), несмотря на общественное давление все же подписал продление действия и расширение полномочий "Патриотического Акта".

2007 год

Выходит очередной "Закон о защите Америки" (Protect America Act), который еще больше расширяет полномочия АНБ и ЦРУ в рамках FISA. При этом Министерство юстиции (Минюст) утверждает, что данный закон вовсе не задевает прав граждан США, а касается только и исключительно "защиты прав лиц, находящихся в Соединенных Штатах" и при этом "не препятствует сбору данных в целях внешней разведки, предоставляя разведывательному сообществу возможность закрыть критический разрыв в качестве разведданных, который существовал до того, как закон PAA стал законом". Это не очень качественный перевод прямой речи, но суть передает.

В рамках PAA спецслужбы теперь имеют право:

1. Вообще не получать никакого разрешения для негласного получения доступа к коммуникациям в отношении иностранных граждан.
2. Если в коммуникациях с иностранцами участвуют граждане США - сами виноваты.
3. Процедуры доступа к портам Lawfull Interception для целей внешней разведки сильно упрощаются.
4. Но сохраняется отчетность по процедурам доступа по "негласному прослушиванию", и спецслужбы все же обязаны отчитываться о своей деятельности. Особенно в отношении лиц и корпораций, которые "не согласились к сотрудничеству".

В октябре 2007 года президент Буш выпускает первую "Национальную стратегию по обмену разведывательной информацией" - National Strategy for Information Sharing (NSI).

Это такая стратегическая стратегия, которая обязывает "делиться информацией" с Департаментом национальной безопасности все правительственные учреждения и организации США.

2008 год

Поняв, что в работе предыдущих актов по сбору разведданных по FISA не приводит к желаемым результатам в отношении особенно иностранных организаций (телекоммуникационных компаний в первую очередь), были предложены ввести не только карательные мероприятия, но и поощряющие. Все еще президент Буш подписывает очередные поправки в FISA, которые вводят иммунитет по судебному преследованию телекоммуникационных компаний в случае утечки данных, которые участились. К некоторым функциям CALEA получили доступ нехорошие хакеры - совершенно очевидное следствие из того бардака, который образовался при неконтролируемом использовании Lawfull Interception.

Такое явление, как WikiLeaks получает всемирное распространение - первые утечки, нужно отметить, стали появляться чуточку раньше - с 2006-го.

2009 год

Очередная разоблачительная статья в "Нью-Йорк Таймз" о превышении полномочий АНБ в области сбора данных простых граждан. Назревает серьезнейшая проблема с overcollection данных и необходимость защиты персональных сведений.

Ссылка на статью - разумеется английскую.

2010 год

Срок действия "Патриотического акта" опять продлен президентом Бараком Обамой. На один год.

США, как один из крупнейших игроков в области воздушных перевозок, стали оказывать давление на организации по управлению воздушным транспортом. В том числе на международные и общественные. Целью давления стала программа Secure Flight, разработанная в "Администрации транспортной безопасности США" (United States Transportation Security Administration - TSA), которая подразумевает ведение списков пассажиров и учета их "благонадежности". Например, если некто включен в "спецсписок нежелательных пассажиров", то вполне возможно, что этому некто даже не продадут билет, если он собирается лететь в США.

Пик скандала с WikiLeaks. Некоторые новостные ресурсы публикуют выдержки из секретных военных документов, которые "слил" рядовой первого класса (ефрейтор в РА) Брэдли Мэннинг. Мэннинг был арестован в мае 2010 года в Ираке по обвинению, как минимум, в 21 эпизоде, связанных с утечкой более полумиллиона секретных армейских документов. Документы эти, включая дипломатическую переписку, были перехвачены в результате работы FISA в кабельном хозяйстве операторов связи в Ираке и Афганистане.

2011 год

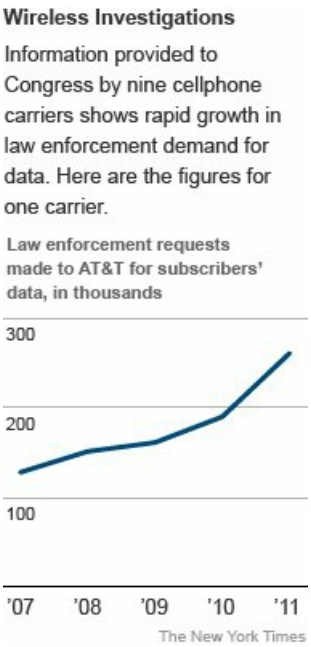
По делу WikiLeaks в суд вызываются представители компании Twitter. Цель - выявить лиц причастных к "сливу информации", поскольку эти самые лица активно использовали социальную сеть для обмена сообщениями. Twitter был вынужден "поделиться" всей известной информацией со спецслужбами. Скандал был раскрыт на страницах Гардиан.

