-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Anonimízate
Anonymise Yourself

Manual de autodefensa electrónica
Electronic Self-Defence Handbook

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.12 (GNU/Linux)

iQEcBAEBAgAGBQJT+e3IAAoJEC4elnvETsq7IMkIAJ2ifrpwP06ijHmsqWkXPczy
EDp3s98oQ8oIVVWn/lxBHDwKiJ+fpFFdG22agvNdLkyRVHPEIq0CfKXIceXXtkGI
yY9GqyLO19bt7wzu74+4iHqeVxjry4IXPIBkQhQ1VUSvELk9emAXnE6I7tYkHtEf
tSteY2chXVp3DtMHp47itlamYNYAV1KEm4MGNdEJAVs1Mi9jKzrksC7//aW9g0sQ
wx8Pjh9bro6McLSLpceTnoe6pwOS7jbDVqSUKbX4s/IWD5FDLvBLcNEvLYIDnDjc
EWN56nWLpfwme0mLKZJroEsUimTSuDArCoNbhrvkRDtbK93smRFUxk7tnY92c8Q=
=9eMM

-----END PGP SIGNATURE——

Lo que sabemos que saben

Internet y el estado de vigilancia masiva

Intentemos imaginar por un momento el vértigo que produciría asomarse al abismo de la intimidad colectiva, a los archivos de la vida cotidiana que se conservan en los Data Centers de los proveedores de Internet, las operadoras telefónicas o las empresas de Silicon Valley: las montañas infinitas de fotos personales, el contenido de los mensajes de correo electrónico, nuestro historial de búsquedas, nuestros pagos con tarjeta de crédito, los registros de todas las llamadas telefónicas que realizamos, la relación de todas las veces que hemos pulsado «me gusta» en una página de Facebook... Imaginemos ahora que toda esa información, que en muchos casos no querríamos compartir con nuestra pareja, nuestros amigos o nuestros familiares, está libremente a disposición de extraños que la almacenan y la analizan, sin necesidad de una justificación previa o supervisión judicial, sin que ni siquiera tengas derecho a saber de qué manera se está utilizando. Imagina, además, que el simple hecho de adoptar medidas de autoprotección, como, por ejemplo, herramientas para encriptar tus comunicaciones, te coloca en una lista de sospechosos, te convierte en un objetivo que hay que seguir. Imagina vivir en un mundo en el que el poder presupone que aquel que quiere preservar su intimidad hasta las últimas consecuencias debe de tener algo que ocultar.

Esta distopía es el mundo en el que nos despertamos el 5 de junio de 2013, el día en que comenzaron a salir a la luz las revelaciones de Edward Snowden. Snowden era un joven contratista de la empresa de seguridad Booz Allen Hamilton que trabajaba para la Agencia Nacional de Seguridad estadounidense (NSA) y escapó a Hong Kong con miles de documentos clasificados. Estos documentos ofrecían una cartografía antes impensable del mundo en la segunda década del siglo xxi, un mundo en el que el escrutinio de los ciudadanos y la violación de su privacidad están a la orden del día.

Si bien muchos expertos en seguridad informática llevan años insistiendo en la fragilidad de nuestras comunicaciones personales y en que toda noción de privacidad en Internet tiene algo de ilusorio, nadie podía imaginar hasta qué grado tan extremo las tecnologías digitales –las mismas que se nos ofrecían como instrumentos de liberación y autonomía que alumbrarían un mundo más igualitario, participativo y democrático– facilitarían la construcción de la estructura de control más sofisticada de la historia de la humanidad.

La paradoja es que esta pesadilla totalitaria ha sido concebida y ejecutada por las grandes democracias occidentales, con la necesaria colaboración –a veces con resistencia activa, otras con resignada connivencia– de la industria tecnológica, a la que hasta ahora se adjudicaba unánimemente efectos sociales positivos. El camino que nos ha llevado hasta aquí es más o menos conocido: la «guerra contra el terrorismo» iniciada por el gobierno estadounidense de G.W. Bush tras los atentados del 11 de Septiembre dotó a las agencias de inteligencia y otras estructuras gubernamentales de amplios poderes para intervenir en las comunicaciones personales de cualquier individuo y almacenarlas. Paralelamente, la explosión digital, de los móviles a la Web 2.0, ofrece la oportunidad de radiografiar detalladamente, en un grado inédito hasta la fecha, la vida cotidiana y la actividad social de la mayoría de los ciudadanos. Nunca había sido tan sencillo interceptar datos personales; nunca había habido tantos datos personales que capturar.

Además, la «inteligencia de señales» (*signal intelligence* o SIGINT), la rama del espionaje dedicada a la captura de comunicaciones, vive –como un sinfín de otras disciplinas– su propia revolución Big Data. Las agencias ya no están interesadas en interceptar un mensaje concreto que incrimine directamente a un sospechoso, sino en disponer de inmensos volúmenes de datos con los que reconstruir su esfera de contactos y movimientos a través de sus interacciones con otras personas. El general Keith Alexander, director de la NSA hasta octubre de 2013, definió este nuevo paradigma de una manera extremadamente gráfica: «para encontrar una aguja, se necesita un pajar». El pajar somos todos nosotros.

Las progresivas revelaciones del caso Snowden dibujan una clara imagen que permite entender hasta qué punto nuestra vida digital resulta transparente y accesible para la maquinaria de la sociedad de la vigilancia masiva.

Sabemos que operadoras de telefonía como Verizon han entregado a la NSA y el FBI los metadatos de millones de llamadas telefónicas que permiten saber a quién ha telefoneado cada uno, desde dónde y durante cuánto tiempo. Sabemos que, con el programa PRISM, la NSA puede acceder directamente y sin necesidad de una orden judicial a los servidores de compañías como Facebook, Google, Skype, Apple o Microsoft, para interceptar datos como los historiales de navegación, el contenido de correos electrónicos o los archivos descargados.

Sabemos que la NSA no solo ha interceptado regularmente las comunicaciones de los ciudadanos particulares, sino también las de los servicios diplomáticos de numerosos países y organismos internacionales, con el fin de obtener ventaja en las negociaciones. Sabemos que la misma infraestructura física de Internet ha sido intervenida por medio de programas que, como el británico Tempura o el estadounidense Upstream, permiten «pinchar» los cables de fibra óptica que canalizan el tráfico telefónico y de datos.

Sabemos de la existencia de infraestructuras paralelas en las que la NSA almacena datos personales para indexarlos y poder investigarlas con facilidad. El programa XKeyscore se basa en una red de servidores distribuidos por todo el planeta en los que los analistas pueden buscar datos vinculados a direcciones de email, nombres o direcciones IP.

Probablemente tardaremos años en comprender las implicaciones finales de las revelaciones facilitadas por Edward Snowden. A corto plazo muestran a las claras que, en la configuración tecnológica de Internet que utilizan millones de usuarios diariamente, cualquier sentido de la privacidad es ilusorio.

CC by-sa 2.0 - Trevor Paglen, 2013 | https://firstlook.org/theintercept/2014/02/10/new-photos-of-nsa-and-others/

We already know the outlines of the surveillance state

Let's try to imagine for a moment the vertigo that would be caused by looking down at the abyss of collective privacy, at the files of everyday life kept at the Data Centers of Internet providers, telephone operators and the companies in Silicon Valley. The infinite mountains of personal photos, the contents of our emails, our search histories, our credit card payments, the records of all the telephone calls we make, the list of all the times we have clicked on "Like" on a page in Facebook... Let's imagine now that all this information, which in many cases we would not choose to share with our partner, our friends or our family, is freely available to strangers who are constantly storing it and analysing it, without the need for any prior justification or legal supervision, and without you even having the right to know how it is being used. Imagine, as well, that the simple fact of choosing to use self-protection measures, such as tools to encrypt your communications, puts you on a list of suspects and converts you into a target to be pursued. Imagine living in a world where the powers that be take for granted that anyone who wants to preserve their privacy down to the last consequences must have something to hide.

This dystopia is the world where we awoke on 5 June 2013, the day that Edward Snowden's revelations saw the light. The young subcontractor from security consultants Booz Allen Hamilton who was working at the National Security Agency (NSA), escaped to Hong Kong with thousands of classified documents that offered a previously unimaginable cartography of the levels of scrutiny and violation of our privacy under which we are living in the second decade of the 21st century.

Although many IT security experts have been insisting for years on the fragility of our personal communications, and that all notion of privacy on the Internet has an air of illusion about it, nobody could imagine the extreme degree to which digital technologies – those tools of liberation and autonomy that promised a fairer, more participative and democratic world, would facilitate the construction of the most sophisticated control architecture in humanity's history.

The paradox is that this totalitarian nightmare has been conceived and executed by the great western democracies, with the necessary collaboration – sometimes with active resistance, others with resigned connivance – of the technology industry, the one whose effects on the social sphere we have read up to know as uniformly positive. The path that has brought us here is more or less well-known: the "war on terror", which was begun by the US administration of G.W. Bush after the attacks of 9/11, empowered intelligence agencies and other governmental structures with wide-ranging powers to intervene and store the personal communications of any individual. In parallel, the digital explosion, from mobiles to the Web 2.0, offers the opportunity to radiograph the everyday life and social activity of the majority of citizens with a level of detail previously impossible. It has never been so easy to intercept and capture personal data; never had there been so many personal data to capture.

Signal intelligence (or sig-int), the branch of espionage that is involved in capturing communications is experiencing, like other countless disciplines, its own Big Data revolution. The agencies are no longer interested in intercepting a specific message that directly incriminates a suspect, but in having access to immense volumes of data that allows them to reconstruct their sphere of contacts and movements through their interactions with other people. General Keith Alexander, director of the NSA until October 2013, defined this new paradigm in an extremely graphic way: "to find a needle, you need a haystack". The haystack is all of us.

The progressive Snowden case revelations sketch a clear image that allows us to understand to what point our digital life turns out to be transparent and accessible for the machinery of the mass surveillance society.

We know that telephone operators such as Verizon have handed over to the NSA and the FBI the metadata of millions of telephone calls that allow them to know who has called who, from where, and for how long. We know that the PRISM program allows the NSA to access directly without any need for a court warrant the servers of companies such as Facebook, Google, Skype, Apple or Microsoft, intercepting data such as search histories, the contents of emails or downloaded files.

We know that in addition to private citizens, the communications of the diplomatic services of numerous countries and international organisms have been regularly intercepted by the NSA, with the aim of obtaining a competitive advantage in negotiations. We know that the very physical infrastructure of the Internet has been intervened, through programs such as the British Tempura or the US Upstream, which allow "tapping" of the fibre optic cables that channel telephone and data traffic.

We know of the existence of parallel infrastructures in which the NSA stores personal data to index them and be able to search in their interior more easily. The program XKeyscore is based on a network of servers distributed around the planet in which analysts can search for data linked to email addressed, names or IP addresses.

It will probably take us years to fully comprehend the ultimate implications of the revelations leaked by Edward Snowden. In the short term, they clearly establish that in the Internet technological configuration that millions of users use daily, any sense of privacy is an illusion.

↙ National Reconnaissance Office (NRO), Chantilly (Virginia)
↓ National Security Agency (NSA), Fort Meade (Maryland)

© Gunnar Svedenbäck | https://www.flickr.com

© Telefónica

© Gigaom | https://www.gigaom.com

© Beyond My Ken

Data Centers:

↗ 60 Hudson Street, Nueva York / New York
Apple, Maiden (Carolina del Norte / North Carolina)
Telefónica, Alcalá de Henares
Facebook, Lulea (Suecia / Sweden)

→ Digital Beijing Building, Pekín / Beijing
Plone - Bahnhof, Estocolmo / Stockholm
Google, Hamina (Finlandia / Finland)
NAP of the Americas, Miami

© Burning7Chrome | http://www.panoramio.com

© Connie Zhou/Google

© http://www.bahnhof.net

© Digital-dreams

Cuando tu eres el producto

Decir que cuando un servicio es gratuito lo que pasa en realidad es que lo pagamos de otra manera (con datos) ya empieza a ser un hecho aceptado por muchas de las personas que utilizan la tecnología de forma cotidiana y tienen una cierta consciencia del rastro de datos que van dejando con cada una de las actividades que realizan.

Sin embargo, más allá del «tú eres el producto», pocas personas conocen de forma detallada en qué consiste o cómo funciona dicho pago con datos. De hecho, no es una cuestión sencilla. El ámbito con el que quizá es más fácil introducir el tema es el de la navegación por Internet: las empresas y prestadores de servicios nos ofrecen de forma gratuita sus páginas web, y a menudo servicios asociados, como la posibilidad para tener contacto con otras personas a través de redes sociales, foros, etc. No obstante, tal como muestra la herramienta Disconnect, cada vez que entramos en una página web una serie de microprogramas conocidos como *cookies* (galletas) se instalan en nuestro dispositivo y mandan al propietario del sitio web información sobre nuestra dirección IP o MAC (la «matrícula» de nuestro dispositivo), el tiempo que utilizamos el sitio web y la manera en que lo utilizamos, y a menudo también sobre los demás sitios web que consultamos mientras tenemos una web concreta abierta. Además, es habitual que distintas empresas paguen a la web que estamos visitando para poder instalarnos galletas de terceros.

