Таймлайн: Прослушка

Неожиданное продолжение "Таймлайнов" даже для меня самого. Появление этого материала связано с огромным количеством сетевых споров, которые, как правило, сводятся к тому, что оппоненты начинают ссылаться на бронебойный аргумент...

"а вот в Америке негров линчуют!"



Дескать, в США давно уже есть CALEA, Echelon и Patriot Act! Поэтому СОРМ, вкупе с "антитеррористическим" 374-ФЗ (aka "Пакет Яровой") - это всего лишь ответ на внешние вызовы. И вообще все так делают.

Конечно же, такой "аргумент" в спорах интеллигентных и образованных людей - недопустим, поскольку, по сути, означает "сам дурак". И особенно этот аргумент выглядит жалким в речах людей, облеченных властью - законодательной ли, или исполнительной. Хотя бы потому, что перечисленные системы электронного шпионажа не столь однозначны и подвергаются жесточайшей критике и собственно в США.

Нужно добавить, что уж если аргумент ~~"а у вас негров линчуют"~~ "в США тоже есть системы слежки за гражданами" принимается к обсуждению, то, будучи последовательным, нужно также и признать, что эти системы подвергаются серьезной публичной критике в тех же США и не только.

Посему, я считаю, что это просто необходимо - выбрать время и попытаться разобраться, что там действительно происходило с прослушкой каналов коммуникаций с целью поимки злодеев, и как этот процесс отражается на жизни граждан. В США, разумеется.

В то же время, предмет прослушки и перехвата сообщений - тема очень обширная и запутанная, где все зависит от точки зрения субъекта и его опять-таки субъективной оценки явлению. Попытки относиться к теме нейтрально и отстраненно, лично у меня к успеху не привели - все равно скатываешься к отстаиванию собственной точки зрения. Моя заключается в том, что тотальная прослушка, и тем паче запись и хранение всех разговоров граждан - нарушает базовые принципы о свободе личности, совести и слова.

Но существует и другая точка зрения, которую необходимо учитывать - безопасность, разведка и прочие государственные надобности. Человеческое общество несовершенно и агрессивно. Здесь существуют мошенники, убийцы, педофилы, террористы, религиозные фанатики и наркодиллеры, которых всенепременно необходимо излавливать и изолировать. Причем, злодеи так же пользуются телекоммуникационными технологиями в своих злодейских целях и необходимо как-то это пресекать.

Следовательно, совершенно нормально, что правоохранительные органы не только интересуются способами гласного и негласного съема информации и слежки в Сетях. И это никакой не секрет, поскольку государства вырабатывают правила с учетом мнения силовых структур и выпускают законы, которые позволяют силовикам некоторые вещи, недоступные "обычным гражданам". Тем не менее, и "силовикам" нельзя позволять все. Действия правоохранительных органов должны контролироваться, регулироваться и ограничиваться - это тоже довольно очевидный факт, но

разработчиками законодательства в одной северной стране напрочь игнорируется.

А вот в США (да-да, любимейший аргумент для сетевых холиваров) - права, обязанности и "законные интересы граждан" довольно четко-конкретно прописаны. Хотя и невероятно запутаны прецедентной системой правосудия. И для того, чтобы разобраться в мешанине я даже попытался прослушать курс на Courser'е на языке вероятного противника под названием "Surveilance Law" (Закон слежки) от Стенфордской правовой школы. Автор - Джонатан Мейер. Курс жесткий, со множеством очень специальной правовой лексики и довольно объемный - 48 видео по 5-10 минут. Не осилил. Но те, кто владеет языком лучше, чем beginers+ получит удовольствие и массу полезных знаний из первоисточника, а не перепевки нодовцев про национализацию Центрального Банка.Вот ссылка.

И заканчиваю введение, перехожу к таймлайну.

Ранняя история

1791 год

Да, эта история настолько ранняя. Этим годом датируется издание "Билля о правах". Сам "Билль" - это поправка к Конституции США, в которой совершенно "забыли" внести раздел о правах и свободах человека. Весь Билль состоит из десяти поправок, но в данном контексте нас интересует две - "четвертая" и "пятая".

Четвертая поправка в переводе звучит так:

> Право народа на охрану личности, жилища, бумаг и имущества от необоснованных обысков и арестов не должно нарушаться. Ни один ордер не должен выдаваться иначе, как при наличии достаточного основания, подтвержденного присягой или торжественным заявлением; при этом ордер должен содержать подробное описание места, подлежащего обыску, лиц или предметов, подлежащих аресту.

