CIBER ESPIONAXE

Internet é un medio de comunicación que cambiou o mundo. Xa coñeces as súas vantaxes, le e descubrirás algúns dos seus riscos. Aprende a facer un uso intelixente para preservar a túa privacidade

QUE CONTA A OUTROS O TEU MÓBIL DE TI CANDO TE SACA A PASEAR.

Cada mañá, levando o móbil no peto, estás a lle facer un choio á túa compañía telefónica: "queres facer e recibir chamadas móbiles; en troco, permites que esa empresa poida saber onde estás en todo momento". Este choio non está especificado en ningún contrato, pero é así como funciona. Os teléfonos móbiles son un gran invento pero non poden funcionar a menos que as empresas de telefonía móbil saiban onde estás, e isto implica que esteas sempre baixo a súa vixilancia.

Esta é unha forma moi íntima de vixilancia. Saben grazas ao teu teléfono móbil onde vives e onde traballas. Saben onde desexas pasar as fins de semana, onde te divirtes pola noite. Controlan a frecuencia coa que vas á igrexa (e cal igrexa e tipo de fe), canto tempo pasas nun bar, e se se superas o límite de velocidade cando conduces. Saben -porque teñen control sobre todos os outros teléfonos na túa área- con quen andas, con quen xantas, e con quen dormes. Os datos acumulados probablemente poden crear unha imaxe de como pasas o tempo mellor do que ti o farías, porque o sistema non ten que confiar na memoria humana. En 2012, uns investigadores foron capaces de usar estes datos para prever onde estarían as persoas 24 horas despois, e nunha área de menos de 20 metros.

Antes da existencia dos teléfonos móbiles, se alguén quería saber todo iso, tiña que contratar un investigador privado para seguilo a todas partes tomando notas. Agora ese traballo está obsoleto; o teléfono móbil no teu peto fai todo isto automaticamente. Pode ser que ninguén teña interese nesta información, pero está aí para quen a queira recoller.

Esta información de localización é valiosa, e todo o mundo quere ter acceso a ela. A policía quere. A análise de localización a través do teléfono móbil é útil en investigacións criminais en varias formas diferentes. A policía pode "establecer conexión" cun teléfono específico para determinar onde está, usar datos históricos para determinar onde foi, e recoller todos os datos de localización de teléfono móbil dunha área específica para descubrir quen estaba alí, preto dese teléfono, e cando. Máis e máis, a policía está a usar estes datos para exactamente estes fins.

Os gobernos tamén usan estes mesmos datos para a intimidación e control social. En 2014, o goberno da Ucraína enviou esta mensaxe de texto positivamente orwelliana a cidadáns en Kiev cuxos teléfonos estaban nun determinado lugar durante un determinado período de tempo: "Estimado subscritor, foi rexistrado como participante nun disturbio multitudinario" Non creo que este comportamento estea limitado a países totalitarios; en 2010, a policía de Michigan buscou información sobre

cada teléfono móbil en servizo preto dunha manifestación laboral. Non se molestaron en pedir unha orde xudicial.

Hai toda unha industria dedicada a seguirte. As empresas usan o teléfono para rexistrar as túas tendas favoritas, que son loxicamente as que máis visitas, coa intención de que cando andes ou conduzas preto de calquera delas enviarche publicidade ao teu teléfono.