De hecho, cada vez que abrimos un sitio web, nuestro ordenador puede recibir entre decenas y cientos de peticiones de instalación de galletas. Cuando navegamos por Internet, pues, somos el producto, porque a cambio de la visita proporcionamos información sobre nuestra actividad digital y, a menudo, datos personales que han sido prepagados por las empresas que han contratado con un sitio web en particular la posibilidad de espiarnos.

Pero si el ejemplo de la navegación web es el más habitual, cada vez es el menos protagonista. El mismo despliegue de conexiones no aparentes ni fácilmente controlables se produce también cuando utilizamos, por ejemplo, una tarjeta de cliente, que relaciona nuestro patrón de consumo con un nombre, una dirección, una tarjeta de crédito y a menudo también con las respuestas al pequeño cuestionario que se nos pide que rellenemos cuando realizamos la solicitud.

Otro ámbito de recogida de datos cada vez más importante es el uso del espacio público. Como muestra la infografía de las página 6 y 7, nuestro deambular incauto por la ciudad cada vez tiene menos de anónimo, y los escáneres de direcciones MAC, las cámaras térmicas y de videovigilancia, las redes Wi-Fi, las farolas «inteligentes» o los sensores de lectura automática de matrículas nos incorporan de forma rutinaria a bases de datos que en algún lugar sirven a alguien para sacarles un provecho que ni conocemos ni controlamos.

En el ámbito doméstico es quizá donde aumenta de forma más preocupante esta monitorización de nuestros movimientos y rutinas para elaborar con ellos patrones vendibles: todos los electrodomésticos «inteligentes», desde el contador hasta el televisor, pasando por la nevera, construyen una red de extracción de datos que trata de perfeccionar la imagen de quién somos y qué deseamos o podemos desear, a fin de adelantarse a nuestras necesidades y tentarnos a adquirir productos o servicios adicionales. Pagamos, pues, dos veces: cuando adquirimos el electrodoméstico y cuando este nos convierte en producto al revender nuestros datos.

Si dibujar el mapa de la serie de mecanismos y procesos que nos convierten en producto es relativamente sencillo, no lo es tanto establecer cuál es el modelo de negocio y el beneficio concreto que creamos con nuestros datos. La empresa Datacoup, por ejemplo, permite al usuario elegir qué datos quiere vender (desde el uso de redes sociales hasta datos bancarios) a cambio de hasta 8 dólares al mes. De forma similar, en una denuncia colectiva presentada en Estados Unidos contra Facebook por apropiarse indebidamente de los nombres y preferencias de los usuarios, la empresa acabó accediendo a pagar 10 dólares a cada usuario. De modo que no nos haremos ricos.

El verdadero dinero de la mercantilización de los datos personales no se halla todavía en esta interfaz concreta entre el usuario y las empresas que recogen datos. Quienes ganan dinero con nuestra despreocupada cesión de datos personales son aquellos que se colocan en las primeras posiciones de la carrera para almacenar datos a la espera de que la promesa de la monetarización se haga realidad. De momento esta promesa solo ha llenado los bolsillos de los fundadores y accionistas de empresas con un modelo de negocio centrado en la compra y venta de perfiles de datos (como la mencionada Facebook, o Tuenti, Google, Foursquare, YouTube, etc.) y ha creado un submercado de *data brokers* (corredores de datos), compañías dedicadas al cruce de distintas bases de datos datos de actividad *online* y *offline* a fin de aumentar el precio de venta de los perfiles generados de esta manera.

Puede que a determinadas personas este panorama no les genere inquietudes, ya que pagar con datos abre también la puerta a la promesa de servicios personalizados y atención individualizada. Sin embargo, los corredores de datos no se limitan a cruzar los datos de lo que compramos, con quién interactuamos y qué nos gusta: el comercio de datos incluye también, y cada vez más, expedientes médicos, datos fiscales y de renta o datos bancarios, o sea, el tipo de información que puede determinar si se nos concede un crédito, si se nos ofrece un seguro médico más o menos caro o si conseguimos un lugar de trabajo. De repente, el precio pagado en datos se revela desproporcionado.

Cuando aceptamos ser el producto, pues, conviene no olvidar que aceptamos también que se nos pueda acabar dejando en el fondo de la estantería, escondidos e ignorados porque nuestro perfil no promete la solvencia, la salud o la obediencia que ofrecen los demás.

↑ https://disconnect.me/disconnect

When You Are the Product

The idea that when a service is free of charge, in reality what happens is that we pay for it in another way (with data), is now becoming an accepted fact for many people who use technology on a daily basis and have a certain awareness of the data trail that each of their activities leaves behind.

However, beyond the fact that "the product is you", few people have detailed knowledge of what this payment with data consists of, or of how it functions. In fact, the question is not a simple one. The area where it is perhaps easiest to introduce the subject is in Internet browsing: companies and service providers offer their websites free of charge, often with associated services, such as the possibility of making contact with other people through the social networks, forums, etc. Nonetheless, as shown by the tool Disconnect, every time we enter a website, a series of micro-programs known as "cookies" install themselves in our device and send the website owner information. This may include our IP address or MAC (Media Access Control address, our device's "registration number"), the length of time and way that we use the website and, often, information on other websites we visit while we have a specific website open. In addition, different companies frequently pay the website we are visiting in order to be able to install third-party cookies in our devices.

In fact, every time we open a website, our computer can receive between dozens and hundreds of requests to install cookies. When we browse the Internet, therefore, the product is us, because in exchange for our visit we provide information on our online activity and, often, personal data that have been paid for in advance by the companies that have made a deal with a particular website in order to be able to spy on us.

However, although website browsing may be the most common example it is increasingly less significant. The very deployment of non-apparent connections that are not easily controllable arises when we use, for example, a customer card that relates our consumption pattern with a name, address, credit card and often the answers to a short questionnaire that we are asked to fill in when we apply.

Another area of growing data collection is in the use of the public space. As shown by the infographic on pages 6-7, our unsuspecting strolls around cities are increasingly less anonymous. Scanners of MAC addresses, thermal and video-surveillance cameras, Wi-Fi networks, smart lamp posts and registration-plate readers with automatic sensors are incorporating us routinely into databases that somewhere are used by someone to make a profit that we neither know about nor control.

It is in the domestic sphere where we should be most concerned about this monitoring of our movements and routines to produce saleable patterns. All "smart" electrical appliances, from the electricity meter to the television, and including the refrigerator, constitute a network of data extraction that strives to perfect the image of who we are and what we want, or may want, in order to be one step ahead of our needs and tempt us into acquiring additional products or services. Thus, we pay twice: when we acquire the electrical appliance and again when the appliance converts us into a product by reselling our data.

If making the map of the series of mechanisms and processes that convert us into a product is relatively simple, it is not so simple to establish which is the business model or the specific profit that we create with our data. The company Datacoup, for example, allows users to choose which data they want to sell (from the use of social networks to bank data) in exchange for up to 8 dollars per month. Similarly, in a collective lawsuit presented in the USA against Facebook for unduly appropriating users' names and preferences, the company ended up agreeing to pay 10 dollars to each user. Which means that we are not going to get rich.

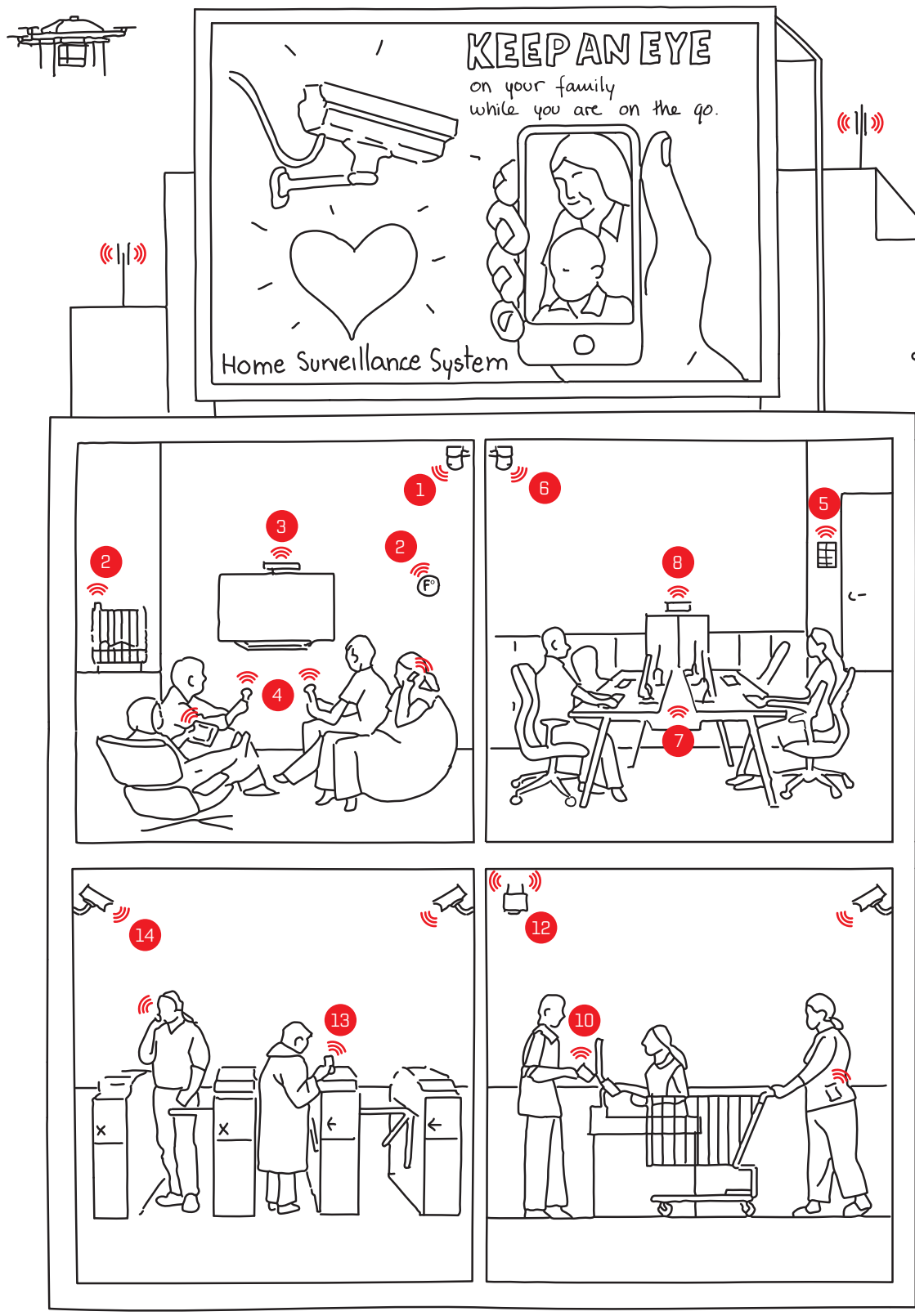
The real money from the commercialisation of personal data is not yet in this specific interface between the user and the companies that collect data... The people who earn money from our carefree surrender of personal data are those who position themselves at the front of the race to store data while waiting for the promise of monetisation to come true. For the time being, this promise has only lined the pockets of the founders and shareholders of companies with a business model focused on the sale and purchase of data profiles (such as the aforementioned Facebook, or Tuenti, Google, Foursquare, YouTube, etc.). It has also created a sub-market of "data brokers": companies that cross different databases to increase the sales price of profiles generated by crossing data on activity online and offline.

For some people, this scenario perhaps poses no concerns. Paying with data also opens the door to the promise of personalised services and individualised attention. However, data brokers do not limit themselves to crossing data on what we purchase, with whom we interact, and what we like. This trade in data also includes, increasingly, medical dossiers, tax and income data or bank details. The type of information that can determine whether we are granted a loan, whether we are offered more or less expensive medical insurance, or whether we manage to land a particular job. In fact, the price paid in data reveals itself to be disproportionate.

When we accept that the product is us, it is important not to forget that we are also accepting that we may end up left at the back of the shelf, hidden and ignored because our profile does not promise the solvency, health or obedience offered by others.

