ЗА ТАЙНАТА НА МЕСТОПОЛОЖЕНИЕТО И КАК ДА НЕ Я ЗАГУБИТЕ ЗАВИНАГИ

Системите, които създават и съхраняват цифрови записи на движението на хора в публичното пространство ще станат неделима част от всекидневието през следващото десетилетие. Ние вече сме свидетели на подобни системи, а в близко бъдеще ще се появяват все повече.

Ето някои примери, за които може вече да сте чели или използвали:

- Електронни билети за градски транспорт.
- Електронни устройства за събиране на такси (FastTrak, EZpass в САЩ).
- Мобилни телефони.
- Услуги, съобщаващи ни, когато имаме познати наблизо.
- Търсения на вашия PDA (джобен компютър) за услуги и компании близо до мястото, на което се намирате в момента.
- Безплатен Wi-Fi с реклами на фирми, близо до вас.
- Електронни магнитни карти за врати.
- Стоянка, отчитаща времето за паркиране, на която можете да се обадите, за да добавите пари и която ви изпраща текстово съобщение (sms), когато времето ви изтича.

Тези системи са изключително новаторски и обещават ползи, започващи от повишено удобство и достигащи до нови видове социално взаимодействие. За съжаление, те представляват и драматична заплаха за тайната на местоположението.

Какво означава “тайна на местоположението”?

Тайна на местоположението (известна още и като “поверителност на мястото”) е правото на всеки да се движи в публичното пространство като очаква, че при нормални обстоятелства местоположението му няма да бъде системно и тайно записвано, за да бъде употребен записа по-късно. Системите, обсъждани по-горе, имат потенциал да лишат хората от тайна на местоположението им, като правят възможно за другите да задават (и да отговарят на) следните видове въпроси, консултирайки се с базата данни за мястото:

- Бяхте ли на антивоенен митинг в четвъртък?
- Присъствахте ли на среща за планиране на митинга една седмица по-рано в къщата на някой “Боб Джаксън”?
- Ходихте ли в клиника за аборти?
- Срещнахте ли се със съветник по въпросите, засягащи заразени с вируса на СПИН?
- Били ли сте в мотел по време на обедната си почивка?
- Защо секретарката ви е била с вас?
- Дали сте отскочил в обедната почивка до потенциален инвеститор, за да му предложите изобретението си? Кой точно инвеститор?
- Вие ли бяхте човекът, който анонимно предупреди контролните органи за опасни стоки или машини?
- Срещахте ли се, Вие и вашият вицепрезидент, с “ACME” ООД в понеделник?
- Коя църква посещавате? Коя джамия? Кои гей барове?
- С кого ще вечеря бившата ви приятелка?

Разбира се, когато напускате дома си, вие жертвате част от неприкосновеността на личния си живот. Някой може да ви види да влизате в клиниката на Маркет Стрийт или да забележи, че

вие и секретарката ви напускате “Хилтън” заедно. Още повече, че в света отпреди десет години, цялата тази информация можеше да бъде получена от хора, които не ви харесват или не ви вярват. Но получаването на тази информация беше скъпо. Вашите врагове можеха да наемат лице, който да ви следи, но трябваше да му плащат. Освен това беше трудно да се запази наблюдението в тайна – беше много вероятно да забележите опашката си да се мотае след вас по алеята.
В днешния и утрешния свят тази информация е тихо събирана отустройства и приложения, достъпни за анализ от много лица и организации, които могат да я предадат, купят или да я изискат по законов ред. А могат и да платят на хакер да открадне архив с данни за местоположението на всеки. Тази нова реалност, при която информацията за вашето местоположение се събира *всепроникващо, тихо и евтино* ни кара да се тревожим.

Заплахи и възможности

Някои заплахи за тайната на местоположението са явни: доказано е как с камери, поддържащи софтуер за разпознаване на лица, може да бъде злоупотребено, за да се проследят хора и да се запишат действията им. В този документ, ние изразяваме загриженост относно заплахите за тайна на местоположението, които възникват като вреден скрит страничен ефект в резултат на *определено полезните* услуги, базирани на местоположение. Не можем да спрем изобилието от нови цифрови услуги, базирани на местоположение. Нито бихме искали – ползите, които те предлагат са впечатляващи. Това, което спешно се нуждае от промяна, е че сигурността трябва да е заложена в тези системи, като част от първоначалното им проектиране. Не можем да позволим да имаме всепроникваща технология за наблюдение, вградена в обществената електронна инфраструктура по случайност. Сега ние имаме възможността да се уверим, че тези опасности са преодолени.