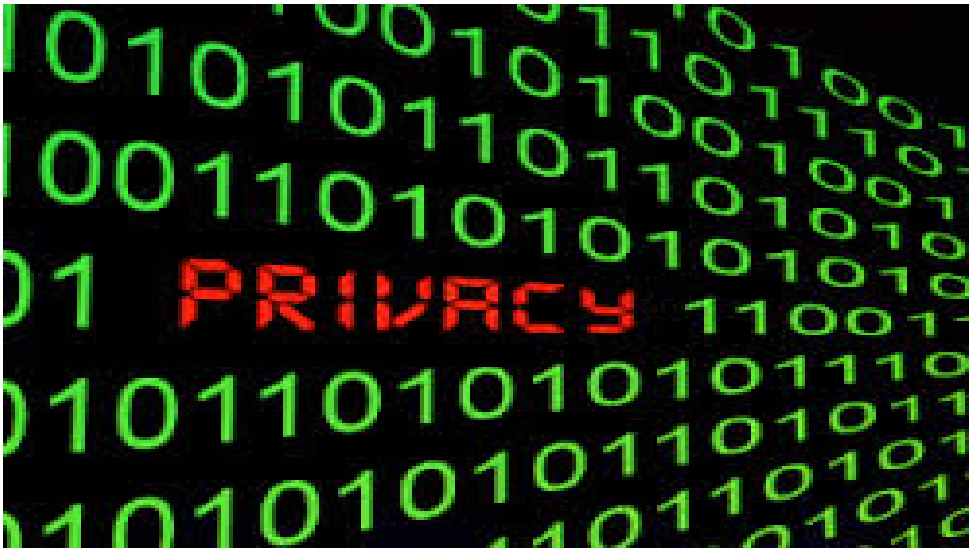
Os teus datos de localización son tan valiosos que empresas de telefonía móbil xa están a vendérllelos a brokers de base de datos, quen á súa vez os revenden a calquera disposto a pagar. Empresas como a Sense Networks está especializada en usar estes datos para crear perfís persoais de cada un de nós.

As compañías telefónicas non son as únicas distribuidoras de datos do teu teléfono móbil. A empresa norteamericana *Verint* vende sistemas de seguimento de teléfono móbil para empresas e gobernos de todo o mundo. O sitio web da empresa di que é "líder global en solucións de intelixencia para a optimización da implicación do cliente, intelixencia en seguridade, fraude, risco e conformidade", con clientes en "máis de 10.000 organizacións e en máis de 180 países." No Reino Unido a empresa *Cobham* vende un sistema que permite que alguén envíe unha chamada "cega" (non soa, non é detectábel). A chamada cega forza ao outro teléfono a transmitir nunha determinada frecuencia, permitindo que este teléfono sexa localizado coa precisión dun metro. A empresa ten clientes en gobernos de Alxeria, Brunei, Gana, Paquistán, Arabia Saudita, Singapur e Estados Unidos. *Defentek*, unha empresa misteriosamente rexistrada en Panamá, vende un sistema que pode "localizar e rastrexar calquera número de teléfono no mundo ...

Tobias Engel demostrou nunha conferencia de hackers en 2008 que os criminais están a facer hoxe o mesmo.

Todo este seguimento de localización non está baseado só na teléfonía móbil. Hai outro sistema de localización totalmente distinto e máis preciso dentro do teu smartphone: o GPS. Algunhas aplicacións usan os datos de localización a cambio de che prestar un servizo: Google Maps, Über, Yelp. Outros, como Angry Birds, só queren recollelos para vendelos.

Se queres, tamén ti podes facelo. HelloSpy é unha aplicación que podes instalar no smartphone doutra persoa para saber onde está, sen o seu consentimento. Perfecto para unha nai ansiosa que quere controlar a filla adolescente ou un home abusador que quere espiar a súa esposa ou moza. Os empresarios teñen usado aplicacións como esta para espiar os seus empregados.



TAMÉN, SE QUEREN, PODEN ACCEDER AO NOSO COMPUTADOR

Non só os móbiles son fornecedores de información persoal e íntima, tamén poden facelo os computadores: a través deles alguén pode saber que les, escribes, ves e escoitas en internet.

O negocio está en permitir que varias empresas nos vixíen a cambio de darnos un servizo gratuíto. O Presidente de Google Eric Schmidt e o seu director de ideas Jared Cohen escribiron no seu libro: 2013, A Nova Era Dixital: "se nos deixas ter os teus datos, imos amosarche anuncios que queres ver e imos xogar gratis na web; terás correo electrónico, e todo tipo doutros servizos". Como somos animais sociais non hai nada máis gratificante que poder comunicarnos con outras persoas. Os medios dixitais son a forma máis fácil e rápida de comunicarnos. E por que permitimos o acceso aos gobernos? Porque temos medo dos terroristas, tememos que os estranxeiros secuestren os nosos fillos, tememos os traficantes de drogas, temos medo ao delicuente máis buscado do momento. Esa é a xustificación do NSA para activar os seus programas de vixilancia total; se nos deixas ter os teus datos, aliviaremos o teu medo.