Escenas cotidianas de una ciudad bajo vigilancia

Everyday Scenes of a City under Surveillance



Probablemente no somos conscientes del número de veces a lo largo del día que entramos en contacto con una tecnología que produce datos en los que se reflejan nuestros actos. Ya sea a pie de calle, en casa, en el trabajo o en los espacios comerciales, la ciudad del siglo XXI es una ciudad bajo vigilancia. Todos estos datos pueden ser, potencialmente, una amenaza para nuestra privacidad. No es exagerado decir que hoy en día son pocos los momentos en que somos auténticamente anónimos.

En casa

1 VIDEOVIGILANCIA DOMÉSTICA: los dispositivos que transmiten vídeo inalámbricamente, como los monitores de vigilancia de bebés, pueden ser interceptados y su señal capturada desde el exterior de la casa.

2 CONTADORES DE LA LUZ Y TERMOSTATOS INTELIGENTES: permiten identificar el comportamiento cotidiano de los habitantes de cada hogar, al mostrar en el registro del consumo cuándo se activa la ducha, la tostadora o la cafetera.

3 TELEVISORES INTELIGENTES: en el futuro inmediato las televisiones conectadas a Internet, con cámara web incorporada, monitorizarán los hábitos familiares de consumo de TV e incluso el uso de espacios comunes en el hogar.

4 CONSOLAS DE VIDEOJUEGOS: las últimas generaciones de consolas llevan incorporadas cámaras de vídeo e infrarrojos que pueden captar y trasmitir imágenes y sonido de la sala de estar sin que el usuario lo sepa.

En el trabajo

5 CONTROL DE ENTRADAS Y SALIDAS BIOMÉTRICO: cada vez más, los sistemas para registrar el momento en que los trabajadores acceden al lugar de trabajo y lo abandonan incorporan sistemas de identificación biométrica como huellas dactilares o reconocimiento ocular.

6 VIDEOVIGILANCIA: las cámaras situadas en el recinto de trabajo y sus grabaciones pueden emplearse para reconstruir los movimientos de los trabajadores, o para comprobar el lugar en el que se encuentran en un momento determinado.

7 MONITORIZACIÓN REMOTA DE LA PANTALLA DE TRABAJO: distintos sistemas de control de la productividad archivan regularmente capturas de la pantalla del trabajador y la envían a superiores o clientes, para comprobar su actividad.

8 BASES DE DATOS PERSONALES: en numerosas empresas, las bases de datos personales de sus clientes son una herramienta de trabajo esencial diariamente. Estas bases de datos pueden incluir historiales financieros, de salud o de riesgos, entre otros.

En los espacios comerciales

9 SENSORES DE CONTEO DE PERSONAS: se utilizan para monitorizar el tráfico de compradores en espacios comerciales, así como para registrar el tiempo que pasan contemplando los escaparates.

10 TARJETAS DE FIDELIZACIÓN: a cambio de ofrecer descuentos y ventajas, se utilizan para crear un perfil del consumidor basado en sus hábitos de compra y conocer mejor sus costumbres como consumidor.

11 IBEACONS: este sistema permite a los comercios enviar anuncios y ofertas a los móviles que se encuentren físicamente cerca de ellos, si se han instalado la aplicación correspondiente. Se teme que se pueda emplear para rastrear los movimientos de los compradores de la zona.

12 WI-FI GRATUITO: a cambio de ofrecer acceso gratuito a Internet, distintos servicios comerciales exigen los datos de identificación en redes sociales como Facebook o Twitter, y acceden a nuestro perfil en estos servicios.

En el transporte urbano

13 ABONOS DE TRANSPORTE PÚBLICO: las tarjetas recargables que se usan en cada vez más redes de autobús y metro producen datos sobre los desplazamientos de sus usuarios.

14 VIDEOVIGILANCIA EN ANDENES Y VAGONES DE TREN Y METRO: tanto los andenes de estaciones como el interior de los vagones están equipados en muchos casos con cámaras de videovigilancia.

15 REDES DE BICICLETAS PÚBLICAS: las tarjetas de usuario registran el trayecto realizado y las horas de salida y llegada del usuario.

16 AUTOMÓVILES: las matrículas de los vehículos pueden ser registradas por sistemas ANPR de reconocimiento de matrículas, tanto en la calle como en los aparcamientos. También se registran los trayectos de los coches que incorporan sistemas de pago de telepeaje (Teletac).

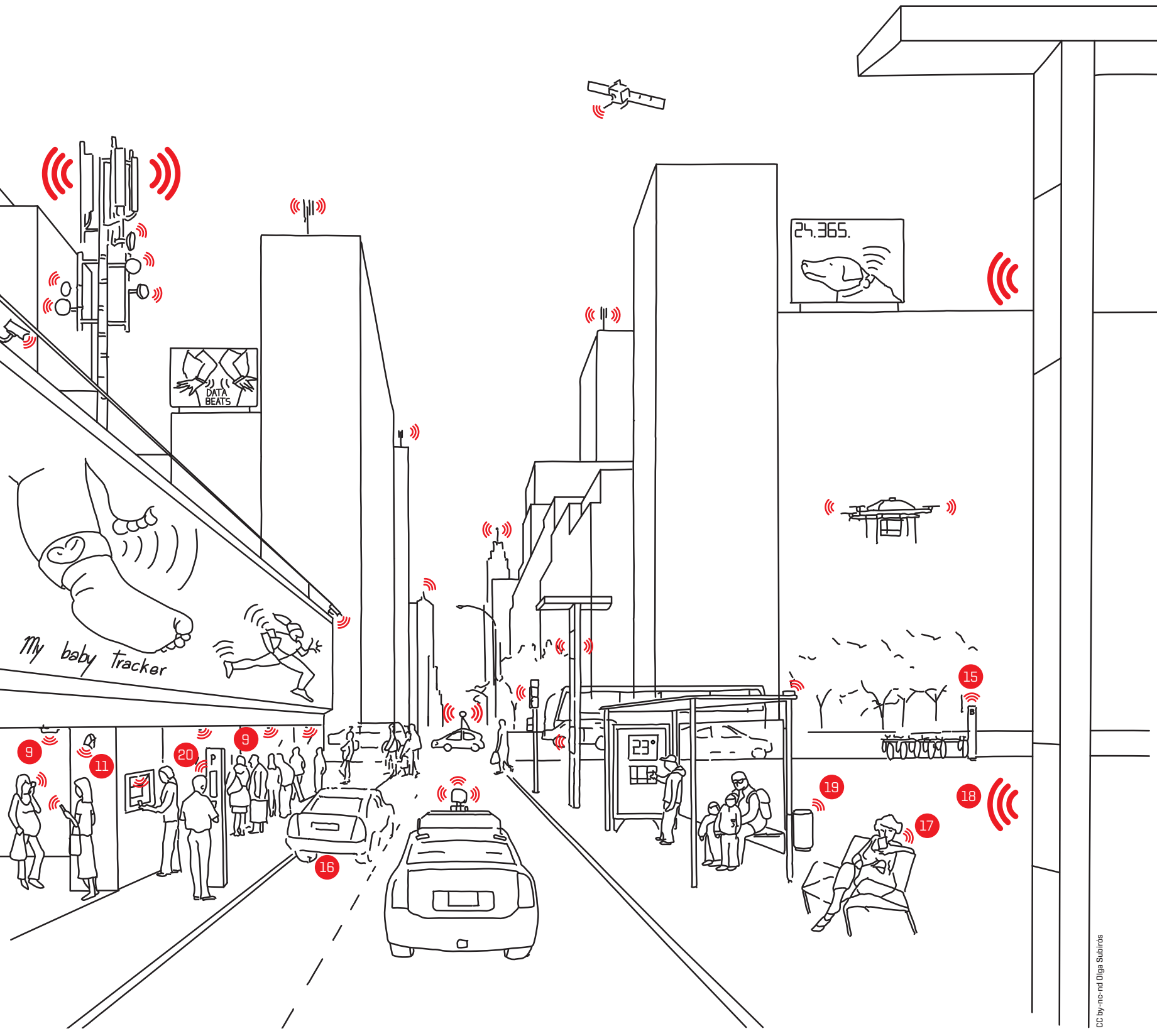
En la calle

17 TELEFONÍA MÓVIL: permite a las operadoras y a servicios de inteligencia determinar –por triangulación de la señal, o GPS– la posición aproximada del usuario y activar remotamente el auricular para usarlo como micrófono.

18 CÁMARAS TÉRMICAS Y SENSORES SONOROS: presentes en muchos espacios públicos de las grandes ciudades contemporáneas, se usan para medir el flujo de peatones o registrar los niveles de ruido.

19 MOBILIARIO URBANO INTELIGENTE: la incorporación progresiva de sensores en paradas de autobús, farolas o papeleras tiene el fin de detectar la presencia de peatones en su proximidad, pero también puede identificarlos captando información de sus teléfonos inteligentes.

20 SISTEMAS DE PARKING: el pago con tarjeta en zonas azules y verdes genera datos sobre el usuario. Las plazas están incorporando progresivamente sensores que determinan si están libres u ocupadas.



We are probably not aware of the number of times over the course of a day that we enter into contact with a technology that produces data in which our acts are reflected. Whether in the street, at home, at work or in commercial spaces, the 21st-century city is a city under surveillance. All these data can be, potentially, a threat to our privacy. It is no exaggeration to say that nowadays there are very few moments when we are truly anonymous.

At home

1 **DOMESTIC VIDEO SURVEILLANCE:** devices that offer wireless video transmission, such as baby monitors, can be intercepted and their signal captured from outside the house.

2 **ELECTRICITY METERS AND SMART THERMOSTATS:** allow the everyday behaviour of the inhabitants of each household to be identified, with the record of consumption showing when the shower, toaster, or coffee-maker are used.

3 **SMART TV:** in the immediate future, televisions connected to the Internet with an integrated webcam will monitor the family's TV consumption habits and even the use of common spaces in the home.

4 **VIDEOGAME CONSOLES:** the latest generations of gaming consoles incorporate video cameras and infrared lights that can capture and transmit images and sound from the room without users having any knowledge of this.

At work

5 **BIOMETRIC ARRIVAL AND DEPARTURE CONTROL:** systems for clocking in and out of the workplace are progressively incorporating biometric identification systems such as fingerprints and ocular recognition.

6 **VIDEO-SURVEILLANCE:** cameras situated in the workplace and their recordings can reconstruct the movements of employees or check their location at a particular moment in time.

7 **REMOTE MONITORING OF THE WORK COMPUTER SCREEN:** different productivity control systems regularly save screen captures from workers' computers and send them to superiors or customers, in order to check on their activity.

8 **PERSONAL DATABASES:** at numerous companies, databases containing personal data on customers are an essential everyday tool. These databases may include financial, health or credit risk histories, among others.

In shopping areas

9 **SENSORS FOR COUNTING PEOPLE:** these are used to monitor the traffic of buyers in shopping areas as well as to analyse the time that they spend window shopping.

10 **LOYALTY CARDS:** in exchange for offering discounts and benefits, they are used to create a consumer profile based on purchasing habits and to find out more about user patterns as consumers.

11 **IBEACONS:** this system allows shops to send advertisements and special offers to those mobile devices that in close physical proximity to them, if they have the corresponding app installed. It is feared that it may be used to trace purchasers' movements in the area.

12 **WI-FI FREE:** in exchange for free Internet access, different commercial services demand identification data via social networks such as Facebook and Twitter, and access our profiles on these services.

On urban transport

13 **PUBLIC TRANSPORT PASSES:** rechargeable cards that are used in increasing numbers of bus and underground networks produce data on the journeys made by their users.

14 **VIDEO-SURVEILLANCE ON PLATFORMS AND IN TRAIN AND METRO CARRIAGES:** both station platforms and the interior of carriages include, in many cases, video-surveillance cameras.

15 **PUBLIC BICYCLE NETWORKS:** user cards register the journey made and the times that users departed and arrived.

16 **CARS:** car registration numbers can be recorded by ANPR registration number recognition systems, both on the street and in car parks. Journeys made by cars that incorporate automatic toll payment systems (e.g. Teletac) are also registered.

In the street

17 **MOBILE TELEPHONES:** allow intelligence services and mobile operators to determine the approximate position of the user through signal triangulation or GPS, and remotely activate the earpiece to use it as a microphone.

18 **THERMAL CAMERAS AND SOUND SENSORS:** present in many public spaces in contemporary cities, they are used to measure the flow of pedestrians or capture noise levels.

19 **SMART URBAN FURNITURE:** the progressive incorporation of sensors at bus stops, on lamp posts or on litter bins, has the aim of detecting the presence of pedestrians in close proximity to them, but it can also identify them by capturing information from their smartphones.

20 **PARKING SYSTEMS:** card payment in blue and green city parking zones generates data on users. Parking spaces are progressively incorporating sensors to determine whether they are occupied or free.