У сего документа сложная история правоприменения, которое можно изучать отдельно. Но в контексте "слежки" было принято судебное решение, что использование подслушивающих устройств и использование других электронных методов снятия информации, не связанные с физическим обыском, также приравнивается к обыску. Решение было артикулировано только в 1967 году Верховным Судом США при разбирательстве дела "Катц против Соединенных Штатов", где Суд установил, что право на неприкосновенность личной жизни защищает человек и от других видов обыска. В частности суд решил, что подслушивающие устройство, установленное с наружной стороны стекла телефонной будки также может быть обыском.

Пятая поправка гласит, что лицо, обвиняемое в совершении преступления, имеет право на надлежащее судебное разбирательство, не должно привлекаться к ответственности дважды за одно и то же нарушение и не должно принуждаться свидетельствовать против себя, а также, что государство "не имеет права изымать частную собственность без справедливого вознаграждения".

В части электронной слежки пятая поправка касается того, что никто не может заставить гражданина свидетельствовать против себя. Следовательно, собственные, например, электронные письма или записи в дневнике не могут рассматриваться в суде, как безусловное доказательство вины обвиняемого.

1928 год

Прошло довольно много времени, прежде чем понятие "Тайны связи" вообще вошло в судебную практику США. И без малого полтора столетия в "самом демократическом государстве" этого понятия не существовало вовсе. Впрочем, судебные решения, тем не менее, существовали и в отношении почты, телеграфов, телефонной связи. И все решения ссылались на ту самую "четвертую поправку".

В частности, были неоднократные разбирательства относительно перлюстрации писем из мест заключения. Были судебные решения в отношении почтовых служащих. И даже однажды был сорван приговор в отношении обыска мусорных ведер за пределами домохозяйства.

Но, повторюсь, какого-то конкретного законодательства, кроме четвертой поправки и внутренних документов, например, адвокатов (адвокатская тайна), врачей (медицинская тайна) или "тайны банковских операций" не существовало. Все договоренности о тайне были джентльменскими и регулировались отношениями субъектов. И даже больше! Считалось, что "четвертая поправка" действует вообще только против федеральных органов, в то время, как законодательство конкретного штата или даже муниципалитета, не подчиняется действию "права на охрану личности

и имущества".

Гром прогремел в суде в 1928 году в деле "Рой Омстед против Соединенных Штатов".

Суть дела заключалась в том, что очень успешный бутлегер (при этом бывший полицейский) был пойман на незаконных операциях с алкоголем, благодаря установленной за ним слежке и прослушке телефонных переговоров.

Надо отметить, что Омстед действительно был крутейшим бутлегером в Сиэтле и ввозил запрещенный "Сухим законом" алкоголь морскими судами, руководя преступной организацией в несколько сотен человек. Но все обвинения против него были основаны на показании полицейских (более 70-ти человек), которые "висели на проводе" в местной телефонной станции несколько месяцев.

Адвокаты Омстеда утверждали, что такие доказательства не могут быть рассмотрены судом, поскольку как раз нарушают "четвертую поправку" о неприкосновенности частной жизни, куда, собственно, и относятся, в том числе, телефонные переговоры.

Но суд, после многомесячных рассмотрений, все же решил, что прослушка ничего не нарушает.

Роя Омстеда посадили.

И почти на каждой крупной телефонной станции появились так называемые "Черные комнаты" (Black Room) - специальные помещения, где сотрудники полиции могли спокойно прослушивать всех, не получая для этого ордеров и санкций суда.

1934 год

Президент Рузвельт подписал "Федеральный Акт (закон) о Коммуникациях (связи)" (Federal Communications Act).

Пожалуй, это первый законодательный акт, регулирующий электронные коммуникации в полном объеме - от телефонной связи, до распределения радиочастотного спектра.

Но вопросов, касающихся тайны связи, законодательный акт почти не касался. Вся собранная в процессе "технических мероприятий" информация не считается противозаконной. Но не может быть раскрыта или опубликована.

Зато в FCA-1934 был пункт об отказе в обслуживании, если оператор заподозрит абонента в незаконной деятельности. Но этот пункт никогда не работал в итоге - суды обычно вставали на сторону абонента, справедливо возражая, что телефонная компания не может квалифицировать деятельности абонентов, как законную, или незаконную, даже если имеет место быть, например, прием ставок на тотализаторе или торговля наркотиками. Только полиция на основании судебного решения может установить "отказ в обслуживании".

1945 год

А возможно и несколько ранее. Стартует проект "Трилистник" (Project SHAMROCK) - является предтечей всех этих страшных PRISM и ECHELON.