И, тем не менее, в мае сего года, действие "Патриотического Акта" опять было продлено и расширено Конгрессом США и подписано президентом Б.Обамой.

2012 год

Конгресс США опять выпускает ряд поправок к FISA. Президент Обама опять подписывает. Срок действия поправок продлен на пять лет. Получается, что они истекают в будущем году и нужно пронаблюдать подпишет ли новые поправки новый президент Трамп.

И снова "Нью-Йорк Таймз" публикует информацию о беспрецедентных масштабах массовой прослушки операторов мобильной связи: всего за год правоохранительными органами было запрошено 1,3 миллиона требований абонентской информации. Полиция запрашивает данные об отправленных SMS или геопозиционирование абонентов. Компания AT&T вынуждена отвечать на 700 подобных запросов в день. Отчеты операторов представляют данные о значительном увеличении интереса спецслужб к данным об абонентах за последние пять лет:



2013 год

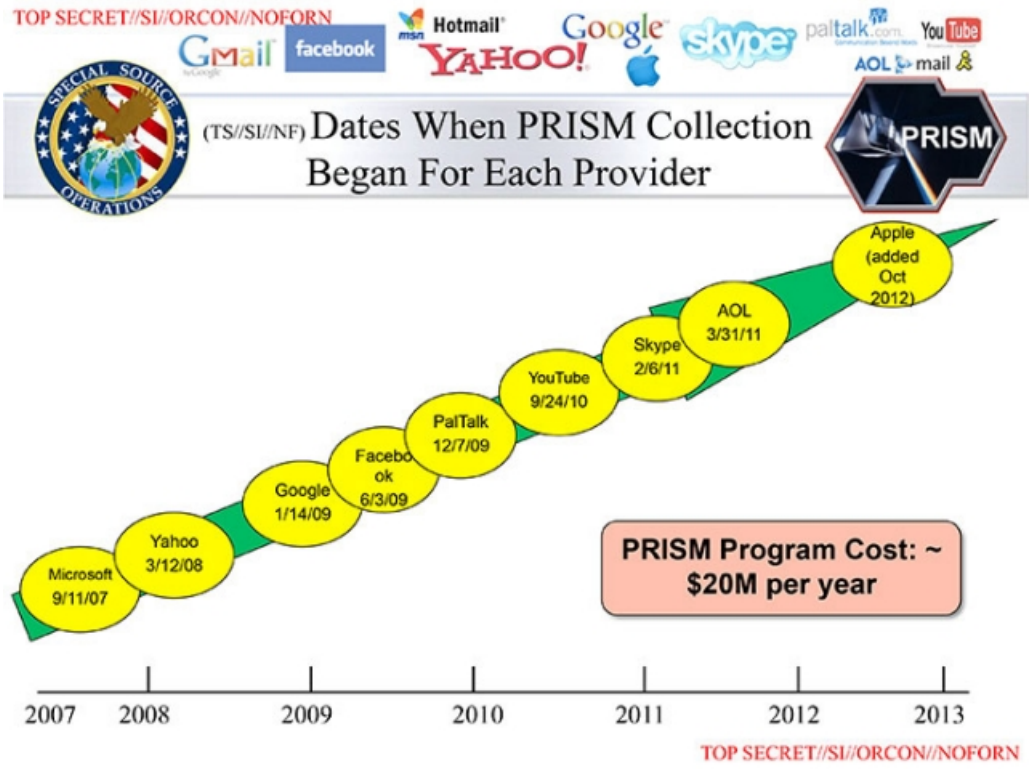
Гардиан сообщает, что федеральный судья Роджер Винсон издал секретное постановление, обязательное для исполнения компанией Verizon, по которому оператор обязан постоянно "сдавать" метаданные о всех вызовах абонентов в АНБ за квартал. То есть все данные о фактах вызовов, номерах, продолжительности разговора и т.п. Всех абонентов.

Есть сведения, что подобные секретные ордеры выданы и другим операторам, но утечка была только про Verizon.

Потом издания The Guardian и The Washington Post почти одновременно публикуют данные о секретном проекте АНБ с кодовым названием PRISM. Вот собственно эта информация.

Оказывается, суперсекретный PRISM был запущен еще в 2009 году и по опубликованным данным почти все интернет-компании, так или иначе, сотрудничают с АНБ и предоставляют информацию по личным данным миллионов пользователей.