Autodefensa electrónica: estrategias y tácticas

Como respuesta a la videovigilancia, activistas y artistas han creado un amplio abanico de métodos para perturbar su funcionamiento, así como para protestar contra otras formas de visibilidad y trazabilidad. La mayoría de las primeras formas de resistencia iban dirigidas a las cámaras de televisión de circuitos cerrados, ya fuera escenificando mensajes políticos de *contestación* ante la cámara (como hacían los Surveillance Camera Players en los años noventa) o sencillamente pintarrajeándolas o reorientándolas.

A medida que la videovigilancia se ha vuelto cada vez más omnipresente y automatizada, lo mismo ha ocurrido con las herramientas y los medios de resistencia. Las cámaras de televisión de circuitos cerrados han ido evolucionando y han pasado del circuito cerrado a métodos de videovigilancia en red, a la par que formas de resistencia como *Life: A User's Manual* han explotado los nuevos medios utilizados por la videovigilancia –por ejemplo, el espectro inalámbrico– para poner de manifiesto las nuevas relaciones sociales creadas por dicha vigilancia. Cuanto más en red se conecta la vigilancia, más lo hacen las formas de conocimiento creadas para resistir a ella, como las bases de datos de cámaras de videovigilancia, y los métodos de elusión se han mezclado cada vez más con la moda (como hace patente CV Dazzle) a medida que han ido ampliándose las capacidades de alcance y de reconocimiento de la videovigilancia, y de las ciudades que la despliegan.

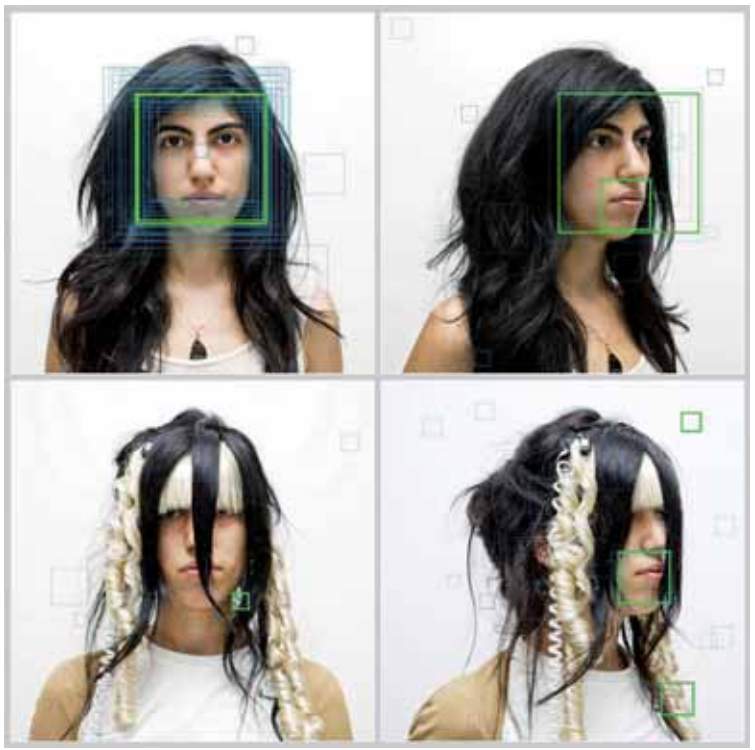
Surveillance Camera Players (1998)
Los Surveillance Camera Players (SCP) son un grupo formado en 1996 que plantó cara de manera directa a las cámaras de videovigilancia mediante performances públicas. Los SCP se inspiran en el movimiento situacionista, que utilizaba el espectáculo disruptivo y la performance pública como medio para destacar o criticar las relaciones sociales. Han escenificado versiones adaptadas de varias obras delante de cámaras de videovigilancia en Nueva York, entre ellas una interpretación en público en Manhattan de *Re-Elect Big Brother* (basada en el *1984* de Orwell) –con vestuario incluido– el día de las elecciones estadounidenses, en noviembre de 1998. Además de quedar grabada por la cámara de videovigilancia, la performance también fue grabada por equipos de filmación para poder emitirla en televisiones por cable locales e independientes. Con sus actuaciones ante la cámara, los SCP luchan de manera efectiva contra la idea de que las personas vigiladas deben resignarse a su suerte.

Institute of Applied Autonomy, *iSee* (2001)
El proyecto iSee, del Institute of Applied Autonomy, es una base de datos geográfica de participación colectiva que ejemplifica perfectamente la táctica de la *sousveillance* o vigilancia desde abajo. Con esta herramienta los usuarios pueden facilitar la localización geográfica de cámaras de videovigilancia y, a su vez, consultar la base de datos para saber dónde se encuentran las cámaras. En lugar de enfrentarse directamente a las cámaras mismas, el iSee ayuda a los usuarios a seguir una «ruta menos vigilada» por la ciudad. El iSee para Manhattan, por ejemplo, se basa en parte en datos de un «censo de circuitos cerrados de televisión» hecho entre 1998 y 2002, y permite que los usuarios creen sus itinerarios evitando tantas cámaras como sea posible. A pesar de ser una herramienta de resistencia a la videovigilancia, lo que hace es reducir, más que anular totalmente, la exposición a las cámaras de vigilancia.

Michelle Teran, *Life: A User's Manual* (2003-2006)
Este proyecto de Michelle Teran juega con la yuxtaposición de mundos virtuales y físicos mediante un receptor inalámbrico que utiliza las transmisiones inalámbricas accesibles públicamente de las cámaras de videovigilancia que estén cerca. El artefacto en sí es una maleta con ruedas arrastrada por un personaje femenino nómada y equipada con una pequeña pantalla negra circular en la que se muestran grabaciones de videovigilancia. Basado en la novela epónima de Georges Perec de 1978, en la que se narran las historias entrecruzadas de los habitantes de un edificio de pisos de París, el proyecto de Teran entreteje el espacio físico de la calle con el espacio virtual de las grabaciones de videovigilancia. *Life: A User's Manual* utiliza el espectro inalámbrico accesible públicamente (para que no se convierta en sí mismo en una tecnología de vigilancia intrusiva) y pone de relieve hasta qué punto las imágenes de las vidas de los habitantes de la ciudad emitidas por ellos mismos hacen posible la vigilancia.

Adam Harvey, *CV Dazzle* (2010)
A medida que las cámaras de videovigilancia proliferan y adquieren capacidades de reconocimiento facial, la necesidad de defender el rostro de cada uno ha pasado a estar ligada a la necesidad de mantener la identidad y las emociones de cada uno en el anonimato. Entrad en CV Dazzle, una herramienta que da consejos de maquillaje y moda para burlar los sistemas de reconocimiento facial. El nombre de esta herramienta es una adaptación en clave de humor de Dazzle, el camuflaje cubista utilizado por los acorazados de la Primera Guerra Mundial, y se basa en unas investigaciones que demuestran que el maquillaje o las obstrucciones en el rostro pueden confundir o inutilizar los sistemas de reconocimiento facial. Además de un *book* de maquillajes y peinados, CV Dazzle ofrece consejos –basados en la investigación– para recuperar la privacidad, incluyendo métodos para oscurecerse los ojos o la nariz y, así, desdibujar los rasgos comunes que buscan los sistemas de reconocimiento facial.

Vecinos de Lavapiés, *Un barrio feliz* (2010)
Cuando en 2010 el Ayuntamiento de Madrid instaló cámaras de videovigilancia en el barrio de Lavapiés, muchos vecinos opusieron resistencia activa a las premisas y las promesas del sistema. Parte del tono crítico de *Un barrio feliz* se proponía poner de relieve la justificación que se hizo de la videovigilancia: ante el descenso de la delincuencia y las insinuaciones del coordinador de seguridad del Ayuntamiento sobre la presencia de «otras personas», se denunciaba que el sistema era un instrumento de fragmentación social. La respuesta de los activistas consistió en parodiar el discurso oficial sobre la videovigilancia mediante pósteres críticos, algunos con la inscripción «Lavapiés 1984». La medida más controvertida del grupo hizo patente la doble vara de medir de la videovigilancia: cuando el grupo instaló una cámara propia en la zona, emulando el proyecto municipal, fue penalizado con una multa de 10.000 euros de la Agencia de Protección de Datos.



© Adam Harvey

↑ http://cvdazzle.com
→ Michelle Teran, Life: A User´s Manual (Berlin Walk) , 2003-2006
→ http://unbarriofeliz.wordpress.com

In response to camera surveillance, activists and artists have created a range of means of disrupting their functioning as well as contesting other forms of visibility and traceability. Most of the early forms of resistance targeted closed-circuit television (CCTV) cameras either by performing political messages "back" at the camera (like the Surveillance Camera Players in the 1990s) or simply by defacing or reorienting them.

As visual surveillance has become increasingly ubiquitous and automated, so have the tools and modes of resistance to it. As CCTV evolved away from the CC – the "closed circuit" –towards networked forms of video surveillance, forms of resistance such as *Life: A User's Manual* have exploited the new media used by video surveillance, such as wireless spectrum, to illustrate the new social relations surveillance creates. As surveillance becomes more networked, so have the forms of knowledge created to resist it, such as databases of surveillance cameras. Meanwhile, modes of evasion have increasingly blended with fashion (as CVDazzle shows) as the reach and recognition capabilities of video surveillance, and the cities housing them, have expanded.

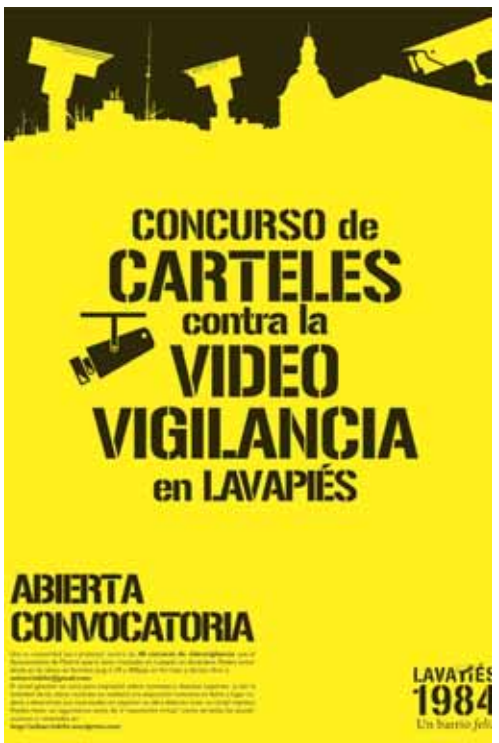
The Surveillance Camera Players (1998)
The Surveillance Camera Players are a group formed in 1996 that directly confront video surveillance cameras through public performance. The SCP are inspired by the situationist movement which used disruptive spectacle and public performance as a mode of highlighting or criticizing social relations. They have performed adapted versions of various plays in front of video surveillance cameras in New York City, including a public rendition of *Re-Elect Big Brother* (based on Orwell's *1984*) – including constumes – in Manhattan on the US election day in November 1998. In addition to being filmed by the surveillance camera, the performance was also recorded by camera crews to be shown on local independent cable TV. By performing for the cameras, the SCP effectively contest the idea that those watched should be resigned to their fates.

Institute of Applied Autonomy, *iSee* (2001)
The iSee project, by the Institute of Applied Autonomy, is a crowd-sourced geographic database that epitomizes the tactic of *sousveillance*, or "surveillance from below". With this tool, users can submit the geographic locations of video surveillance cameras and in turn consult the database for information about where cameras are. Rather than directly contesting cameras themselves, the iSee tool helps users to take a "path of least surveillance" through the city. The iSee tool for Manhattan, for example, relies partly on data from a "CCTV census" conducted in 1998-2002 and allows users to generate an itinerary that will avoid as many cameras as possible. While iSee is a surveillance resistance tool, it minimizes rather than totally negates one's exposure to video capture.

Michelle Teran, *Life: A User's Manual* (2003-2006)
Michelle Teran's project plays with the juxtaposition of virtual and physical worlds by using a wireless receiver to draw on publicly-accessible wireless transmissions from surveillance cameras in proximity. The artefact itself is a wheeled suitcase, pulled by a nomadic female character, featuring a small circular black screen on which captured camera feeds are shown. Based on the eponymous 1978 novel by Georges Perec, featuring cross-cutting stories of people living in an apartment building in Paris, Teran's project similarly weaves together the physical space of the street and the virtual space of the camera feed. *Life: A User's Manual* uses publicly accessible wireless spectrum (lest it become an intrusive surveillance technology itself), illustrating the extent to which the surveillance is enabled by city dwellers' own broadcasts of their lives.

Adam Harvey, *CVDazzle* (2010)
As surveillance cameras proliferate and gain facial recognition capabilities, the need to defend one's likeness has become tied to the need to keep one's identity and emotions anonymous. Enter CVDazzle, a makeup and style toolkit to thwart facial recognition systems. The toolkit's name is a playful adaptation of "Dazzle", the cubist camouflage used by World War I battleships, and draws on research showing that facial recognition systems may be confused or rendered ineffective by makeup or obstructions to the human face. In addition to a "lookbook" of makeup and hair styles, CVDazzle offers research-based tips to reclaim privacy including methods for obscuring one's eyes or nose to confuse the common features that facial recognition systems look for.