O certo é que hoxe, a tecnoloxía dá aos gobernos e ás corporacións capacidades absolutas para a vixilancia masiva. A vixilancia masiva é perigosa. Permite a discriminación entre as persoas pola raza, relixión, clase ou crenzas políticas. Controlan o que vemos, o que facemos, e, en definitiva, o que dicimos, sen ofrecer aos cidadáns o recurso ou calquera capacidade real de evitalo. Fainos menos seguros. Fainos menos libres

COMO CAPTAN A INFORMACIÓN QUE QUEREN DE NÓS

O teu procesador de texto mantén un rexistro do que escribes. Cando fas clic en "salvar" o teu procesador de texto rexistra a nova versión, pero o computador non elimina as versións antigas ata que necesita espazo no disco duro para outra cousa. O teu procesador de texto salva automaticamente o teu documento de cando en vez; Microsoft Word salva o meu cada 20 minutos. Word tamén mantén un rexistro de quen creou o documento, e moitas veces de quen máis traballou nel.

Ao Conectáreste á Internet o computador leva un rexistro dos sitios que visitas, os anuncios en que fas clic, as palabras que escribes. O teu navegador envía datos para sitios sobre o software que tes, cando se instalou, que recursos están habilitados, etc. En moitos casos, estes datos son suficientes para identificar o teu computador.

ESTE PODERÍAS SER TI, PODERÍA SER EU, PODERÍA SER CALQUERA DE NÓS

Para comprender o que significa toda esta acumulación de datos para a nosa privacidade, considera o caso do estudante de dereito austríaco Max Schrems. En 2011, Schrems esixiu que Facebook lle entregase todos os datos que a empresa tiña sobre el. A Unión Europea (UE) ten unha lei que o permite. Dous anos máis tarde, despois dunha batalla xudicial, Facebook enviolle un CD con 1.200 páxinas en PDF. Estaban non só os amigos e contactos en Facebook senón tamén os seus comentarios e todas as fotos e páxinas en que fixo clic. Facebook non usa todos estes datos, pero no canto de separar o que lle interesa e o que non, a empresa considera que é máis fácil ou barato simplemente gardar todo.

GOOGLE SABE O QUE PENSAS

Google sabe qué tipo de pornografía buscas; en que antigas noivas e amantes estás aínda a pensar; aquilo que non nos gusta de nós e procuramos evitar; as nosas preocupacións e os nosos segredos. Se o Google quixer, podería descubrir quen de nós está preocupado pola súa saúde mental, quen busca información sobre a evasión fiscal, ou planea protestar contra unha política de goberno.

É posíbel dicir que Google sabe máis sobre o que eu estou pensando ca a miña muller.

Unha experiencia interesante é probar a escritura automática durante unha busca calquera en Google. Escribes e o motor de Google acabar de escribir as túas consultas de investigación en tempo real, con base ao que outras persoas inseriron. Cando eu escriba "debo contar á miña m...", Google suxeriu "debo contar á miña muller que teño un lío" Un Alto executivo de Google Eric Schmidt admitiu que: "Sabemos onde estás. Sabemos onde estiveches. Podemos máis ou menos saber o que estás a pensar.

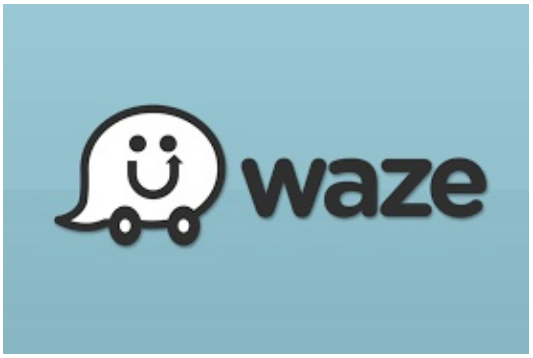
OUTROS USOS PARA AS **GOOGLE-GLASS**

O FBI ten unha base de datos con máis de 52 millóns de rostros, e un software de recoñecemento facial moi bo. A policía de Dubai están integrando o software de recoñecemento facial personalizado con Google-glass para identificar automaticamente sospeitosos. Con suficientes cámaras nunha cidade, os policías serán capaces de seguir os coches e as persoas en todo momento, sen saíren dos seus despachos.