Вот такой таймлайн "подключения к программе":



Microsoft сдался первым. Yahoo, Google, Facebook, Apple, AOL - все "под колпаком".

Два дня спустя, 8 июня, Канцелярия директора АНБ выпускает трехстраничный комментарий со ссылкой на FISA и поправки к нему, устанавливая точкой отсчета 2008 год, когда поправки начали действовать. Не поленитесь и вернитесь к этому году на нашем таймлайне...

21 июня правительство предъявляет обвинения в шпионаже против Эдварда Сноудена - бывшего сотрудника АНБ.

Далее события развиваются как в плохом детективе: директор ФБР Роберт Мюллер признает, что Соединенные Штаты используют беспилотники в рамках программы внутреннего надзора. То есть, военные дроны используются, в том числе, и для физического наблюдения за гражданами США. Выступая перед Законодательным комитетом Сената, Мюллер соглашается с тем, что иногда наблюдение с помощью БПЛА нарушали право на тайну личной жизни. И "высказал озабоченность данным фактом". "Использование беспилотников является достойным обсуждения и, возможно, законодательного регулирования".

Против программ неконтролируемой слежки развернуто широкое общественное обсуждение и, в том числе, назначены судебные слушания. Первое решение против программы наблюдения АНБ было вынесено 16 декабря судьей Ричардом Леоном из Федерального окружного суда округа Колумбия. По его словам, действия спецслужб "скорее всего, значительно" нарушает действие Четвертой поправки против необоснованных обысков. "Я не могу себе представить более неизбирательного и произвольного вторжения в личную жизнь граждан, чем это систематическое и всеобъемлющее коллекционирование данных на практически каждого гражданина без предварительного согласия суда", - заявил судья Ричард Леон. Правительство опиралось на прецедент, установленный Верховным Судом (США) от 1979-года в деле "Смит против штата Мэриленд" (суд признал, что метаданные - вызовы номеров и их длительность - не являются нарушением "разумного ожидания сохранения частной жизни"), чтобы оправдать свою шпионскую программу. Таким образом, сбор данных о вызовах и их длительности обо всех абонентах телефонной сети без надлежащего судебного ордера является вопиющим нарушением Четвертой поправки, а абоненты вправе рассчитывать, что таковая информация не станет доступной третьим лицам. На возражения защиты FISA судья Леон заявил, что с учетом изменений в технологиях, "прецедент Смита" больше не может относиться к текущим обстоятельствам.

В итоге, 18 декабря, по заказу президента Обамы некая "консультативная группа" выпустила 300-страничный доклад, в котором были рекомендованы 46 изменений в программы слежки АНБ.

Рекомендации, в том числе, включают:

Обязательную авторизацию на получение метаданных с целью проведения оперативных мероприятий на оборудовании третьих лиц - телекоммуникационных и/или интернет компании. То есть, аналитики АНБ обязуются получить распоряжение суда до факта получения доступа к данным.

Требование получения постановления суда правительственными организациями в случае необходимости раскрытия клиентской информации.

Запрет на использование "бэкдоров" в программном обеспечении для получения разведывательной информации.

В судах при рассмотрении дел по практике действий спецслужб должен быть введен "приорат гражданских свобод". То есть, в тех случаях, когда делается выбор между получением важных разведсведений и нарушением частной жизни большого количества граждан, то выбор должен быть "за гражданские права". В настоящее время такие дела рассматриваются, как правило, в частном порядке, и только правительственные организации определяют целесообразность и приоритет выдачи ордеров.

В то же время, доклад признает однозначную важность ведущихся программ негласного наблюдения и слежки в АНБ с целью "предотвращения террористических атак".

2014 год

17 января 2014 года президент Обама объявил о подготовке соответствующих реформ спецслужб на основании представленных (выше) рекомендаций. Обама признал, что, несмотря на всю важность и текущую законность (действительно - есть же законы) работы АНБ, некоторые действия Агентства ставят под угрозу гражданские свободы.

Но готовящиеся реформы, по мнению той же EFF, несколько половинчаты и компромиссные. Например, за АНБ остается право доступа ко всей инфраструктуре без санкций судов в случае введения чрезвычайных ситуаций. Метаданные операторы, тем не менее, все же обязаны собирать и хранить за квартал и предоставлять к ним доступ по запросу спецслужб. АНБ, тем не менее, будут обязаны приостановить оперативную разработку (прослушку, короче) на лидеров союзных государств, но государства "не союзные" такой привилегии не дождутся. В тоже время, "глубина

анализа" связей и контактов лиц, связанных с террористической деятельностью, должна будет ограничена "вторым уровнем", то есть наблюдение "только за друзьями террористов", а наблюдение за "друзьями друзей" должно быть прекращено. В то же время Конгресс должен назначить специальных адвокатов для обеспечения принципа судебной состязательности при рассмотрении дел о прослушке и электронной разведке. Но дела по линии FISA (иностранная разведка) будут рассматриваться как прежде.