Residents of Lavapies, *Un barrio feliz* (2010)
When Madrid City Council introduced video surveillance cameras to the Lavapies neighbourhood in 2010, many residents actively resisted the premises and promises of the system. Part of the critical edge that *Un barrio feliz* ("a happy neighbourhood") brought was attention to the justification for video surveillance: with crime falling, and the City Council's security coordinator suggesting the presence of "other people", the system was denounced as a tool of social fragmentation. In response, the activists' parodied the official line on video surveillance through critical posters, some emblazoned with "Lavapies 1984". The group's most controversial measure showed the double standard of video surveillance: having installed a camera of its own in the area, mimicking the city's own project, the group was met with a € 10,000 penalty from the Data Protection Agency.



© Heather Dewey

↑ http://privacygiftshop.com
↓ http://privacygiftshop.com

↑ http://biogenfutur.es
↓ https://www.blackphone.ch

Stealth wear
Adam Harvey / Undisclosed LCC
40 - 2.500 $
http://privacygiftshop.com

Invisible
Biogenfutur
230 $
http://biogenfutur.es

Adam Harvey, miembro del colectivo Undisclosed de Nueva York, pretende llevar a cabo una tarea de concienciación sobre el auge de la Sociedad de la Vigilancia mediante un original proyecto artístico que intenta combinar privacidad y moda. Se trata de diferentes prendas «anti-drone» creadas con un material que evita la detección por parte de las cámaras térmicas con las que están equipados los aviones no tripulados. El inevitable color plateado que el material protector da a estos diseños recuerda sin duda a la imaginería futurista propio de décadas anteriores.

Off pocket
Adam Harvey / Undisclosed LCC
80 $
http://privacygiftshop.com

El Off Pocket es una funda para teléfonos inteligentes con protección de ondas de entre 500 Mhz y 5 Ghz. Previene el intercambio indeseado de información creando el efecto jaula de Faraday, lo que evita la revelación accidental de cualquier dato o metadato proveniente de las señales emitidas por los dispositivos Wi-Fi, Bluetooth o GPS, o por el propio teléfono. Funciona en todos los países y con todos los operadores. Este complemento está fabricado con un material flexible que permite que su peso no llegue a los cien gramos. Está disponible en tres tamaños diferentes y además es resistente al agua. Si su precio no está al alcance de nuestro bolsillo, podemos optar por la versión «háztelo tú mismo» que ofrece killyourphone.com, tal vez menos glamurosa pero más auténtica y asequible.

No solo de vigilancia electrónica vive el Panóptico. Biogenfutur nos ofrece una solución para todos esos pequeños rastros de saliva, pelos, uñas y escamas de piel con los que vamos geolocalizando nuestra presencia allá donde vamos y dando pistas sobre nuestras acciones. Con tan solo 0,5 nanogramos de ADN ya es posible realizar un análisis forense de nuestro «DNI biogenético». Gracias al líquido Erase se puede eliminar el 99,5% del rastro de ADN, y completando la acción con Replace se logra crear confusión sobre el 0,5% Restante. Quizá parezca exagerado, pero en 2013 Heather Dewey-Hagborg logró crear retratos realistas a partir de las muestras de ADN aún presentes en las colillas, pelos y chicles que recolectó en las calles de Nueva York.

Blackphone
Silent Circle / Geeksphone
629 - 829 $
https://www.blackphone.ch

Si queremos una alternativa mucho más práctica y operativa al Off Pocket que no nos impida utilizar el teléfono mientras garantizamos la privacidad, Blackphone nos ofrece un teléfono específicamente diseñado para evitar el rastreo por parte de terceros. Cuenta con una versión de Android creada expresamente para este teléfono, el PrivatOS, y múltiples herramientas para la comunicación segura y anónima: Silent Phone, Silent Text, Silent Contacts, búsqueda y navegación anónima, y el uso de VPN que ofrece Disconnect; además ofrece almacenamiento seguro en la nube mediante SpiderOak, sistema antirrobo y el servicio de atención de Black-phone Security Center.

Stealth wear
Adam Harvey / Undisclosed LCC
$40.00 - $2,500.00
http://privacygiftshop.com

From the Undisclosed research and design studio in New York, Adam Harvey aims to raise awareness regarding the rise of the Surveillance Society through an original artistic project that aims to combine privacy and fashion. It involves different items of "anti-drone" clothing created based on a material that avoids detection by the thermal cameras that equip unmanned aircraft. Their inevitably silver-coloured design due to the protective material is undoubtedly reminiscent of the futurist imaginary typical of previous decades.

Off Pocket
Adam Harvey / Undisclosed LCC
$80.00
http://privacygiftshop.com

The Off Pocket is a privacy accessory for smartphones with protection from waves between 500 Mhz and 5 Ghz. It prevents the undesired exchange of information by creating a "Faraday cage" effect, thus avoiding the accidental revelation of any datum or metadatum originating from the signals emitted by Wi-Fi, Bluetooth, or GPS devices or the telephone itself. It works in all countries and for all telephone operators. This accessory is made from a flexible fabric that keeps its weight below 100 grams. It is available in three different sizes and is waterproof. If the price proves to be out of our range, our next best option is the DIY version offered by killyourphone.com, perhaps less glamorous but more authentic and accessible.

Invisible
Biogenfutur
$230.00
http://biogenfutur.es

The Panopticon does not live by electronic surveillance alone. Biogenfutur offers us a solution for all those small trails of saliva, hairs, nails and skin flakes with which we geolocate our presence wherever we go and leave clues to our activities. With just 0.5 nanograms of DNA it is now possible to carry out forensic analysis of our "biogenetic identity card". Thanks to Erase liquid, it is possible to eliminate 99.5% of our DNA trail. By completing the action using Replace, it is possible to create confusion over the remaining 0.5%. Perhaps this seems exaggerated but, in 2013, Heather Dewey-Hagborg managed to create realistic portraits by collecting cigarette ends, hairs, and chewing gum from the streets of New York, through the DNA samples still present.

Blackphone
Silent Circle / Geeksphone
$629.00 - $829.00
https://www.blackphone.ch

If we want a much more practical and operational alternative to Off Pocket, and one that does not prevent us from using the telephone while guaranteeing our privacy, Blackphone offers us a telephone specifically designed to avoid tracking by third parties. It uses an Android version created especially for the occasion, the PrivatOS, and numerous tools for secure and anonymous communication: Silent Phone, Silent Text, Silent Contacts, anonymous search and navigation, and the use of VPN offered by Disconnect; it also offers secure storage on the cloud through SpiderOak, and anti-theft system and the Blackphone Security Center customer service.

Autodefensa 1.0: el sabotaje

Defender nuestra intimidad y nuestros datos no siempre requiere un conocimiento avanzado de tecnologías alternativas. No es necesario saber cómo funciona Tor ni cómo montar un servidor doméstico seguro para desbaratar los planes de quienes construyen modelos de negocio opacos con los datos personales de los demás. De hecho, partiendo de un conocimiento bastante rudimentario de cómo funcionan los mercados secundarios de datos y los mecanismos de creación de perfiles a partir de cálculos algorítmicos, es posible subvertir la mayoría de las esperanzas de monetarización de nuestra actividad cotidiana.

La primera opción de cualquiera que quiera proteger su identidad *online* y *offline*, por lo tanto, es el sabotaje. En las páginas de este manual encontraréis diferentes experiencias de sabotaje, desde los Surveillance Camera Players al CV Dazzle: ejemplos de sabotaje premeditado, organizado y con el objetivo de concienciar.

El sabotaje, sin embargo, también puede ser una estrategia personal y cotidiana, orientada a distorsionar el perfil que pretenden hacer de nosotros las empresas y los prestadores de servicios. Si distorsionamos nuestra identidad digital, el valor de la información recogida y agregada disminuye, y así podemos recuperar un cierto control sobre el proceso.

Sabotaje a redes sociales: La única referencia cierta que es necesario dar a las redes sociales para poder comunicarse con amistades y conocidos es el nombre. Todo lo demás se puede sabotear: fecha de nacimiento, e-mail, estado civil, gustos y preferencias, etc. Puedea jugar con estos sistemas para ver cómo cambia el tipo de anuncios que recibes según si estás soltera o casada, o si tienes 18 o 68 años. ¡Disfruta!

Sabotaje en las tarjetas de cliente: ¿Te resulta tan irresistible ese descuento que te ofrecen que quieres tener la tarjeta de cliente pero no convertirte en un perfil comercial? Muy fácil: identifica qué dato personal es imprescindible para acceder al preciado descuento (si te envían cupones, el e-mail o la dirección postal; si son descuentos en caja, el nombre) y utilízalo, pero distorsiona el resto. Facilitar tu teléfono móvil, por ejemplo, no te aportará ningún descuento y es un dato que a buen seguro estarás regalando a cambio de nada. En muchos casos, el dato personal clave es uno solo y el resto te los puedes inventar sin renunciar a los descuentos.

Sabotaje en el comercio en línea: La lista de nuestras compras en Internet es un bien preciado para las empresas de publicidad y corredores de datos personales, ya que de ella se puede inferir información sobre nuestros deseos futuros. Así, cosas tan sencillas como comprar algún regalo o cosas para otra persona pueden deformar esta fotografía. ¿Un hombre de mediana edad que compra revistas para adolescentes? ¿Una chica que un día compra libros de Corín Tellado y al siguiente las obras completas de Thomas Mann? Los algoritmos, que viven de los perfiles fáciles y sin matices, sudarán la gota gorda. Además, también se puede seleccionar una dirección de entrega que no corresponda a nuestra residencia.

Sabotaje a las cámaras de vigilancia: En los países con más presencia de videovigilancia hace ya tiempo que los jerséis con capucha se han convertido en elemento habitual del vestuario urbano. Las personas que quieren cometer actos delictivos tienden a decantarse por dejarse el casco de la moto puesto. Quizá no sea necesario ir tan lejos, o quizás en el futuro todos iremos con peinados y maquillaje antivigilancia, como sugiere Adam Harvey. O es posible que, como hacen los Surveillance Camera Players, acabemos buscando las cámaras para salir en ellas. De momento, una buena manera de sabotear la videovigilancia consiste en identificar las cámaras y no normalizar los espacios públicos bajo vigilancia.

Sabotaje a la ciudad inteligente: Si los sueños húmedos de parte de la industria de chismes inteligentes se cumplen, la Internet de las cosas y las capacidades de identificación y reidentificación de la infraestructura urbana, sincronizada con los *wearables*, puede hacer que toda nuestra existencia acabe registrada y procesada. Para evitarlo, el sabotaje más obvio consiste en no comprar mecanismos inteligentes que cobran en dinero y en datos (como los televisores inteligentes o los *wearables*), en comprar teléfonos móviles que anonimicen las direcciones MAC y en apagar el detector de redes Wi-Fi que permite la lectura de nuestro dispositivo sin que nos demos cuenta.

De la misma manera que para proteger nuestros datos podemos sabotear sistemas y procesos, el ser conscientes de qué se hace con nuestros datos, cómo se hace y quién lo hace puede llevarnos a gestionar nuestra información de forma responsable y consecuente: cediéndola cuando nos parece procedente y proporcionado, ocultándola o enmascarándola cuando no, e incluso regalándola voluntariamente como una forma de contribución no monetaria a proyectos o productos que nos inspiren simpatía.

El sabotaje como estrategia de autodefensa electrónica, de hecho, combina lo mejor de la conciencia ciudadana (y los derechos relacionados) con las posibilidades del consumo responsable. Y tú, ¿qué has saboteado hoy?

Self-Defence 1.0: sabotage

Defending our privacy and our data does not always require a high degree of knowledge of alternative technologies. It is not necessary to know how Tor works, or how to set up a secure domestic server, in order to disrupt the plans of those who build opaque business models based on personal data. In fact, based on a fairly rudimentary knowledge of how the secondary data markets work, along with the mechanisms for creating profiles based on algorithmic calculations, it is possible to subvert the main expectations of monetisation of our everyday activity.

The first option facing anyone who wants to protect his or her identity online and offline is sabotage. On the pages of this manual, you will find different sabotage experiences, from the Surveillance Camera Players to CV Dazzle – all examples of premeditated, organised sabotage whose aim is to raise awareness.

Sabotage, however, can also be a personal and everyday strategy, aimed at distorting the profile that companies and service providers aim to make of us. If we distort our "data double", the value of the information that they collect and aggregate is reduced, and thus we can recover a certain control over the process.

