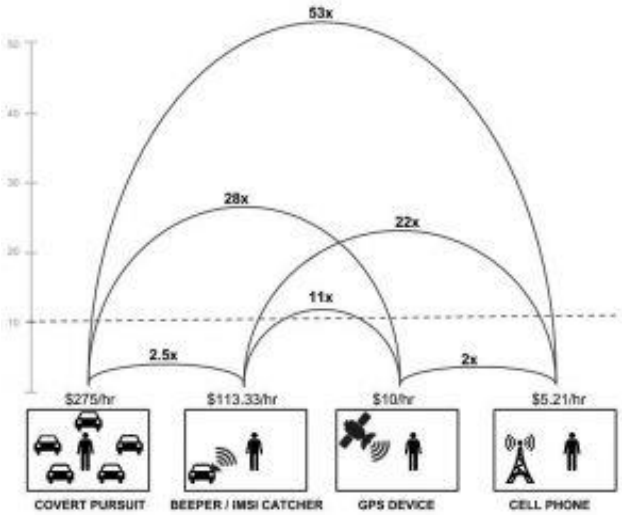
В XX веке многие детективы начинались с того, что главный герой замечал слежку за собой. Это служило явным показателем чьей-то серьезной заинтересованности, потому что такая слежка совсем не дешева. Согласно недавнему (и уже вполне реальному) исследованию, опубликованному в The Yale Law Journal, примерная стоимость скрытного слежения при помощи квалифицированных агентов составляет 275 долларов в час.

При исполнении на высоком уровне, слежка требует пять машин и пять агентов. С учетом естественного ограничения в виде всего 14000 спецагентов в штате, ФБР, например, не могло следить более чем за 2800 подозреваемыми. Конечно, это ограничение больше не актуально, поскольку современные технологии позволяют следить за подозреваемым, вообще к нему не приближаясь. По оценкам исследователей, установив специальный GPS-трекер, за человеком можно следить, затрачивая всего 10 долларов в час, а запросив данные о местоположении у сотовых операторов, можно тратить на слежку еще вдвое меньше.

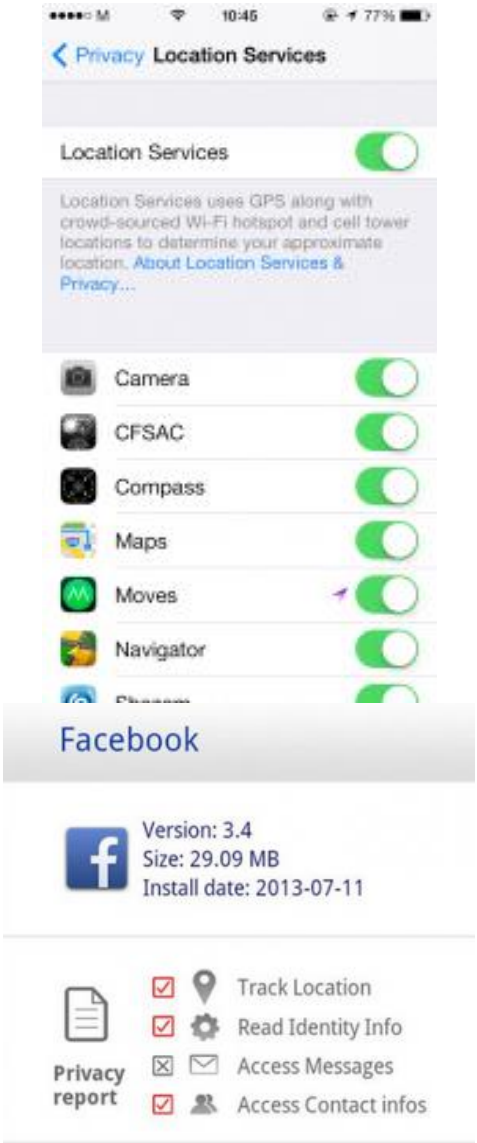


Это означает, что то же ФБР легко может отслеживать в 50 раз больше людей, чем в прошлом веке.

Более важно другое - подобная слежка по силам и по средствам не только ФБР или ФСБ, но и многим другим. Ваш смартфон отправляет данные о текущем времени и вашем местоположении целому ряду структур, включая владельца смартфонной экосистемы (Apple, Google, Microsoft), мобильным рекламным сетям (AdMob и др.) и разработчикам приложений. Например, популярные фитнес-приложения наподобие

Moves собирают и анализируют информацию о местонахождении, чтобы посчитать потраченные калории и пройденные километры. Более того, есть приложения, специально созданные сугубо для шпионажа и доступные любому заинтересованному лицу, будь то ревнивая жена, начальник или конкуренты.

Единственный путь избежать этого дешевого и эффективного способа слежки довольно радикален. Надо прекратить пользоваться мобильным телефоном или как минимум не брать его, отправляясь по секретным делам. Если ваша озабоченность слежкой не настолько высока, можно уменьшить доступность своих данных, проанализировав и проредив список приложений, следящих за вашим местоположением. Для этого в iOS есть особый экран настроек, а в Android - целая пачка специализированных приложений.



Кроме того, для борьбы со шпионскими вредоносными приложениями требуется полноценная система защиты смартфона, которая также защитит от SMS-спама, фишинга и кражи устройства.

Источник: http://blog.kaspersky.ru