Суть проекта - сбор, хранение и обработка всех сообщений, передаваемых по телеграфу. Сначала проект "SHAMROCK" был чисто "учебно-тренировочным" - "Агентство безопасности вооруженных сил" (AFSA - The Armed Forces Security Agency) начали разведывательную игру (подробностей не уточнял) в связи с известными военными действиям. В результате "игры" накопился какой-то массив данных по отправленным телеграфным сообщениям в компаниях Western Union, RCA и ITT, который хранился на микропленках. Аналитики AFSA начали анализировать и сопоставлять сообщения и в итоге были пойманы какие-то шпионы.

Идея анализа всех коммуникаций понравилась "силовикам" и впоследствии к "игре" присоединились ФБР, ЦРУ, Сикрет Сервис и Управление по борьбе с наркотиками.

И ни один суд не санкционировал сей масштабный проект - служители плаща и кинжала просто писали, хранили и анализировали данные. Когда (в 1975 году!) масштаб деятельности "Трилистника" достиг полутора миллионов перехваченных телеграмм в месяц, кто-то "проболтался в прессу". Программу разогнали, а результатом стал выход специального акта - Foreign Intelligence Surveillance Act (FISA), о котором мы поговорим чуть позже. Потому что более важное событие произошло в 1952 году.

Средняя история

Технологии после Второй мировой войны начали стремительно развиваться. Имеются в виду технологии сбора, хранения и обработки информации. Собственно WWII тоже оказала значительное влияние на процесс. Особенно военных впечатлил нацистский проект Enigma, который был в клочья разнесён британским проектом Bombe. Про этот эпизод криптовойны снято сотни кинофильмов и написано тысячи книг, поэтому в данном материале мы просто о них упомянем и двинемся дальше

1952 год

Проект "Трилистник" впечатлил причастных к военной разведке не меньше Энигмы. Оказалось, что не только "закрытая" информация может приносить пользу в военном деле. Но и вполне себе "открытая" информация не менее, а подчас даже более полезна для победы ~~добра над злом~~ разведки над шпионами (вот тут вы должны прекратить читать и тут же начать комментировать, разъясняя автору разницу между "шпионом" и "разведчиком". Автор очень ждет этих комментариев).

Так вот. На базе упомянутой AFSA, в 1952 году создается ужасная NSA - National Security Agency - Агентство Национальной Безопасности. Страшный сон всех ~~шпионов~~ разведчиков и ~~диверсантов~~ патриотов других (не США) государств.

Создал АНБ своим секретным указом президент Трумэн. В состав Агентства вошло то самое AFSA вместе со всем персоналом и накопленными телеграфными сообщениями на микропленках. И, разумеется, все "Черные комнаты" теперь становятся вотчиной АНБ, которая имеет высший приоритет доступа к ним. Миссия АНБ при основании - неизвестна. Секрет же. В настоящее время частично такая: "чтобы победить террористов (врагов США) в стране и за рубежом, в соответствии с законами США. А также для защиты неприкосновенности частной жизни и гражданских свобод".

1967 год

"Дело Катца против Соединенных Штатов" - судьбоносный процесс, в котором песочные часы "приватность против безопасности" были перевернуты.

Верховный суд США отменил прецедент Омстена 1928 года.

Дело было так: Чарльз Катц занимался приемом игорных ставок по телефону из Лос-Анжелеса, где игорный бизнес был запрещен, и передавал ставки в Майами и Бостон, где такая деятельность была разрешена.

Для решения вопроса о приватности, Катц занимался сим не совсем законным (в Л-А) делом в телефонной будке (в США с самого начала каждая телефонная будка имела возможность принимать входящие звонки, в отличие от). В общем, у него был эдакий "мобильный офис" в телефонных будках.

Сотрудники ФБР, которые занимались оперативной работой по данному случаю, просто установили прослушивающие устройства на внешней строне телефонных будок, где Чарльз обделывал свои делишки, справедливо считая, что раз будки общественные, а жучки установлены снаружи, то никакая четвертая поправка тут не сработает.

Но когда доказательная база была приобщена к делу в суде, то адвокаты Катца выиграли дело, создав тем самым прецедент по "разумному ожиданию сохранения частной жизни" (Expectation of privacy).

Катц был оправдан, а в законодательстве появился принцип определения приватности, в том числе в публичных местах, на основе двух определений: "ожидание приватности" и "признание разумности ожиданий".

Более подробно, пожалуй, пусть этот случай рассматривают юристы.

1968 год

Конгресс США (очевидно, под впечатлением от дела Катца) принимает первый в своем роде законодательный акт "Закон Омнибуса о безопасности на улицах". Закон известен, прежде всего, установлением федерального правила "предупреждения Миранды" (ну, все знают про это: "Вы имеете право хранить молчание, все, что вы скажете - будет использовано против вас...") и федеральным же ограничением возраста права на оружие.