Имаме предвид, че най-лесното и най-добро решение на проблема с тайната на местоположението е да се конструират системи, които *на първо място не събират данни.*Това изискване звучи невъзможно (как да ви кажем, че вашите приятели са наблизо без да знаем къде се намирате вие и къде се намират приятелите ви?), но всъщност, както обсъждаме по-долу, това е разумна цел, която може да бъде постигната с модерни криптографски техники.

Модерната криптография всъщност позволява обществени системи за обработка на данни да бъдат проектирани с цял спектър от мерки за поверителност, с диапазон от пълна анонимност до ограничена анонимност, която да подпомага прилагането на закона. Необходимо ни е да се уверим, че системите не се конструират с нулева защита на данните и всичко се записано просто, защото това е пътят на най-малкото съпротивление.ю

Услуги, базирани на местоположението, които не знаят къде сте

Модерната криптография предлага някои наистина умни начини за разполагане на автомати за пътни такси, билети за пътуване, GPS и всички други мобилни услуги, които искате, без да се регистрира мястото, на което сте. Наистина важно е политиците и проектантите на системи за определяне на местоположението да знаят за това. Тази секция съдържа само няколко примера за видове системи, които са осъществими.

Автоматично таксуване и изпълнение на стоп сигнал

В много урбанизирани зони шофьорите са насърчавани да използват малки електронни предаватели (комуникационни сателитни канали) (FastTrak, EZpass в САЩ), за да заплащат пътните такси на мостове и тунели. Нуждата да се регулира трафика и да се избегнат задръствания ни кара да очакваме да видим нарастване на такива устройства и методи за таксуване.

За прости такси (например пътна такса “мост”), протоколи, които криптографите наричат *електронни пари* са превъзходно решение. В криптографски смисъл електронните пари се отнасят до начините, по които едно лице може да плаща нещо, използвайки цифров подпис, които е анонимен, но гарантира, че получателят може да откупи продукта за пари. Електронните, действат точно като истинските пари! Вижте тази статия за детайли на модерно изпълнение. По този начин шофьорът “Вера” би купувала пачка електронни пари на всеки няколко месеца и била зареждала своя предавател. Когато Вера кара през мостове и тунели, таксуващият предавател анонимно ще плаща таксите й. За по-сложни таксуващи системи (при които цената зависи от конкретно изминатия път), могат да се използват някои по-активни въведения (обсъдени детайлно в тази техническа статия).
Внедрените системи за определяне на такса при задръствания са с ниска чувствителност относно поверителността, те просто записват шофьорите и използват записаната информация, за да генерират такси. Например вие може да имате информация за всички автомобили, използвайки малко радио устройство, което да докладва местоположението им през цялото време. Докато Вера кара през натоварен платен район (например по улица в центъра на Лондон), устройството казва: “Здравей, аз съм колата на Вера.” То регистрира всяко място, на което Вера е била. Еквивалентно на това, някой може да сложи камери навсякъде, които да запишат регистрационния номер на Вера докато тя кара и да запазят записи отвсякъде, където тя е ходила, за да изчислят по-късно таксите. И двете решения нарушават тайната на местоположението на Вера.
По-малко очевиден, но много по-добър начин да избегнете таксуващи автомати такси е устройството на Вера да се обвърже със секретен лист от “динамични регистрационни номера” – дълъг списък от произволно изглеждащи криптографски номера. Това обвързване приема формата на цифрова сигнатура, давана на таксуващите апарати. Докато Вера кара през регион, който се таксува, нейният апарат циркулира през тези числа бързо, изпращайки текущото число към мониторинговите устройства, през които тя преминава. Никое от тези числа в действителност не идентифицира Вера и докато те продължават да се сменят няма начин да ги навържете заедно, за да я проследите. Но на края на месеца Вера трябва да плати своите пътни такси като свърже устройството на колата с компютъра си. Компютърът извършва криптографски процес, наречен “защитена многопластова комуникация”. На края, нейният компютър показва, че тя дължи 17 долара пътни такси за този месец, без да показва как е натрупала тази сметка. Обвързващото разменяне в началото уверява, че Вера не може да мами: тя не може да получи по-малка обща сметка, ако действително е карала през мост с активирано устройство.
Този подход може да бъде прилаган към различни автоматизирани транспортни нужди. Например всеки път, когато Вера преминава през светофар, мониторингово устройство може да запише текущия “динамичен регистрационен номер”. Въпреки че, отново, събраната информация може да бъде използвана, за да следи Вера. Ако тя премине на червен светофар, системата може да засече това и да й издаде билет.