Sabotage on the social networks: in order to be able to communicate with friends and acquaintances, the only true reference it is necessary to give to the social networks is your name. Everything else is subject to sabotage: date of birth, email address, civil status, tastes and preferences, etc. You can play with these systems, seeing what kind of advertisements you receive depending on whether you claim to be single or married, or that you are 18 or 68 years old. Have fun!

Sabotage on customer loyalty cards: is that discount you are being offered so irresistible, that you want a customer card but do not want to become a commercial profile? Simple: identify which personal data components are essential to access the prized discount (if they send you coupons, it will be your email or street address; if they are discounts for the checkout, your name) and use that personal data while distorting the rest. Providing your mobile telephone number will not earn you any discounts and is a piece of data that you are certainly giving in exchange for nothing, for example. In many cases, the key piece of personal data is only one, and the remainder can be invented without missing out on the discounts.

Sabotage in online commerce: the list of our online purchases is an asset highly valued by advertising companies and data brokers, as information on our future desires can be inferred. Thus, such simple things as purchasing a gift or buying things for somebody else can deform this snapshot. A middle-aged man who buys magazines for teenagers? A young girl buying romantic novels by Corin Tellado one day, and the complete works of Thomas Mann the next? This will make the algorithms, which are based on easy profiles without nuances, sweat buckets. Additionally, we can also select a delivery address that does not coincide with our home address.

Sabotage of security cameras: in the countries with more video surveillance, for some time tops with hoods have become a habitual element of urban clothing. People who want to commit crimes tend to opt for leaving their motorbike helmet on their head. Perhaps it is not necessary to go that far, or perhaps in the future we will all be wearing anti-surveillance hairstyles and make-up, as suggested by Adam Harvey. Alternatively, it is possible that, like the Surveillance Camera Players, we end up searching for cameras to appear on them. At present, however, a good way of sabotaging video surveillance involves identifying the cameras and not normalising those public spaces under surveillance.

Sabotage in the smart city: if the dreams of the smart tales are fulfilled, the Internet of Things and the capacities for the identification and re-identification of the urban infrastructure, synchronised with wearables, may end up ensuring that all our existence is recorded and processed. To avoid this, the most evident sabotage involves not purchasing smart mechanisms that charge in money and data (such as smart television sets and wearables), to purchase mobile telephones that anonymise MAC addresses and to turn off the Wi-Fi networks detector that allows the reading of our device without us realising.

In the same way that in order to protect our data we can sabotage systems and processes, the awareness of what is done with our data, how it is done and who does it, can lead us to manage our details in a responsible and consistent way – providing it when we feel it is advisable and proportionate to do so and hiding it or masking it when not, and even voluntarily giving it as a form of non-monetary contribution to projects or products that inspire sympathy in us.

Sabotage as an electronic defence strategy, in fact, combines the best of citizen's awareness (and related rights) with the possibilities for responsible consumerism. So, what have you sabotaged today?

Guía de herramientas de autodefensa

Para estar viviendo, como dijo Mark Zuckerberg, la era del fin de la privacidad, es sorprendente la cantidad de alternativas a los sistemas y soluciones más habituales para compartir datos *online* que están apareciendo. De las redes sociales al correo electrónico, pasando por los buscadores, los servicios en la nube o la voz por Internet, los últimos años han sido testigos de una eclosión de alternativas a los estándares desarrollados por las grandes empresas, que a menudo crean estos servicios solo como señuelos para conseguir datos («tú eres el producto»). La tabla que reproducimos, orientativa y no exhaustiva ni definitiva, recoge algunas de las alternativas de mayor impacto en ámbitos aún hoy controlados por las grandes corporaciones, así como soluciones que ayudan a cobrar conciencia de cómo se (mal) gestionan los datos personales en el mundo digital. Con niveles diferentes de facilidad de uso, protección de la privacidad e implantación, dibujan un mapa de lo que puede ser el futuro de la autodefensa electrónica: un mundo en que el cliente-producto se afirma como ciudadano y exige tener el control sobre los datos que genera y la información que se deriva de ellos.

Categoría	Descripción/Productos convencionales	Alternativas
Audio/ Vídeo/ VoIP	La extensión en el uso de alternativas a la telefonía convencional a través de servicios de Voz sobre IP (VoIP) no está relacionada con las revelaciones llevadas a cabo por Edward Snowden, las cuales dejaron más que claro que las llamadas telefónicas no están a salvo de ser interceptadas. En realidad, el recurso a programas como Skype (Microsoft), Hangouts (Google) y VoIPbuster (Betamax GmbH & Co KG) tiene que ver con tarifas más competitivas que incluyen servicios similares e incluso ventajas adicionales sin coste (mensajería instantánea, videoconferencia, llamadas entre múltiples usuarios). La alternativa que ofrecen los servicios de VoIP no aporta ninguna garantía de privacidad, sino más bien al contrario. Ya en 2012, Skype fue acusado de cambiar su infraestructura para facilitar la interceptación de las conversaciones entre usuarios. Por eso surgen programas específicos que hacen de la privacidad su bandera y prometen una encriptación de las comunicaciones mucho más meticulosa.	**Jitsi** Aplicación multiplataforma de voz (VoIP), videoconferencias y mensajería instantánea libre y de código abierto para Windows, Linux y Mac OS X con licencia GPL. Admite distintos protocolos populares de mensajería instantánea y telefonía y también permite compartir el escritorio. https://jitsi.org/ **Redphone** Es una aplicación de código abierto con licencia GPL que ofrece llamadas con encriptación de extremo a extremo para usuarios que la tengan instalada a fin de garantizar que nadie más pueda escuchar sus conversaciones. https://whispersystems.org **Tox** Programa que permite realizar videoconferencias, llamadas y mensajería de texto priorizando la privacidad y sin coste añadido ni contenidos publicitarios. http://tox.im
Almacenamiento en la nube	La conjunción entre las crecientes necesidades de almacenamiento y las tendencias en el terreno de la movilidad dio como resultado la llegada de la «nube»: soluciones de almacenamiento remoto fácilmente accesibles desde cualquier dispositivo conectado a la red. Existen verdaderas «granjas» de servidores interconectados destinados simplemente a ofrecer copias de respaldo y servicios de almacenamiento. A día de hoy, servicios como Google Drive, iCloud y Dropbox encabezan las soluciones de almacenamiento en la nube para los usuarios pequeños y medianos. Sin embargo, dejar una copia de nuestra información en manos ajenas, almacenada en lugares desconocidos cuyos marcos legales ignoramos y sin saber quién tiene acceso a ella, no puede ser lo más tranquilizador, sobre todo si se trata de documentos que contienen información confidencial o que revelan secretos al público (y han de ser depositados de forma totalmente anónima). En el caso del servicio ofrecido por Google, uno de los principales riesgos es que el acceso está vinculado al resto de los servicios que ofrece a través de su identificador único de usuario, de modo que, si no se tiene especial cuidado de cerrar la sesión, el acceso a los archivos queda expuesto. La necesidad de servicios de almacenamiento en la nube con una protección especial de la privacidad es una demanda que poco a poco va siendo atendida. Claro que lo más seguro siempre será almacenar los archivos en cualquier dispositivo sin ningún tipo de conexión a la red.	**DocumentCloud** Alternativa a scribd respetuosa con la privacidad. DocumentCloud procesa todos los documentos que se es suban mediante OpenCalais y da acceso a información extensa sobre las personas, los lugares y las organizaciones que se mencionan en dichos documentos. https://www.documentcloud.org/home **SecureDrop** Es una plataforma de software de código abierto para la comunicación segura entre periodistas y fuentes de información (informantes). Originariamente diseñada y desarrollada por Aaron Swartz y Kevin Poulsen con el nombre de *DeadDrop*. https://pressfreedomfoundation.org/securedrop **SpiderOak** Permite almacenar, sincronizar, compartir y acceder privadamente a los propios datos desde cualquier lugar, a partir de un entorno «conocimiento cero». https://spideroak.com/ **Tresorit** Almacenamiento de objetos digitales de valor, accesible desde cualquier lugar y compartible de manera segura. El grado más elevado de encriptación protege todos los aspectos de la gestión de contenidos en la nube. https://tresorit.com
Encriptación de unidades	Aunque un dispositivo de almacenamiento no esté conectado a la red, si lo roban o confiscan podrá ser examinado sin problema en caso de que no cuente con una buena encriptación. Un mecanismo adicional de seguridad consiste en codificar no solo los intercambios de información, sino también la información en sí, disponible en nuestra unidad de almacenamiento local. Los discos duros no vienen por defecto con un sistema de encriptado, por lo que si queremos aumentar la seguridad, tendremos que configurarlo nosotros mismos.	**Bitlocker** Función de encriptación total de unidades incluida en ciertas versiones de Windows, diseñada para proteger datos mediante la encriptación de volúmenes enteros. http://www.microsoft.com/en-us/download/details.aspx?id=7806
Correo electrónico	La mayoría de los particulares utilizan cuentas de correo electrónico basadas en sistemas de correo web, es decir, que confían el acceso, la gestión y el almacenamiento de su correspondencia virtual a grandes empresas que ofrecen dichos servicios: MSN (Microsoft), Gmail (Google), Yahoo!, etc. En tanto que productos gratuitos, la rentabilidad del correo web se basa en la vigilancia anonimizada de carácter comercial, de cara a adaptar la publicidad resultante a las características del usuario. Por otro lado, las prácticas demostradas de espionaje masivo por parte de agencias públicas de inteligencia han mostrado que, si se desea defender la privacidad de las comunicaciones electrónicas, los niveles de seguridad convencionales nunca son suficientes y es necesario ir más allá. Las alternativas requieren claves de encriptación, proyectos de correo web con garantías e incluso direcciones de correo electrónico «desechables».	**Enigmail** Es una extensión de seguridad para Mozilla Thunderbird y Seamonkey. Permite redactar y recibir mensajes de correo electrónico firmados o encriptados con el estándar OpenPGP. https://www.enigmail.net **GnuPG (GPG)** GNU Privacy Guard o GPG es una herramienta de cifrado y firmas digitales, sustituto del sistema PGP (Pretty Good Privacy) con la ventaja de ser software libre con licencia GPL. GPG utiliza el estándar del IETF denominado OpenPGP. https://www.gnupg.org **MailPile** Un proyecto de «correo web» que permite elegir entre utilizar el ordenador propio como servidor, para poder controlar los datos y la privacidad propios, o bien ejecutar MailPile en un ordenador en la nube. https://www.mailpile.is **RiseUp** Un proyecto para crear alternativas democráticas y practicar la autodeterminación mediante la promoción de medios de comunicación seguros. Ofrece correo web respetuoso con la privacidad: tráfico encriptado, ubicación anónima, dirección IP anónima, etc. https://www.riseup.net/
IM (Mensajería instantánea)	La mensajería instantánea permite la comunicación en tiempo real a través de texto y se popularizó hace ya varios años gracias a los clientes ofrecidos por MSN Messenger, ICQ o AIM. A día de hoy, existen decenas de opciones disponibles, algunas de ellas basadas en el protocolo abierto XMPP. El uso del sistema de IM se ha extendido ampliamente a través de terminales móviles. Destacan programas como Line, Hangouts (Google), WhatsApp o Facebook Messenger y se tiende hacia el intercambio multimedia, que completa la comunicación a través de texto con imágenes, sonidos y vídeos. Algunas de estas opciones para comunicarse han mostrado graves vulnerabilidades; sin embargo, no cabe duda de que, en el caso de estas herramientas, quienes más curiosidad muestran por espiarnos son precisamente personas de nuestro entorno: no hay más que echar un rápido vistazo en Internet para comprobar la gran demanda y oferta de herramientas para interceptar conversaciones. Es precisamente en el ámbito de la mensajería instantánea donde ha surgido un amplio abanico de alternativas que aseguran proteger la privacidad del usuario.	**Chatsecure** Es un cliente de chat encriptado libre y de código abierto para iPhone y Android que admite encriptación «Off-the-record» (OTR) por XMPP. https://chatsecure.org **Cryptocat** Una aplicación de código abierto, de software gratuito y accesible, desarrollada por profesionales de la encriptación, que ofrece un chat encriptado en el navegador o en el móvil. Ni siquiera la misma red de Cryptocat puede leer los mensajes. https://crypto.cat **Telegram** Telegram Messenger es un servicio de mensajería multiplataforma con clientes de código abierto. Los usuarios de Telegram pueden intercambiar mensajes, fotos, vídeos y documentos (admite todos los tipos de archivos) encriptados y autodestructibles. https://telegram.org **TextSecure** Encripta los mensajes de texto y de chat con conexión inalámbrica y en el teléfono. Todos los mensajes se encriptan localmente, de modo que si el usuario pierde el teléfono los mensajes no se perderán. https://whispersystems.org/#encrypted_texts
Gestión de contraseñas	Cuando nos advierten de que elijamos una clave segura, no se está exagerando en absoluto. La capacidad para averiguar y predecir contraseñas ha adquirido niveles de sofisticación aterradores. Uno de los mayores errores y riesgos es el de utilizar una mismo *password* para todo o casi todo. SplashData saca cada año su lista de las 25 claves más comunes, que además hacen gala de su inseguridad. En 2013 el ranking estaba encabezado por «password» y «123456». Ante la idea de tener que recordar cientos de nombres de usuario y contraseñas, muchas veces se recurre a un gestor de claves; la fragilidad de centralizar toda la información de acceso en un mismo lugar hace que sea fundamental elegir un gestor en el que podamos confiar. Sin embargo, por muy segura que sea una contraseña, gran parte de la responsabilidad recae en las organizaciones a las que accedemos, ya que se han dado múltiples casos en los que se ha hackeado directamente la base de datos y se ha logrado un acceso masivo a las *passwords* de los usuarios.	**Encrypter** Gestor de contraseñas, almacén de tipo clave-valor y cartera electrónica de código abierto, de «conocimiento cero» y basado en la nube. https://encryptr.crypton.io/ **KeePassX** Guarda una gran diversidad de información –como nombres de usuario, contraseñas, URL, archivos adjuntos y comentarios– en una sola base de datos y ofrece una pequeña utilidad para generar contraseñas seguras. https://www.keepassx.org **LastPass** El galardonado gestor de contraseñas LastPass guarda las contraseñas y proporciona acceso seguro desde cualquier ordenador y dispositivo móvil. https://lastpass.com
Votaciones	Las aplicaciones para la coordinación de eventos y voto electrónico como Doodle pueden desvelar información personal acerca de las preferencias o la disponibilidad de un usuario, manipular sus respuestas e incluso conducir a procesos de reidentificación.	**Dudle** Generador de votaciones que mejora la privacidad. El acceso y la edición están mejor controlados y las votaciones se eliminan automáticamente si no se accede a ellas durante más de tres meses. https://dudle.inf.tu-dresden.de/