Но в том числе, в "Законе Омнибуса" содержалось ограничение на прослушку телефонных разговоров без санкций судебных органов. То есть, даже если технически силовые структуры ничем не ограничивались в слежке за гражданами (а технически никак и не уследить же), то в случае судебных разбирательств, записи перехватов и/или запись разговора (помните эти

диктофоны/микрофоны на спине в полицейских фильмах?) не принимались во внимание без судебного ордера. И даже немножко больше - полицейский сам мог быть подвергнут судебному преследованию, если о прослушке без ордера становилось известно.

Но в "Акте Омнибуса" существует и оговорка о преимуществе президента США в данном вопросе "в целях защиты власти против свержения государственного строя". То есть, санкции на прослушку могли дать два органа власти: судьи США и собственно действующий президент.

А еще, был серьезно увеличен бюджет ФБР. И АНБ.

1972 год

Знаменитейший "Уотрегейтский скандал".

Когда-то давно, еще при "советской власти" я очень любил перелистывать старые подшивки журналов "Крокодил", "Огонек" и "Нева". И если журнал был начала семидесятых, то с вероятностью 95% он содержал хотя бы одно упоминание об Уотергейте. Очень знаковое событие, в результате которого импичмент получил тогдашний президент Ричард Никсон.

Собственно, причиной скандала стал факт ловли с поличным "подозрительных личностей", которые занимались установкой прослушивающей аппаратуры в предвыборном штабе от демократов. Никсон был республиканцем.

История не просто запутанная, но содержит адовое количество нестыковок, домыслов, инсинуаций и просто политических ошибок. Смотрите фильм "Глубокая глотка".

1974 год

Импичмент Никсона с формулировкой "незаконное прослушивание телефонных разговоров, злоупотребление ЦРУ, лжесвидетельство, взяточничество, воспрепятствование осуществлению правосудия и другие злоупотребления исполнительной властью".

1975 год

"Комитет Черча", возглавляемый сенатором Фрэнком Чёрчем, начинает серию расследований о методах сбора разведывательных данных в ЦРУ и ФБР. Публикуются сотни вопиющих фактов нарушения четвертой поправки в части организации прослушки (wiretapping) без судебного ордера и установки несанкционированного наблюдения "электронными методами".

Итогом расследований (помимо сотен фильмов про шпионов, которые легко и непринужденно убивают друг друга) стала инициация закона FISA. Но это чуть позже.

1978 год

Собственно, принятие FISA - Foreign Intelligence Surveillance Act - "Акт о негласном наблюдении в целях внешней разведки".

Подписал Акт президент Картер. Собственно закон предписывает процедуры физического и электронного наблюдения и сбора внешней разведывательной информации, передаваемой иностранными державами и агентами иностранных держав (которыми, в том числе, могут быть американские граждане).

Считается, что Закон не применяется вне США. В FISA после террористических атак 11 сентября неоднократно вносились поправки.

1986 год

К третьей части "Закона Омнибуса" вносится поправка, которая потом становится отдельным законодательным актом, известным сейчас как Electronic Communications Privacy Act of 1986 (ECPA) - Закон о защите электронных коммуникаций.

Он прямо запрещает следственным агентствам США любые формы перехвата любых электронных сообщений или их чтения в местах временного хранения (до полугода) без соответствующего ордера. То есть, к "Закону Омнибуса" о простой телефонной прослушке (wire tap), которая запрещается без ордера, добавлены другие средства коммуникаций, которые появились к тому времени. А это: пейджинг, мобильные телефоны, трекинговые системы и прочие системы передачи информации электронным способом.

В ECPA имелась одна "дырка", которая впоследствии подвергнута жесткой критике - акт защищал

коммуникации "реального времени", но если какие-то сообщения хранятся "более 180 дней", то они полностью выводятся из поля правового регулирования. То есть, электронная почта, которая могла храниться явно больше квартала, могла быть прочитана без судебных санкций.

И вот то, что "больше 180 дней", оно регулировалось другим Актом - SCA - Stored Communications Act. Закон о хранимых коммуникациях (некорректно перевел - как лучше?).

Закон довольно запутан, и в некотором смысле противоречив, поскольку никакой практики по хранению данных в те времена просто не существовало.

Но с одной стороны - закон защищал пользователей "электронных средств коммуникаций" от вмешательства третьих лиц, поскольку предусматривал уголовное преследование вообще всех, кто обращался за информацией, переданной по сетям электросвязи, без судебного ордера.

С другой стороны, ограничение в 180 дней было обусловлено тем, что хранение массивов данных большее время было экономически неэффективным, и считалось, что если вот некто не "забрал", например, письмо с почтового сервера, то через 180 дней (разумный и достаточный срок), то по аналогии с почтовыми сообщениями (US Post может вскрыть отправления, если фактически не могут их доставить, с целью выяснения адреса возврата), их могли прочесть, в том числе провайдеры.