Локализация, базирана на местоположение

Локализация на базата на мобилно устройство е друг важен пример. Определянето на местоположението на телефоните вече е възможно на основата на силата на сигнала или видимостта на близките безжични мрежи или GPS данни. Естествено компаниите също се надпреварват да осигурят търсещи устройства, които използват тази информация, за да предоставят на хората различни резултати от търсенето в зависимост от това къде се намират те във всеки един момент. Простичък начин да се осъществи търсене на местоположение чрез мобилния е устройството да каже: “Тук е нокиата на Франк. Виждам следните пет WiFi мрежи със следните пет сили на сигнала”. Услугата отговаря “добре, това означава, че вие сте на ъгъла на 5та и Мейн в Спрингфийлд”. Тогава вашето устройство пита: “Какви сандвичи има наблизо? Разхождат ли се наоколо приятели на Франк?”. Този вид търсене записва всяко

място, на което отидете и всичко, което сте търсил там. По-добър начин да извършите търсене на базата на местоположение е нещо такова:”Здравейте, аз съм мобилно устройство. Ето криптирано доказателство, че имам акаунт за вашата услуга и не съм спамър. Виждам следните пет безжични мрежи”. Услугата отговаря: “добре, това означава, че вие сте на ъгъла на 5та и Мейн в Спрингфийлд. Ето голям списък с некриптирана информация за нещата, които са наблизо.” Ако някоя от тези некриптирани информации е бележка от приятел на Франк, който казва:”Здрасти, аз съм тук”, тогава неговата Нокиа ще може да я прочете. При желание, той може също да каже:”хей, имам некриптирана бележка за постване за други хора, които са наблизо.” Ако някои от тях са негови приятели, ще могат да я прочетат. (Добра подробна дискусия за подобни подходи чрез многостранна комуникация са представени на тази страница).

Транзитни преминавания и карти за достъп.

Друга широка област на приложение е има при пропуски и устройства, позволяващи достъп до защитени територии. Например пропуски, които позволяват достъп до заключващи се помещения за колела близо до гарите или месечни карти за автобуса. Просто изпълнение може да накара карта, използваща RFID (радио честотна идентификация), да докладва, че Боб е оставил колелото си във или извън благоприятната зона (и да намали или увеличи сметката му в съответствие с това) или равнозначно, Боб се качва в автобуса (и проверката се уверява, че Боб е платил за своята карта). Този тип схеми могат да изложат Боб на риск. По-добър подход би включил използването на неотдавнашни изследвания върху *анонимни удостоверения.* Те дават на Боб специален набор от цифрови сигнатури, с които той може да докаже, че наистина е влизал в помещението за заключване на колелета (т.е. доказва, че е платежоспособен клиент) или се е качил в автобуса. Но протоколите взаимодействат помежду си така, че не могат да бъдат свързани с него лично, нещо повече повторящите се влизания не могат да бъдат свързани едни с други. Това е – автоматът за заключване на велосипеди знае, че някой е оторизиран да влезе, но не може да кажи кой е той и не може да каже кога за последно е минал човекът. Комбинирани с *електронните пари,* пропуските дават възможност за широк диапазон от решения, запазващи тайната на местоположението.

Защита на интереси и анонимизирани бази данни

Длъжни сме да отбележим, че дори съществуването на бази данни за местоположението, лишени от идентификационни признаци, могат да пропуснат информация.

Например ако знаем, че Вера е единственият човек, който живее на Дед Ед Лейн, фактът, че някой е използвал услуга базирана на местоположението, на Дед Ед Лейн може основателно да бъде свързан с Вера. Този проблем също така е широко известен (и изучаван) в контекста на епидемиологичните данни:оказва се относително лесно да се открие идентичността на жертви на заболяване от “анонимизирана” географска информация за местоположението на случаите. Общо казано, едно от решенията на проблема е да се ограничи използването на услуги, основаващи се на местоположението до райони с висока плътност на населението. Съществуват и по-сложни криптографски решения, които също са възможни. Вижте тази статия, в която се дискутират (и предлагат решения) на този проблем в контекста на събирането на обобщена статистика на трафика и тази статия за обсъждане на “диференцирана поверителност”, формализация на идеалните гаранции за поверителност в лицето на съществуването на бази данни.

За повече информация

Безопасното и правилно прилагане на такива модерни криптографски протоколи може да бъде истинско техническо предизвикателство. Ефикасното им приложение изисква много

работа, но може да бъде направено – това е точно типът криптографски софтуер, които защитава сигурността на финансовите мрежи (например банкомати), дава ни сигурност да пазаруваме онлайн и кодира телефонните ни разговори. Големите софтуерни предприемачи (например IBM и Siemens) поддържат големи криптографски екипи.