Xa non é aquilo de "siga ese coche"; agora é "siga a todos os coches." A policía podería estar virtualmente detrás dun sospeitoso, pero cunha rede urbana de cámaras, escáneres e software de recoñecemento facial, poden vixiarnos a todos, sospeitosos ou non.

En 2008, a empresa Waze (adquirida por Google en 2013) introduciu un novo sistema de navegación para smartphones. A idea era que a empresa podería, grazas ao seguimento que esta fai dos condutores usuarios do programa, inferir datos de circulación en tempo real coa finalidade de facilitar información sobre estradas alternativas para evitar os atascos. Todos queremos evitar atascos. En realidade, toda a sociedade, e non só os clientes de Waze, nos beneficiamos cando procuramos non provocar atascos. O problema é que non somos conscientes da cantidade de datos privados que estamos dando.

Por primeira vez na historia, os gobernos e as empresas teñen a capacidade de realizar unha vixilancia masiva sobre toda a poboación. Poden facelo co noso uso de Internet, as nosas comunicacións, as nosas transaccións financeiras, os nosos movementos ... todo. Mesmo os alemáns orientais non podían seguir a todo o mundo todo o tempo. Agora é doado.



SON AS VIDEO-CÁMARAS PARA NOS ESPREITAREN OU PARA A NOSA SEGURIDADE?

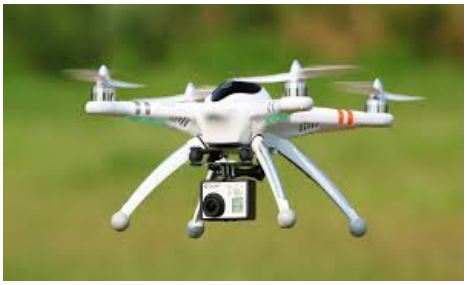
Podemos estar seguros de que estes poderosos instrumentos de vixianza non son usados para rexistrar as nosas vidas privadas?

Nalgunhas cidades hai video-cámaras que capturan a nosa imaxe centos de veces ao longo dun día. Algunhas son doadas de ver mais outras non, porque somos incapaces de ver se hai unha cámara CCTV incrustrada no teito dunha habitación ou dentro dun caixeiro automático ou colgada dun edificio a unha mazá de distancia. Os Drones, que poden portar unha cámara, son cada vez máis pequenos e difíciles de ver. Xa os hai do tamaño dun insecto e axiña dun lixo.

Se engadimos a toda esta infraestrutura de gravación un software de identificación temos un sistema de vixilancia automático e omnipresente. O recoñecemento facial é o xeito máis doado para identificar a unha persoa cunha cámara e a tecnoloxía necesaria é cada día máis accesíble e precisa. En 2014 os algoritmos de recoñecemento facial que utiliza unha máquina xa son máis eficaces ca as persoas. Ademais xa hai outras tecnoloxías de recoñecemento e identificación dun individuo en desenvolvemento:

escaneadores de iris que funcionan a distancia, sistemas de recoñecemento do andar, etc.

E isto non é todo aínda hai máis sistemas de vixilancia ocultos á vista nas rúas das cidades. Os móbiles constan de chips que emiten sinais de radio frecuencia e poden ser utilizados para localizar xente. Son moitos os negocios de venda que rexistran os movementos da xente a través da MAC e das ID dos Bluetooth dos seus teléfonos



os usos positivos dos drones son moitos: contra incendios, busca de desaparecidos...

móbiles. O obxectivo é saber os lugares dun supermercado ou centro comercial polos que máis transitan os clientes, en que lugares se paran a curiosear, etc.

En 2014 un executivo da *Ford Motor Company* dixo en público durante un Evento de Novidades Electrónicas: "Sabemos quen incumpre a lei e cando. Temos un GPS no voso coche así que sabemos que é o que estades a facer". Isto provocou un impacto e sorpresa porque até entón ninguén sabía que Ford mantiña os propietarios dos seus coches baixo constante vixilancia. A empresa deuse présa en desdicirse mais o comentario deixou sospeitas de que Ford podía estar facéndoo en verdade. Sabemos por un informe dunha Oficina do Goberno USA que tanto as empresas de coches coma as empresas de navegación gps almacenan moita información dos seus usuarios.