Paquete de privacidad

Algunos entornos *online* y sistemas operativos dan cierta sensación de fragilidad en términos de privacidad. La usabilidad, compatibilidad e interoperabilidad que ofrecen (entre programas, servicios, dispositivos, etc.) es posible en muchos casos gracias a la cesión de información personal (total o parcialmente anonimizada). Esta es en gran medida la base para rentabilizar dichas empresas, ya que el pago directo por servicio no es tan atractivo para el consumidor. Ya sea en entornos de Windows, Apple o Android, la idea de ir dejando un rastro informacional puede resultar muy inquietante, por lo que algunos desarrolladores han creado herramientas complejas de acción múltiple que ayudan a contrarrestar al mismo tiempo varios de los problemas aquí planteados, y así no tener que estar pendiente de mantener una larga lista de aplicaciones.

Disconnect Juego de herramientas con navegación privada, búsqueda privada, previsualización de política de privacidad de sitios web, privacidad para niños y conexión inalámbrica segura. https://disconnect.me

Freedome Paquete de seguridad y privacidad para dispositivos móviles: navegación segura, máscara de dirección IP, irrastreabilidad, seguridad Wi-Fi, *antiphishing*, antivirus... http://freedome.f-secure.com

Tails «TheAmnesicIncognitoLiveSystem» es un sistema operativo en directo que puede iniciarse en casi cualquier ordenador a partir de un DVD, una memoria USB o una tarjeta SD. Utiliza la red Tor, no deja rastros en el ordenador y utiliza las últimas herramientas criptográficas para encriptar los archivos, los correos electrónicos y la mensajería instantánea. https://tails.boum.org

Buscador

Mientras que muchos de nuestros correos electrónicos o llamadas pueden resultar aburridos y carentes por completo de interés para los expertos en minería de datos, nuestras búsquedas por Internet a través de motores como Google o Bing (Microsoft) dicen qué nos inquieta o qué buscamos en cada momento: verdadero oro digital. Si resulta ser algo que se pueda vender (ya sea una bicicleta, un remedio para la calvicie o nuestra media naranja), siempre habrá un anunciante deseando saber quiénes son sus potenciales clientes para estamparles un banner que les oriente. Igualmente, si lo que buscamos en los oráculos *online* es comprar amplias cantidades de fertilizante, adquirir una copia del Corán o entrar en un foro en el que compartir nuestro descontento con las autoridades, más bien llamaremos la atención de los servicios de inteligencia y abriremos la posibilidad de ser clasificados como delincuentes potenciales y que la vigilancia a la que nos someten sea aún más intensiva.

DuckDuckGo Pone el acento en la privacidad del usuario que busca evitando los resultados de búsqueda personalizados. Genera los resultados a partir de sitios web clave de participación colectiva, como la Wikipedia, y de partenariados con otros buscadores, como Yandex, Yahoo!, Bing y WolframAlpha. https://duckduckgo.com

Ixquick Es un potente buscador que no compila ni comparte ninguna información personal y ofrece una Guía Telefónica Internacional y acceso a 18 millones de horas de vídeo con su buscador de vídeos. https://ixquick.com

Startpage Buscador anónimo que presenta la misma política de privacidad que Ixquick. No registra la dirección IP del usuario ni rastrea sus búsquedas. Galardonado con el Sello Europeo de Privacidad. https://startpage.com

Red social

Los Servicios de Red Social (SRS) como Facebook, Twitter, Tuenti o MySpace no se pagan con dinero, se pagan con datos. Sin duda, para aprovechar al máximo estos servicios lo mejor es ajustar la identidad virtual a la real (a fin de poder ser encontrado y darse a conocer); esto permite a estas empresas hacer perfiles más ajustados, pero en términos de privacidad los usuarios se exponen a unos niveles de transparencia no siempre deseables. Ante el falso mito de que lo que se exponga en un SRS es información «pública», se puede hacer un uso de dichos entornos limitado a círculos más cercanos, por lo que hablar de privacidad en redes sociales no debería ser ninguna paradoja. Si bien la circulación en una red es más eficiente cuando ha de cruzar el mínimo número de nodos posible, algunas iniciativas pretenden ofrecer SRS menos jerarquizadas, más distribuidas y descentralizadas, libres de vigilancia comercial y sin una «puerta trasera» de acceso para miradas indiscretas.

Diaspora Surge en 2010 como alternativa a Facebook. Ofrece la primera red social gestionada por la comunidad, distribuida, descentralizada y respetuosa con la privacidad, que permite a los usuarios tener el control de sus datos.
https://joindiaspora.com

N-1 Es un «dispositivo tecnopolítico» sin ánimo de lucro que promueve el uso de herramientas libres, desarrolladas y autogestionadas con una ética horizontal y antagonista. Es una de las redes de Lorea, un proyecto que engloba varias redes sociales y aspirar a lograr su federación. También está conectado con Rhizomatik Labs.
https://n-1.cc

Navegación web

https://

La navegación web es la puerta de entrada para el intercambio de un amplio volumen de información *online*. Para su utilización muchas aplicaciones utilizan directamente como interfaz el navegador, el cual almacena infinidad de información que dice muchísimo sobre nosotros: galletas, historial de navegación, marcadores, nombres de usuario y contraseñas, e incluso datos introducidos previamente en formularios. La opción de navegación privada (*private browsing*) no garantiza que no se produzca un rastreo de nuestra sesión. La navegación en sí está llena de riesgos aunque seamos prudentes: pantallazos ilegítimos, *phishing*, *spambots*... Incluso existen troyanos que pueden tomar el control de tu cámara web. El protocolo más común para la navegación segura es el HTTPS, que previene los pinchazos y las interceptaciones (*man-in-the-middle*), pero toda precaución es poca: antivirus, cortafuego, detectores de software malicioso, anonimizadores...

Anonymizer Un proxy que hace de intermediario y de escudo de la privacidad entre un cliente y el resto de Internet. Accede a Internet en nombre del usuario y protege la información personal ocultando la información identificativa del cliente.
http://www.livinginternet.com/i/is_anon_work.htm

Bleachbit Libera memoria caché rápidamente, elimina galletas, borra el historial de navegación, destruye archivos temporales para evitar que puedan recuperarse, elimina registros y descarta basura que no sabíamos que teníamos.
http://bleachbit.sourceforge.net

Do Not Track Es una tecnología y propuesta de política que permite a los usuarios darse de baja voluntariamente del seguimiento de sitios web que no visiten, por ejemplo servicios de analíticas, redes de publicidad y plataformas sociales.
http://www.donottrack.us

HTTPS Everywhere Es una extensión de Firefox, Chrome y Opera que encripta las comunicaciones con muchos sitios web importantes y así hace más segura la navegación. https://www.eff.org/https-everywhere

Maskme Derrota el correo basura, detiene el telemarketing y evita los cobros no deseados y el fraude ofreciendo la posibilidad de enmascarar el correo electrónico, el teléfono y la tarjeta de crédito cuando se navega y se realizan compras por Internet.
https://www.abine.com/maskme/

Privacy Badger Es un complemento del navegador que evita que los anunciantes y otros rastreadores rastreen secretamente qué visita el usuario y qué páginas web mira.
https://www.eff.org/privacybadger

Tor Un navegador web respetuoso con la privacidad muy extendido. Tor es un software libre y una red abierta que ayuda al usuario a defenderse de los análisis de tráfico. https://www.torproject.org

Data doubles

El *data double* es el conjunto de información que vamos dejando o que hemos almacenado a nuestro alrededor, y constituye una segunda imagen incorpórea de nuestra vida. Este «cuerpo» incorpóreo, más comúnmente conocido como «huella digital», está formado por las distintas trazas digitales que vamos dejando como ciudadanos y consumidores. Si bien la existencia de información sobre nosotros fuera de nosotros no es algo nuevo, el *data double* indica la existencia de datos en formato digital, lo cual ha permitido el rápido crecimiento de nuevas maneras de procesar, combinar y analizar dichos datos. Se podría generar un *data double* relativamente completo asociando varios perfiles diferenciados: si se combina el historial de compras por Internet de una persona, su perfil en medios sociales y los datos de seguimiento de su geolocalización, se puede obtener un retrato de su vida bastante denso.

Se trata de consecuencias casi inevitables en una era digital, y el uso (y abuso) de *data doubles* –que no siempre son representaciones precisas del individuo– está muy extendido. Uno de los usos más frecuentes que tienen los *data doubles* es la categorización. Algunas aplicaciones de la categorización permiten unas prácticas relativamente inofensivas, como adaptar la publicidad de los medios sociales a los gustos y costumbres de los usuarios. Sin embargo, a causa de la asociación de los *data doubles* con la autenticidad –los datos «no mienten»–, esta información personal ha permitido una serie de formas más perniciosas de clasificación social. Los registros de nombres de pasajeros generados por las compañías aéreas, ahora compartidos en el ámbito internacional, se pueden utilizar potencialmente para crear un perfil completo de un pasajero a partir de la información de los vuelos e incluso de la elección del menú, y partiendo de esta información pueden tomarse decisiones sobre la fiabilidad de los viajeros. Asimismo, ante el gran interés de las compañías de seguros por comprar a la policía los datos de seguimiento de las matrículas de los vehículos para afinar las primas que cobran, y ante los métodos de puntuación de riesgo que se aplican cada vez más en el control de las fronteras y en las herramientas de reputación en Internet, el uso de *data doubles* puede tener efectos muy concretos en nuestra vida cotidiana de una manera que no siempre podemos controlar, o bien puede llegar a afianzar las desigualdades sociales.

La creciente confianza depositada en los *data doubles* proviene de la fe en la veracidad de los datos, pero la inexactitud potencial de estos puede tener consecuencias sociales nocivas. El retrato que se genera cuando se agregan bits de información de nuestras actividades digitales cotidianas a menudo es una caricatura de la persona en cuestión. Uno de los mejores ejemplos de ello lo hallamos cuando, en caso de robo de identidad, la solvencia de un individuo puede no reflejar su trayectoria vital real. La confianza que depositada en los *data doubles* también modifica la relación entre los ciudadanos y el Estado: los estados recorren cada vez más a los datos y se vuelven más desconfiados, de modo que las personas son tratadas como puntos de datos potencialmente sospechosos más que como ciudadanos.

Guide to Digital Detoxification

Considering that we are living in what Mark Zuckerberg has called the age when privacy is over, there are a surprising number of alternatives developing in the most common systems and solutions for sharing data online. From the social networks to email, and passing through search engines, services in the cloud or voice over Internet, in recent years we are witnessing the emergence of alternatives to the standards developed by large companies, which often create these services simply as bait for getting hold of data ("the product is you"). The table that we reproduce below, that does not aim to be exhaustive nor definitive, but illustrative, includes some of the alternatives with the greatest impact in spheres still controlled today by those large corporations, as well as solutions that help to raise awareness of how personal data are (mis)managed in the digital world. With different levels of user-friendliness, privacy protection, and implementation, they sketch a map of what could be the future of electronic self-defence: a world in which the client-product is affirmed as a citizen and demands control over the data he or she generates and the information deriving from them.