Дали сме връзки към някои от източниците, които биха били полезни на конструкторите, искащи да разберат как работят тези протоколи. Ако вие сте висш чиновник или конструктор и имате въпроси относно начина на работа на тези методи, не се колебайте да се свържете с нас: ние можем да ви насочим към подходящата литература и да ви свържем с експерти, които да отговорят на въпросите ви.

Защо трябва фирмите от частния сектор да поставят като приоритет тайната на местоположението?

Вярваме че правителствата имат обществена отговорност към своите граждани и гарантират, че разположената от тях инфраструктура защитава тайната на местоположението. Но съществуват и финансови причини, поради които частният сектор да отдели време, за да проектира поверителността на системите за местоположение, които са изградени.

Избягвайте скъпо струващи юридически разходи

Ако една корпорация запазва файлове, проследяващи нечие местоположение, тя може да бъде обект на съдебни искания за тази информация. Такива искания могат да дойдат под различни форми (включително неформални въпроси, призовки или заповеди) и от различни страни (наказателен или граждански процес). Съществуват комплекс от правни въпроси като дали изпълнението на конкретна молба е правно необходимо, възможно или дори забранено и какъв евентуален риск поражда.

Тази правна сложност може дори да включва международен закон. Например американски корпорации, които имат дейност и в ЕС, могат да бъдат обект на Европейския закон за защита на данните, когато граждани на ЕС посетят Съединените щати и използват услугите на американски компании.

Корпорациите с големи масиви от данни за местоположението се сблъскват с риска, че адвокатите и правоприлагащите органи ще узнаят, че информацията съществува и ще започнат да използват правни начини, за да я получат. Най-добрият начин да избегнат този скъпо струващ е да избягват да имат идентифициращи данни за местоположението на първо място.

Получаване на конкурентно предимство

Хората бавно започват да осъзнават потенциалните негативи на това да има постоянно запис на местоположението им. Възможността да се предложи надеждна защита на личните данни все повече дава на фирмите конкурентно предимство – особено, ако те могат да убедят индивидуалните потребители или правителствени клиенти, че продуктът им предлага по-стабилна и надеждна защита на поверителността.

Няма ли по-лесна/различна алтернатива?

Използването на криптография и внимателното планиране на защитата на тайната на местоположението още от самото начало изисква техническо усилие. Затова е важно да попитаме дали няма други адекватни начини да запазим поверителността в тези системи. За съжаление, ние вярваме, че алтернативите са ненадеждни или по-трудни за изпълнение и прилагане.

Съхраняване и изтриване на данни.

Един вид защита, на който можете да се надявате е, че записите на местоположението ви ще бъдат изтрити преди вашите неприятели да ги вземат. Ако компанията, която ви предоставя локализиране чрез вашия клетъчен телефон, не е необходимо да пази вашите архиви една седмица по-късно, може би може да бъдат убедени да ги забравят бързо. Може би са обещали, че ще го направят.

За съжаление, няма база за много оптимизъм на фронта на съхраняването на информация. Компаниите, предлагащи търсене, имат стимули да пазят пространни записи на въпросите на потребителите си, така че да могат да научат как да подобряват резултатите от тях (и да продават по-ефективни реклами). Паметта за съхраняване е евтина и става все по-евтина. Таксуващите агенции имат стимул да пазят обширни записи от потребителските такси за уреждане на жалби и предоставяне на обобщена статистика и счетоводна информация.

Дори ако събиращият екип обещае да изтрие информацията след определено време, няма гаранция, че в действителност ще го направи правилно. Първо, необходими са инструменти за сигурно изтриване, за да е сигурно, че изтритата информация наистина не съществува; много системни администратори биха се провалили в правилното им използване. Второ, политиката на поверителност на компанията може внезапно да се промени от изтриване към съхранение. За да станат нещата още по-лоши, няма гаранция, че правителството няма внезапно да наруши законното изискване подобни компании и правителствени агенции да пазят всички свои записи с години, само в случай, че записите са необходими за целите на "националната сигурност". Тази последна загриженост не е само празна параноя: това вече се случи в Европа и администрацията на Буш си игра със същата идея.