Дикий 1986 год.

1995 год

Год можно назвать концом "средней истории". В этом году был зафиксирован случай преднамеренного взлома компьютерных сетей по предписанию суда. Офицер "Службы криминальных расследований ВМС США", Питер Гарза (Peter Garza) выследил и представил доказательства "хакерских действий" со стороны некоего Julio Cesar Ardita, широко известного в узких кругах, как "El Griton".

Ардита занимался взломом аккаунтов в Гарварде, через которые выходил на различные правительственные информационные системы. В том числе, военные. Чем он там насолил - неизвестно. Но раз к этому делу подключился NCIS, то дело, очевидно, было серьезное...

Новая история

Отсчетом новой истории "прослушки" следует считать 1996 год, когда вышел новый федеральный закон "О связи". Или тот же 1995-й, когда вступил в действие CALEA - Communications Assistance for Law Enforcement Act.

На самом деле, эти два законодательных акта тесно переплетены - просто законодатели решили разнести две правовых сущности с целью изменять при необходимости по частям.

Немного подробнее рассмотрим оба Акта:

CALEA

Закон "о прослушке", как это ни странно, появился чуточку раньше нового закона "о связи". Собственно, цель CALEA простая - ловить злодеев посредством негласной, но законной прослушки телефонных переговоров (потом расширено на VoIP и ШПД). Решительный подход был связан с очень быстрым развитием технологий и ростом абонентской базы, "органы правопорядка" стали отмечать, что "черных комнат" им становится как-то недостаточно. Да и оборудования в black room становится слишком много и оно слишком дорогое.

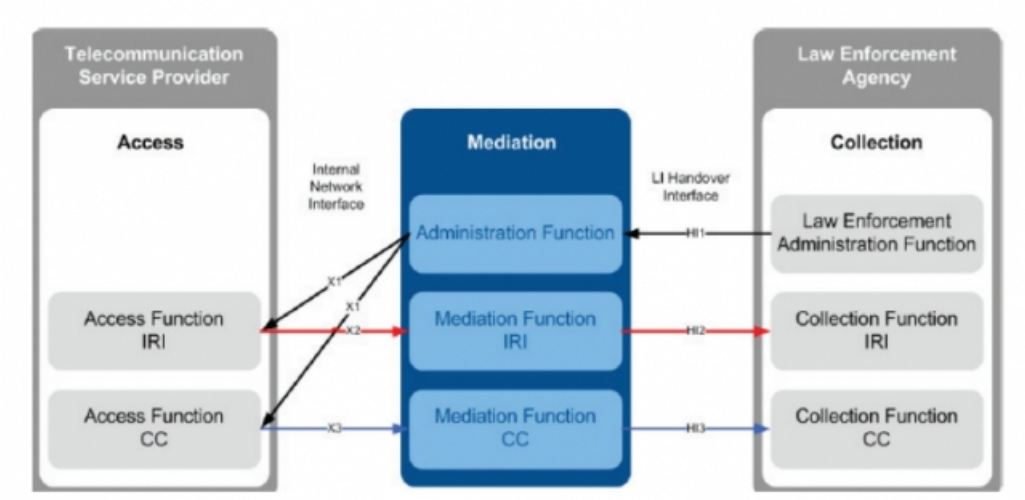
Хотя по целям и реализации CALEA очень напоминает российский СОРМ, за исключением одной маленькой, но существенной детали, которая ставит два закона с одинаковыми целями в разные углы ринга. Реализацией.

Дело в том, что CALEA не предусматривает никакого вмешательства операторов в работу системы. Вообще никакой - ни финансовой, ни технической, ни эксплуатационной. Поступили гораздо проще - всем производителям оборудования заранее выдали спецификации "как нужно делать". Причем, стандарты были предварительно и основательно обсуждены в мировом масштабе. И не в США, а в Европе. Этим занимался European Telecommunications Standards Institute - ETSI (Европейский институт по стандартизации в области телекоммуникаций), со штаб-квартирой в Софии Антиполис, Франция. Потом вопросами стандартизации "законного съема информации" занимались еще 3GPP и CableLabs.

Технические стандарты и тонкости реализации в данном материале не рассматриваются - цель несколько другая. Но любопытный читатель сможет легко ознакомиться и изучить все подробности

Lawfull Interception на официальном сайте ETSI.