Os radares dentro da escala dos terahércios pode detectar se unha persoa leva un arma oculta e obxectos inseridos dentro de cemento a unha profundidade de oito pulgadas. As cámaras poden "escoitar" unha conversa telefónica enfocando obxectos próximos como unha bolsa de patatillas ao medir a vibración. O NSA ou probabelmente outras axencias poden activar remotamente o micro do teu teléfono e escoitar todo o que pasa ao seu arredor.

Xa hai sistemas de recoñecemento do olor corporal en desenvolvemento. Hai unha empresa en internet a traballar para identificar a calquera persoa polo xeito de escribir no teclado do seu computador.

NOTA DOS AUTORES:

Este monográfico está escrito con, sobre todo, fragmentos escollidos do libro:

Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World, escrito por Bruce Schneier, editorial: W. W. Norton & Company

ANALIZANDO OS NOSOS DATOS

E non só para souberen que é o que nos gustaría mercar

En 2012 o *New York Times* publicou unha historia sobre como as corporacións procesan na rede os nosos datos para proporcionarnos, segundo elas, proveitosas vantaxes. O artigo desvelou que ***Target Corporation*** podía precisar grazas ás buscas ou compras dunha muller se ela estaba embarazada e que podía utilizar esa información para lle enviar anuncios ou cupóns de desconto para a compra de artigos relacionados coa maternidade. A historia inclúe a anécdota dun pai de Mineapolis que se queixou ante unha Tenda Target polo envío que esta fixo de cupóns para bebés á súa filla adolescente. A verdade é que Target soubo antes ca el que a súa filla estaba embarazada.

Os fabricantes de coches almacenan datos dos nosos coches para mellorar o seu rendemento; os concellos almacenan datos para mellorar as condicións de circulación polas cidades. O noso xenoma é explorado e almacenado para a investigación médica. Empresas como Facebook ou Twitter almacenan datos para enviarnos anuncios e autorizaron a investigadores das universidades a empregar eses datos para investigar aspectos da nosa vida social.
Se tes a lista de contactos de alguén, a quen escribe ou chama, podes deducir quen son os seus amigos. Se tes a relación de webs que visita ou unha lista de libros que acaba de comprar podes inferir os seus intereses.

Outras posíbeis deducións son máis sutís. A lista da compra de alimentos de alguén pode ser moi útil para supoñer a que grupo étnico pertence. A súa idade, xénero ou relixión. Ou o seu historial médico ou se bebe alcohol ou non. Os vendedores están constantemente á procura de patróns que indiquen que alguén está a piques de facer unha gasto importante, como casar, ir de vacacións, mercar unha casa, ter un fillo, etc. A policía en varios países usa estes patróns como evidencias ante un tribunal. Facebook pode predicir a raza, personalidade, orientación sexual, ideoloxía política, uso de drogas polos clicks que fagamos en "gústame". A empresa sabe que estás comprometido ou es homosexual antes incluso de que o anuncies publicamente e ademais as mensaxes que Facebook insire no teu perfil pode facer que outras persoas o saiban sen ti sabelo ou permitilo. Isto é algo que dependendo do país onde vivas pode ser un asunto simplemente embarazoso ou pode ser te maten.

Ao longo da Historia os gobernos veñen recollendo todo tipo

Seguir alguén de incógnito, a pé ou en coche, custa uns 175,000 dólares por mes, sobre todo o salario dos axentes que fan o seguimento. Pero se a policía pode pór un rastreador no coche do sospeitoso, ou usar un dispositivo para enganar o teléfono móbil do sospeitoso e que aporte a súa información de localización, o custo cae a preto de 70.000$ por mes, pois require só un axente. E se a policía pode ocultar un receptor GPS no coche do sospeitoso, de súpeto, o prezo cae a preto de 150$ que é o que custa a instalación clandestina do dispositivo. Obtendo a información de localización do proveedor de móbil do sospeitoso é aínda máis barato.