Колкото до правителствените агенции, досегашният опит със съхраняване на данни не е обнадеждаващ. Интересен пример за това е предоставен от автоматични таксови данни (записи от FastTrak и EZpass). Различните щати дават различни обещания за това колко дълго ще пазят информацията и има различни степени на ефективност при спазването на тези обещания. Информацията често остава достъпна за много години. Правните санкции за нарушаване на тези обещания в момента са минимални.

Ограниченото съхраняване на информация е важна защита за поверителността, но не може да замени най-добрата защита: на първо място – не записвайте информация!

Избягване на нежелана информация за продукти и услуги

Понякога хората отговарят на подобен род притеснения с твърдението, че свободният пазар ще реши този проблем. "Хора, които са загрижени за поверителността на личните си данни не ползват подобни услуги." – казват те. "Ако хората наистина се интересуват, ще се появят компании, предлагащи поверителност като специална услуга."

Ние не смятаме това за приемлива гледна точка – има твърде много насилие в играта. Често няма адекватна замяна на въпросната услуга и е или скоро ще бъде ужасно трудно да се избягва използването ѝ. Да предположим, че част от съединените щати приемат задължителна "плати докато караш" застраховка или такса "задръствания", които са базирани на записване на местоположението. В повечето части на съединените щати не е реалистично да се предполага, че хора, които се тревожат за поверителността на личните си данни не трябва да шофират (или не трябва да шофират до избраната от тях религиозна институция). И в този случай на услуги, базирани на определяне на местоположението е ясно, че всичко е нагласено срещу хора, избиращи да вземат неудобни мерки, за да защитят себе си: твърде трудно е да знаете какво е било записано от кого и каква възможност имате да избегнете записването и е твърде трудно да продължите да проучвате тези въпроси докато взаимодействате с новите творения на техниката. В такава обстановка, хората просто нямат потенциал да се приспособят към загубата на *основателното очакване* за поверителност на

публични места. Нашите чувства не са в крак с напредъка на технологиите.

Мобилните телефони и кредитните картиоставят следи

Мобилните телефони осигуряват информация на телекомите за местоположението на потребителя, когато са включени, а използването на банкова карта оставя информация и за мястото, където е използвана. Зависимостта на тези технологии от информация за местоположението, не е причина да се изостави искането за гарантиране тайна на местоположението, а по-скоро причина да се борим за по-добри практики или закони за технологията за клетъчни телефони и транзакциите с кредитни карти. Проблемите, които имаме сега с кражбата на идентичност дават яснота колко проблеми може да предизвика обработката на лични данни.

Гражданите, спазващи закона, не се нуждаят от поверителност.

Друг често срещан отговор на тревогите за тайната на местоположението е, че гражданите, които спазват закона, не се нуждаят от поверителност. “Не прелюбодействам, не нарушавам закона” – казват хората (и подразбиращо се “Не съм в прикрит гей, не принадлежа към никоя малцинствена религизона или политическа група”). Един отговор на това е напомнянето, че има много по-важни причини за необходимостта от поверителност.Тези, от които трябва да се предпазвате не са само правителството, правоохранителите или политическите врагове.

- Не е необходимо работодателят ви да знае дали, кога и къде ходите на църква.
- Не е нужно съдружниците ви да знаят колко закъснявате за работа и къде пазарувате.
- Бившият приятел на сестра ви няма нужда да знае колко често тя прекарва нощите в апартамента на новото си гадже.
- Корпоративните ви конкуренти не трябва да знаят с кого говорят вашите продавачи.

Спазването на тайната на местоположението е важно за поддържане на достойнството и спокойствието ви докато се движите по света. Тайната на местоположението е също и за това да знаете кога други хора знаят неща за вас и да имате възможността да кажете кога те взимат решения въз основа на тези факти.

Да предположим, че застрахователна компания успее да получи запис от движенията на Алис през изминалата година и реши, че има факти в тези записи, които са предпоставка за увеличаване на вноските или отказване на застраховка. Проблемът с това решение не е само, че е несправедливо, но и че Алис може да няма възможността да го оспори. Ако застрахователната компания има политика на дезинформиране, ще има ли Алис практически начин да знае това и да го оспори? Аргументът “нямам нищо за криене” насочен срещу политиката на поверителност е разгледан по-подорбно в тази статия.

Заключение

В крайна сметка, решението за това кога ще запазим нашата тайна на местоположението (и ограничените обстоятелства, при които ще се откажем от нея) би трябвало да бъде определено с демократични действия и изготвяне на закони. Сега е ключов момент за организациите да изградят и разположат информационната инфраструктура за местоположение, да покажат лидерство и да изберат проекти, които са отговорни и не предават данните за местоположението на потребителите просто по целесъобразност.