Общая схема организации LI-портов выглядит как-то вот так:

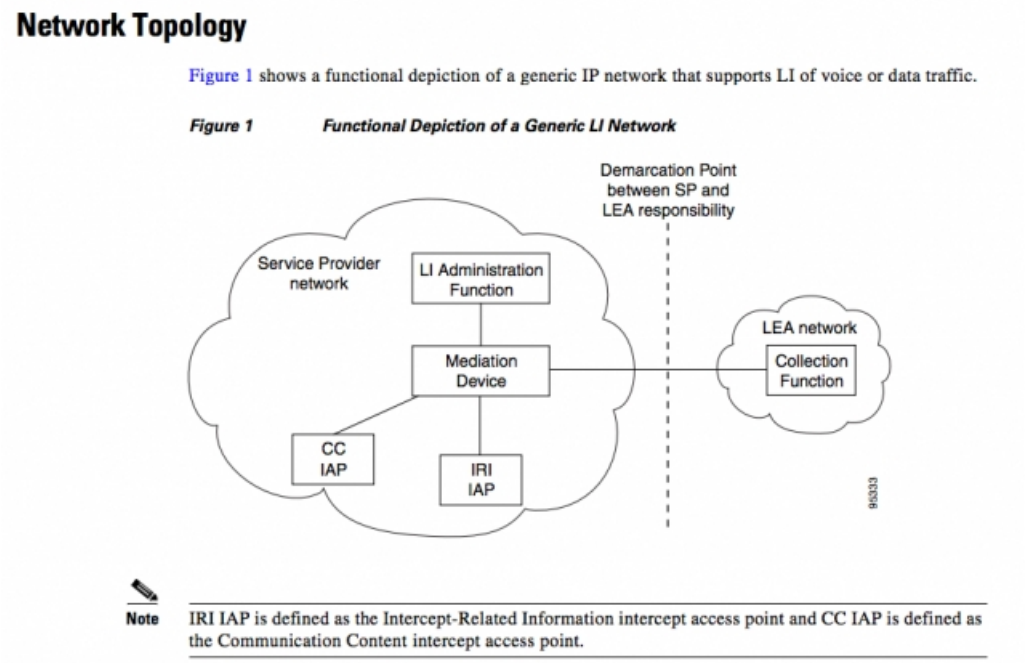


Вот тут есть хороший отчет "как это работает", если Wikileaks у вас не заблокирован. Но главное - в Акте CALEA нет требования для операторов строить сию систему за свой счет. Просто все приобретаемое после 1995 года оборудование уже должно иметь функции Lawfull Interception (пресловутые LI-порты, которые, кстати, не существуют в виде "отдельной дырки"). Если оборудование было приобретено оператором до 1995 года, то на модернизацию оператору выделялись некоторые средства, разумеется, по очень бюрократическому процессу, но выделялись.

Если оборудование приобреталось после 1995 года и не имело LI-функционала, то оператор сам себе злобный буратино, и модернизировал его за свой счет.

Достаточно просто и справедливо.

Подключение физическими каналами и установка аппаратуры съема (Mediation Device) осуществляется за счет "органов" из специального бюджета. Вот так выглядит структурная схема LI от Cisco:



Network Topology

Figure 1 shows a functional depiction of a generic IP network that supports LI of voice or data traffic.

Figure 1 Functional Depiction of a Generic LI Network

Note IRI IAP is defined as the Intercept-Related Information intercept access point and CC IAP is defined as the Communication Content intercept access point.

Достаточно подробно все описано тут.

И, кроме того, процесс "легального съема" - LEA на аппаратном уровне по стандарту не может быть осуществлен без процесса согласования.

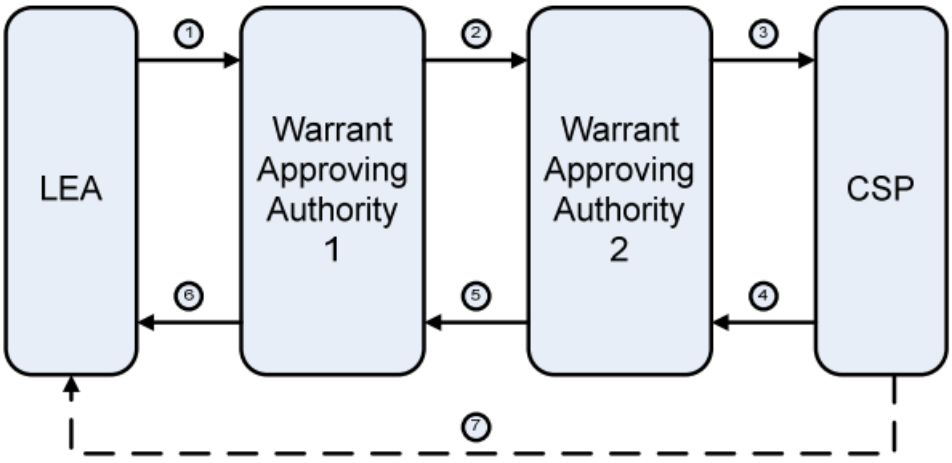


Figure A.3: Scenario with multiple Approving Authorities

Иногда очень запутанного и многоступенчатого. Это как определят конкретные органы правопорядка - напомню, что стандарт LEA от ETSI - международен, а в США в разных штатах могут быть различные законы касающиеся описанной темы. Главное соответствовать федеральному стандарту, описывающие минимум, но в процесс могут быть внесены значительные изменения.