Другими словами, Обама выполнил не все рекомендации комиссии.

Стоит отметить еще один доклад, который был выпущен наконец-то заработавшего "Совета по надзору в области защиты частной жизни и гражданских свобод" - Privacy and Civil Liberties Oversight Board (PCLOB). Это такой комитет консультативного характера при Конгрессе. Был основан еще в 2004-ом году, но потом прекратил деятельность.

С текстом доклада можно ознакомиться здесь, только осторожно - 238 страниц юридического английского. Кратко, "есть мнение, что программы слежки АНБ, очень может быть, вероятно, не очень законны и не совсем конституционны. Кроме того, и это важно, все эти программы и не доказали свою эффективность в борьбе с терроризмом. В докладе, в который раз, содержится рекомендация о закрытии темы массового сбора метаданных.

И на фоне всего этого политеса и юридической возни выясняется, что в Германии был раскрыт подкуп чиновника, который копировал и пересылал в США массу разведывательных данных и документов. Потом был раскрыт еще один шпион ЦРУ в Германии. В качестве протеста против не очень дружественных действий Германия высылает всем известного (раскрытого) резидента ЦРУ из Берлина.

2015 год

В мае сего года, судейская коллегия 2-го окружного апелляционного суда США Манхэттена, по результатам рассмотрения дел о деятельности АНБ, вынесли решение, что Конгресс никогда не санкционировал массовый сбор, запись и обработку телефонных разговоров граждан США. При этом деятельность АНБ противоречит даже собственно "Патриотическому Акту". И даже больше! Сбор огромных массивов данных о гражданах начался ДО собственно появления "Патриотического Акта" и, следовательно, деятельность некоторых программ Агентства национальной безопасности, является незаконным. Коллегия, тем не менее, руководствуясь интересами национальной безопасности, прямо не запретила все программы прослушки и сбора данных, но призвала Конгресс внести поправки в закон.

В 97-ми страничном решении суда, федеральный судья Джерард Линч написал: "Столь масштабное и экспансивное развитие государственных хранилищ записей о частной жизни миллионов граждан США является беспрецедентным нарушением разумного ожидания о конфиденциальности всех американцев".

И самое, пожалуй, интересное. Вся эта "программа массовой слежки" была абсолютно засекреченной до 2013 года. До того момента, пока она не была раскрыта Эдвардом Сноуденом.

2 июня 2015 года (запомните эту дату) был принят "Закон о свободах в США" - The USA Freedom Act. Президент Обама подписывает этот закон.

По данному Акту АНБ запрещается собирать массивы данных о гражданах США (речь идет о гражданах - еще раз, иностранцев этот акт не касается) по результатам телефонных переговоров или других средств коммуникаций.

Теперь ответственность за сохранность этих данных переходит на коммуникационные компании, которые могут предоставить данные по запросу правительству только на основании судебных ордеров.

Однако закон совершенно не отменяет те самые три положения "Патриотического Акта", а наоборот - продлевают их, поскольку положения Акта как раз истекли 1 июня: "особая прослушка", право на взлом и право требования любых документов. Но с ограничениями по правоприменению и введению персональной ответственности за нарушение регламентов.

Заключение

Я уже писал, что тема очень тонкая и запутанная. Данный материал не претендует на "истину в последней инстанции", но я постарался снабдить свои сентенции ссылками на викифицированные (то есть подтвержденные другими ссылками из нескольких источников) статьи в английской Википедии.

Русская Вики, увы, не полна и кое-где даже противоречит первоисточникам. Возможно, кое-где я допустил ошибку фактологическую или просто неправильно перевел.

По этому поводу не нужно истерить в комментариях, а просто укажите на неточность - я постараюсь оперативно исправиться. В конце концов, это не диссертация, а просто попытка разобраться и разложить факты во времени.

Вполне возможно, что в скором времени появится более подробная статья про PRISM - материалов Гардиан достаточно для разбора. Вполне возможно, что отдельного таймлайна заслуживает противостояние NSA versus Apple. И вполне возможно, что для полного понимания нужно описать еще такое явление, как "Свидетельство канарейки". Тема, повторюсь, столь обширна, что потянет на объемную книжку, но у меня не так много времени, увы.

Традиционная гифка нынче такая:



Это, если что - Джеймс Коми. Директор ФБР с 2013 года. Гифка хорошая.