Se estás lendo este libro nun Kindle, Amazon sabe cando o empezaches a ler e o rápido que o les. A empresa sabe se estás lendo con dedicación, ou se les só algunhas páxinas cada día. Sabe se saltas para o final, se reles unha sección ou se desistes e non rematas o libro. Se subliñas ou comentas algún fragmento Amazon tamén o sabe. Non hai nada no noso Kindle que nos avise de que está enviando datos a Amazon sobre os nosos hábitos de lectura. Isto acontece, silenciosa e constantemente.

de información. Na era ***McCarthy***, por exemplo, o goberno tiña en conta a militancia política, a subscrición a revistas, testemuñas de amigos, familia e colegas. A diferenza é que agora a capacidade de recoller e almacenar información é moito máis completa e barata e a tecnoloxía necesaria para a súa análise é moito máis sofisticada.
Velaquí 4 exemplos de como a Axencia Nacional de Intelixencia (NSA) utiliza a información recollida dos móbiles:

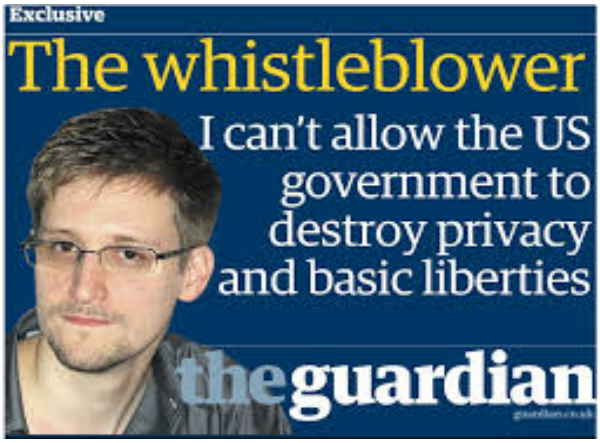
1. A NSA usa a tecnoloxía de localización dos móbiles para seguir a aquela xente cuxos movementos se cruzan. Por exemplo, se a NSA está interesada en vixiar a Alice e Bob está no mesmo restaurante ca ela un día e unha semana máis tarde volven a coincidir tomando noutro lugar un café e un mes máis tarde os dous están no mesmo aeroporto o sistema dá aviso de alarma. Podemos deducir que Alice e Bob son socios potenciais incluso sen que houbese entre eles ningunha comunicación electrónica.

2. A NSA fai un seguimento polo mundo dos seus espías monitorizando os seus móbiles. Se hai algún outro móbil próximo pode deducir que ese espía está sendo controlado por unha organización ou goberno inimigo.

3. A NSA ten un programa informático que detecta mediante a metadata dos móbiles cales só se acenden para falar uns segundos e son desconectados para non ser usados nunca máis. Con esta técnica localiza a aquelas persoas que buscan non ser detectadas.

4. A NSA tamén almacena información da xente que apaga o teléfono e durante canto tempo. Mantén un seguimento de toda esa xente para saber cando os apaga e busca a outros próximos a eles que tamén apaguen os seus móbiles durante o mesmo tempo. Noutras palabras busca reunións secretas.

Investigadores da Universidade de Carnegie Mellon puxeron unha cámara nunha área pública e gravaron a xente camiñando. Identificaron a cada viandante cun programa de recoñecemento facial contrastárono coa base de fotografías dos usuarios de Facebook e os nomes doutras redes sociais. O resultado foi que foron quen de reunir información persoal de cada unha das persoas que transitaban por diante da cámara en tempo real. Esta tecnoloxía podería estar ao alcance de calquera mediante as cámaras dos smartphones ou das futuras google-



Snowden era un informático controlador de sistemas contratado pola CIA. Grazas ao seu traballo tivo acceso aos plans que o Goberno dos USA en colaboración coas principais empresas de telecomunicacións e os principais gobernos de Europa para estableceren un sistema de vixilancia muncial amparándose no dereito a facilitar a Seguridade Nacional. Snowden considerou que estaba en perigo a Privacidade individual e enviou milleiros de documentos secretos da Axencia de Seguridade Nacional dos EEUU á prensa. Hoxe está asilado en Rusia e reclamado polo seu país acusado de Alta Traición. Para outros moitos é un heroe.