Ситуацию с российскими СОРМами (и тем более с последним "антитеррористическим пакетом") вы можете обрисовать самостоятельно.

The Telecommunications Act of 1996

"Закон о связи" от 1996 года вообще никак не касался темы "прослушки", а главная его цель в те времена было приведение в соответствие с появившимися новыми технологиями - интернет, мобильная связь, телевещание, кабельное ТВ и т.п., которых в Законе от 1934 года просто не было.

А еще в ТА-96 была прописана демонополизация рынка и ставилась точка в процессе демонополизации гиганта AT&T. Ну, и либерализация телекома вообще. Девиз закона: "let anyone enter any communications business -- to let any communications business compete in any market against any other" - "пусть в телеком-бизнес приходит, кто захочет - пусть все конкурируют со всеми".

Особое внимание в ТА-96 было уделено распределению радиочастотного ресурса, который является ограниченным по определению. И главное - в США отсутствует понятие "лицензирования деятельности операторов связи". То есть, оператором может стать любой субъект предпринимательства, который ни у кого не обязан справляться, но обязан соблюдать общие правила, принятые в общей бизнес-среде - соответствие стандартам, принципу "недискриминации", соответствие другим законодательным актам, например, CALEA.

Кроме того, в ТА-96 был включен раздел (Title) VII под заголовком "Прочее", где запрещались "недобросовестные практики" и вменяется в обязанность защита клиентской информации - sec.702.

В завершение нужно отметить, что Закон постоянно подвергается жесточайшей критике и в него вносятся изменения. Плюс - прецедентное право на основании судебных решений. В 2006 году (забегаем вперед) ТА-96 был дополнен и расширен Биллем (Telecommunications Bill of 2005), где были описаны услуги и сервисы, не существовавшие в 1995 году - VoIP, перенос номеров (MNP/LNP), обязательные службы-911 и тому подобное.

2001 год

В этом году все изменилось. И необходимо начинать новую главу "новейшая история прослушки", которая получается слишком большой и будет опубликована отдельно.

Почему 2001 год стал переломным?

Ну, потому что событие 9/11 привело к пересмотру всей парадигмы информационной безопасности вообще.

Почти сразу же после обрушения башен WTC одиннадцатого сентября, Конгресс США усаживается за работу и пересматривает положения FISA и ECPA. Принимается Patriot Act - "Закон о борьбе с терроризмом".

Но это не значит, что в период с 1995-го по 2001 годы ничего не происходило. В это время как раз бушевал первый скандал, связанный с реализацией масштабнейшего ~~шпионского~~ разведовательного проекта ECHELON.

ECHELON

Глобальная система радиоэлектронной разведки, названная секретно-кодовым словом ECHELON появилась не вдруг. Пожалуй, для этой системы нужен отдельно-параллельный таймлайн или даже отдельная статья.

Впрочем, статей про это существует великое множество, и еще она не добавит смысла и обзорности.

Посему, очень кратко:

ECHELON начал создаваться еще во время WWII на почве союзнических отношений между армиями США, Великобритании и примкнувшим к ним Канады, Австралии и Новой Зеландии. Все вместе это называлось Пять Глаз (Five Eyes).

В разгар "холодной войны", примерно с начала шестидесятых годов, работы по проекту были интесифицированы, что привело к построению станций радиослежения по всем миру.

По сути - ECHELON это огромная сеть огромных радиоприемников, которые сканируют весь радиоэфир и записывают всю передающуюся по радио информацию.

И было бы странным, если б такая система не появилась - в СССР тоже пытались строить что-то похожее.

Но средствами радиоперехвата не ограничивались, и где-то в семидесятых (точные даты, имена/фамилии, явки, координаты - до сих пор секретны), в компании Lockheed Martin были заказаны спецсредства по съему информации из других сред. Проект в LM носил код P415, а созданное программное обеспечение (очевидно, не только программное, но и аппаратное - на дворе семидесятые и микрокомпьютеры только-только появляются) называлось SILKWORTH и SIRE.

Впрочем, все это вы сможете более подробно прочитать в соответствующих статьях, которыми наполнены интернеты. В основном они содержат конспирологию и домыслы, поскольку, повторюсь, большая часть информации о системе все еще засекречена в соответствии с FISA, которая появилась как раз в 1978 году.