AS COOKIES

Unha *cookie* é unha mensaxe enviada ao teu navegador desde un servidor web. O teu navegador almacena esa mensaxe como arquivo de texto. Cada vez que visites esa mesma páxina web o seu servidor lerá esa cookie almacenada co "boa" intención de identificarte para que a túa visita sexa cada vez máis personalizada, mellor adaptada aos teus intereses e necesidades.

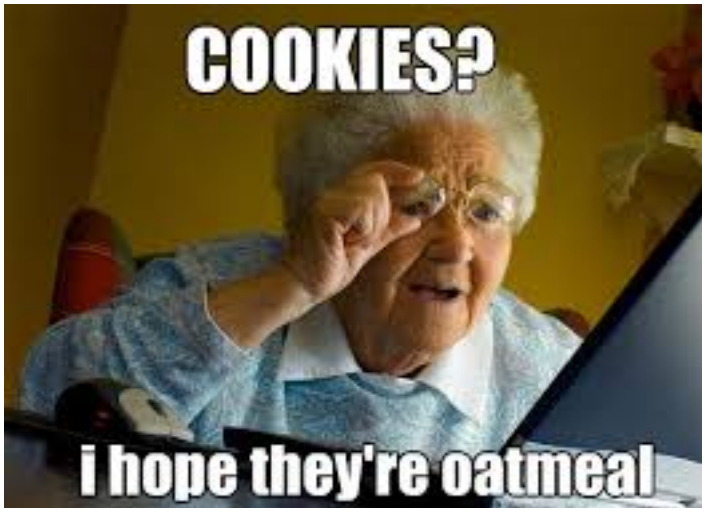
A vixilancia en internet desde o principio está basada nas cookies. En principio a palabra soa moi ben (galleta en inglés) pero o seu nome técnico resulta máis preciso: identificador persistente.
As cookies non foron pensadas para vixiarnos. Foron deseñadas para axudarnos a navegar pola rede. As webs non se lembran de nós cando as visitamos e as cookies foron a solución. Cada cookie contén un número diferente que permite que a web nos identifique. Agora cando clicas nunha web de vendas lle estás a dicir: son o cliente #608431. Así pode localizar o teu perfil de antigo cliente, actualizar a túa cesta de compra e gardar toda a información até a túa próxima visita, etc.

As empresas decatáronse con rapidez que podían instalar as súas cookies en webs doutras compañías co seu persmiso e pagando. Así naceron as cookies de terceiros. Empresas como DoubleClick (comprada por Google en 2007) empezaron a rastrexar internautas a través de moitas webs diferentes. Desde ese momento cando navegas os anuncios persíguente dunha páxina a outra. (...) Facebook, por exemplo, sabe de ti cada vez que premes o botón Gústame Facebook sexas membro ou non de Facebook e Google fai o mesmo cada vez que premes en Google Plus + ou usas a utilidade de Google Analytics.

Se queres saber quen está detrás dos teus pasos na rede instala un accesorio no teu navegador que permite monitorizar as cookies. Ficarás abraiado. Un reporteiro descubriu que 105 empresas rastrexaran o seu uso de internet durante 36 horas seguidas. En 2010 unha web aparentemente tan inofensiva coma Dictionary.com instalaba unhas 200 cookies no teu navegador durante unha visita.

Pasa o mesmo no teu móbil. As apps tamén te espían. Controlan a túa localización, e poden descargar a túa axenda, citas de calendario, e historial de navegación. (...) O xogo de ***Angry Birds*** segue os teus movementos incluso cando non xogas.

Actualmente a vixilancia en internet é moito máis insistente ca as cookies. De feito hai unha pequena guerra aberta. O teu navegador -si, incluso google chrome- permite bloquear e controlar o acceso das cookies. ***DoNotTrackMe*** é un dos accesorios máis populares. Máis a industria da vixilancia en internet contratacou coas "flash cookies" que son arquivos parecidos ás cookies pero que se almacenan no interior de Adobe's Flash cando os navegadores dan orde de borrar as cookies. Para bloquelas recoméndoche que instales FlashBlock.



galletas?
Que sexan de avea!