В 1988 году произошла первая утечка о системе в прессу - статья "Кто-то слушает" в журнале "The Statesman" (очень рекомендую!) произвела эффект разорвавшейся бомбы.

Оказывается, во-первых, систему использовали не только против "агрессивного СССР и стран СЭВ", но и против граждан США. Во-вторых, слушаются не только военные, но и вообще всё. Ну, по крайней мере, есть техническая возможность слушать телефоны почти по всему миру. В статье как раз рассказывается, что с помощью прослушки ловятся и "кокаиновые бароны" из Колумбии - тогда как раз было обострение на почве борьбы с наркомафией.



Далее последовала длинная череда утечек, интриг, скандалов и расследований по всему миру. Напомню, что в программе участвовали не только США, а сама программа сначала называлась "пять глаз". А там, где тайну знает больше двух - тайны не существует.

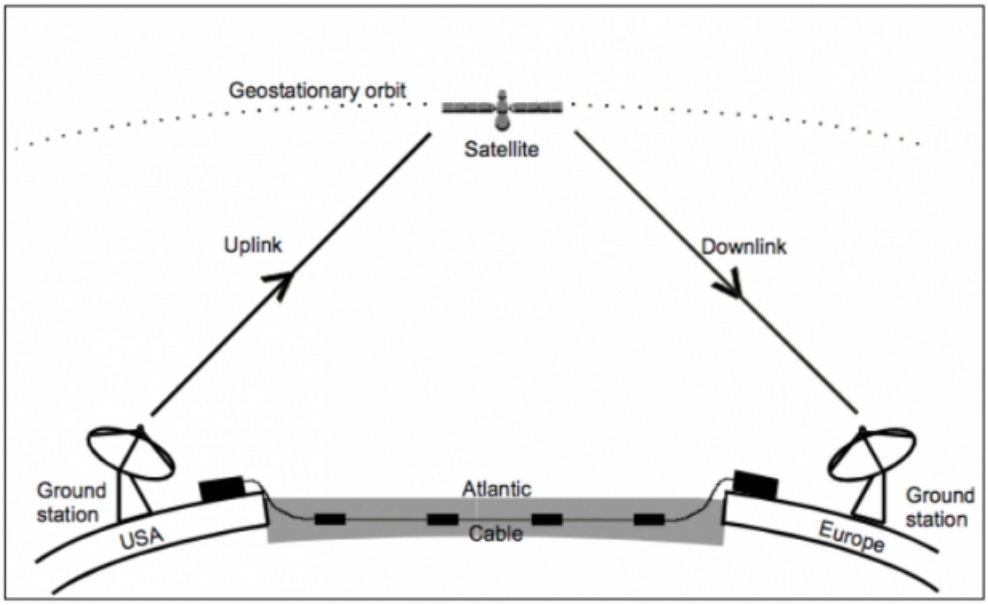
Хотя секреты остались.

Итак, "Эшелон" действительно существует. "Эшелон" действительно может перехватывать почти все сообщения в радиочастотном спектре (с оговоркой - дальней связи - вряд ли "Эшелон" прямо вот сейчас слушает мой трафик в 2,4GHz Wi-Fi). И "Эшелон" был создан в процессе "холодной войны" для противодействия СССР. Это все действительные факты, подтвержденные в прессе и заявлениями ответственных лиц.

По правовым вопросам существования ECHELON ведутся жаркие споры и по сей день, а вот в девяностые велось расследование по вопросу вообще возможности существования данной системы.

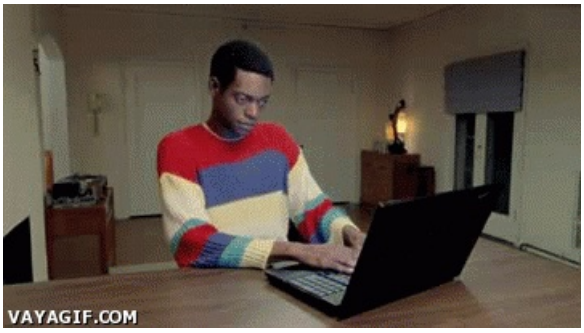
И вот буквально в июле 2001 года, за считанные месяцы до событий 9/11, Европейской комиссией был опубликован доклад "О возможности существования глобальной системы электронной слежки". С текстом доклада можно ознакомиться лично.

Например, вот схема из доклада, "которая многое объясняет":



4.2.3. The most important satellite communication systems

И только после прочтения всех 194 страниц вступать в бурные конспирологические дискуссии. Но помните, что с вероятностью 95% ваши сообщения будут прочитаны западной разведкой:



Продолжение следует...