Category	Description/Conventional products	Alternatives
Audio/ Video/ VoIP	The spread of the use of alternatives to conventional telephone services through Voice over IP (VoIP) services is not related with the revelations made by Edward Snowden, which made it even clearer that telephone calls are not safe from being intercepted. In reality, resorting to programmes such as *Skype* (Microsoft), *Hangouts* (Google) and VoIPbuster (Betamax GmbH & Co KG) is related with more competitive tariffs that include similar services and even additional benefits without cost (instant messaging, video-conferencing, party calls, etc.). The alternative offered by VoIP services offers not guarantee of privacy, rather to the contrary. Already in 2012, Skype was accused of changing its infrastructure to facilitate the intercepting of conversations between users. It is for this reason that specific programmes emerge that make privacy their flag by promising a much more meticulous encryption of communications.	**Jitsi** Free and open-source multiplatform voice (VoIP), videoconferencing and IM application for Windows, Linux and Mac OS X with LPG license. It supports several popular instant-messaging and telephony protocols and also allows desktop sharing. https://jitsi.org/ **Redphone** Open-source application with GPL license that provides end-to-end encryption calls for users who have this app installed, securing their conversations so that nobody can listen in. https://whispersystems.org **Tox** Program that offers users video-conferencing, calls and text messaging, prioritising privacy and without added cost or advertising contents. http://tox.im
Cloud storage	The combination of growing needs for storage and tendencies in the area of mobility led to the arrival of the "cloud": remote storage solutions that are easily accessible from any device connected to the Internet. There are true "farms" of interconnected servers that are designed simply to offer back-up copies and storage services. Today, services such as *Google Drive, iCloud* and *Dropbox* head up cloud storage solutions for small and medium-sized users. However, leaving a copy of our information in the hands of others, without knowing who has access and it being stored in unknown places whose legal frameworks we ignore, cannot give us the greatest peace of mind. Above all, if we are talking about documents that contain sensitive information or that reveal secrets to the public (and have to be deposited in a 100% anonymous way). In the case of the service offered by Google, one of the main risks is that the access is linked with the rest of the services through a unique user identifier, exposing access to files if one is does not take special care to close the session. The need for cloud storage services with special privacy protection is a demand that is gradually being attended. Of course, the most secure option will always be to store the files in a device without any kind of connection to the Internet.	**DocumentCloud** Privacy-friendly alternative to Scribd. *DocumentCloud* runs every document you upload through *OpenCalais,* giving you access to extensive information about the people, places and organizations mentioned in each. https://www.documentcloud.org/home **SecureDrop** Open-source software platform for secure communication between journalists and sources (whistleblowers). It was originally designed and developed by Aaron Swartz and Kevin Poulsen under the name *DeadDrop*. https://pressfreedomfoundation.org/securedrop **SpiderOak** Makes it possible for you to privately store, sync, share & access your data from everywhere, based on a "Zero-knowledge" environment. https://spideroak.com/ **Tresorit** Storage for digital valuables, anywhere accessible, safely shareable. Highest-grade encryption protects every aspect of the content management in the cloud. https://tresorit.com
Drive Encryption	Even if a storage device is not connected to the Internet, if it is robbed or confiscated it can be examined without any problem if it does not have good encryption. An additional security mechanism consists of codifying, not only information exchanges, but also the information in itself, available on our local storage unit. Hard disks do not come with an encryption system by default, therefore if we want to increase security, we will have to configure it ourselves.	**Bitlocker** Full disk encryption feature included with the certain versions of Windows, designed to protect data by providing encryption for entire volumes. http://www.microsoft.com/en-us/download/details.aspx?id=7806
E-mail	The majority of private individuals use email accounts based on webmail systems, in other words, the access, management and storage of our virtual correspondence is entrusted to large corporations that offer said services: *MSN (Microsoft), Gmail (Google), Yahoo!,* etc. In so far as they are free products, the profitability of webmail is based on anonymised surveillance of a commercial nature, with regard to adapting the resulting advertising according to the users' characteristics. Furthermore, evidence on mass espionage by public intelligence agencies have shown that if we wish to defend the privacy of electronic communications, conventional security levels are never sufficient and it is necessary to go further. The alternatives include encryption keys, projects offering webmail with guarantees and even "disposable" email addresses.	**Enigmail** Security extension to Mozilla Thunderbird and SeaMonkey. It enables you to write and receive email messages signed and/or encrypted with the OpenPGP standard. https://www.enigmail.net **GnuPG (GPG)** Gnu Privacy Guard or GPG is a tool for encryption and digital signatures, a substitute for the PGP (Pretty Good Privacy) system with the advantage of being free software licenced under GPL. GPG uses the IETF standard known as OpenPGP. https://www.gnupg.org **MailPile** "Webmail" project that allows you to choose between using your own computer as server, so you have control over your data and your privacy, or running MailPile on a computer in the cloud. https://www.mailpile.is **RiseUp** Project to create democratic alternatives and practice self-determination by promoting secure means of communication. It offers privacy-friendly webmail: encrypted traffic, location anonymity, IP anonymity, etc. https://www.riseup.net/
IM (Instant Messaging)	Instant messaging offers communication in real time through text and was popularised several years ago thanks to the clients offered by *MSN Messenger, ICQ,* and *AIM*. Today there are dozens of options available, some based on the XMPP open protocol. The IM system has widely spread its use through mobile terminals, prominently with programs such as *Line, Hangouts (Google), WhatsApp, Facebook Messenger,* and tending towards multimedia exchanges, which completes the communication with images, sounds, and videos. Some of these options for communication have shown serious vulnerabilities. However there can be no doubt that in the case of these tools, those who show most curiosity in spying on us, are precisely people from our environment: one only has to take a glance at the Internet to see the great demand for and supply of tools for intercepting conversations. In the area of instant messaging is precisely where a great range of alternatives has emerged that affirm the protection of user privacy.	**Chatsecure** Free and open-source encrypted chat client for iPhone and Android that supports "Off-the-record" (OTR) encryption over XMPP. https://chatsecure.org **Cryptocat** Open-source, freeware, accessible app developed by encryption professionals that offers encrypted chat in the browser or the mobile phone. Even the Cryptocat network itself can't read your messages. https://crypto.cat **Telegram** Telegram Messenger is a cross-platform messenger whose clients are open-source. Telegram users can exchange encrypted and self-destructing messages, photos, videos and documents (all file types are supported). https://telegram.org **TextSecure** Encrypts your text and chat messages over the air and on your phone. All messages are encrypted locally, so if your phone is lost, your messages will be safe. https://whispersystems.org/#encrypted_texts
Password management	When we are warned to choose a secure password, it is absolutely no exaggeration. The capacity to discover and predict passwords has acquired terrifying levels of sophistication. One of the greatest errors and risks is that of using a single password for everything or almost everything. *SplashData* publishes each year its list of the 25 most common passwords, also showing their lack of security. In 2013, the ranking was headed by "password" and "123456". Faced with the idea of having to remember hundreds of user names and passwords, often people resort to using a password manager; the fragility of centralising all access information in a single place makes it fundamental to choose a manager in which we can trust. But, however secure a password may be, a large part of the responsibility lies with the organisations that we access, as there have been numerous cases where databases have been hacked and access gained to user passwords on a massive scale.	**Encrypter** Open-source, "Zero-Knowledge", cloud-based password manager, key/value store and e-wallet. https://encryptr.crypton.io/ **KeePassX** Saves many different pieces of information e.g. user names, passwords, urls, attachments and comments in one single database and offers a basic utility for secure password generation. https://www.keepassx.org **LastPass** Award-winning password manager, it saves your passwords and gives you secure access from every computer and mobile device. https://lastpass.com
Polls	Applications for the coordination of events and electronic polls such as Doodle may reveal personal information regarding a user's preferences or availability, manipulate their responses, and even lead to processes of re-identification.	**Dudle** Privacy-enhanced poll generator. Access and edit is better controlled and polls are deleted automatically if they are not accessed for more than 3 months. https://dudle.inf.tu-dresden.de/

Privacy Pack

Some online environments and operating systems give a certain sensation of fragility in terms of privacy. The usability, compatibility, and interoperability that they offer (between programs, services, devices, etc.) are possible in many cases thanks to transfer of personal information (totally or partially anonymised). This is largely the basis for making a profit from such undertakings, as direct payment for the service is not as attractive for the consumer. Whether in *Windows, Apple* or *Android* environments, the idea of leaving an information trail can be very concerning, therefore some developers have created complex multiple action tools that help to counteract the at the same time several of the problems raised here, and thus not have to keep an eye on maintaining a long list of applications.

Disconnect Toolkit with private browsing, private search, website's privacy policy preview, kids privacy and secure wireless. https://disconnect.me

Freedome Security and privacy pack for mobile devices: Safe Browsing, IP-mask, untraceability, WiFi Security, anti-phishing, anti-virus… http://freedome.f-secure.com

Tails "TheAmnesicIncognitoLiveSystem" is a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It uses the Tor network, leaves no trace on the computer, and uses state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging. https://tails.boum.org

Search engine

While many of our emails or calls may turn out to be boring and completely lacking in interest for data mining experts, our Internet searches using engines such as *Google* or *Bing (Microsoft)* say what we are concerned about or searching for at any time: true digital gold. If it turns out to be something that can be sold (whether a bicycle, a cure for baldness or a partner), there will always be an advertiser wanting to know who his potential customers are to brandish a banner to guide them. Equally, if what we are searching for in the online oracles is to purchase large quantities of fertiliser, a copy of the Quran or a forum in which to share our unhappiness towards the authorities, we may rather attract the intention of the intelligence services, opening up the possibility of our being classified as potential delinquents and the surveillance to which we are subjected will be even more intensive.

DuckDuckGo Emphasizes searchers' privacy avoiding personalized search results. It generates its results from key crowdsourced sites such as Wikipedia and from partnerships with other search engines like Yandex, Yahoo!, Bing and Wolfram-Alpha. https://duckduckgo.com

Ixquick Powerful search engine that does not collect or share any personal information and offers an International Phone Directory and access to 18 million hours of video with Ixquick's Video Search. https://ixquick.com

Startpage Anonymous search engine that shares the same privacy policy as Ixquick. It does not record your IP address or track your searches. Awarded the European Privacy Seal. https://startpage.com

Social networking

The Social Networking Services (SNS) such as *Facebook, Twitter, Tuenti* and *MySpace* are not paid for with money, but with data. Undoubtedly, to make the best use of these services the best course of action is to adjust one's virtual identity with one's real identity (in order to be found and make oneself known); this allows these companies to produce better adjusted profiles, but in terms of privacy, users are exposed to levels of transparency that are not always desirable. Before the false myth that what is exposed on social network services is "public" information, use can be made of these environments that is limited to one's closest circles, therefore talking about privacy on the social networks should not be a paradox. Although circulation on a network is more efficient when the minimum number of nodes possible have to be crossed, some initiatives aim to offer less hierarchized, more distributed and decentralised SNSs, free of commercial surveillance and without a "back door" offering access to prying eyes.

Diaspora Emerged in 2010 as an alternative to Facebook. It offers the first community-run, distributed, decentralized and privacy-aware social network which puts users in control of their data.
https://joindiaspora.com

N-1 Non-profit "techno-political device" that promotes the use of free tools, developed and self-managed from a horizontal and antagonistic ethic. It is one of the networks of Lorea, a project that encompasses several social networks and pursues their federation, also linked with Rhizomatik Labs.
https://n-1.cc

Web navigation

Web navigation is the entrance door to the exchange of a broad volume of online information. Many applications use the browser directly as an interface for their use, and it stores an infinite amount of information that says a great deal about us: cookies, browsing history, bookmarks, user names and passwords, and even data previously entered on forms. The private browsing option does not guarantee that no tracking of our session will take place. Browsing in itself is full of risks even if we are careful: illegitimate screen captures, phishing, spambots… there are even Trojans that can take control of your webcam. The most common protocol for secure navigation is HTTPS, which prevents bugs and "man-in-the-middle" attacks, but every precaution must be taken: antivirus, firewall, malware detectors, anonymizers, etc.

Anonymizer Proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information.
http://www.livinginternet.com/i/is_anon_work.htm

Bleachbit Quickly frees your cache, deletes cookies, clears Internet history, shreds temporary files to prevent recovery, deletes logs, and discards junk you didn't know was there.
http://bleachbit.sourceforge.net

Do Not Track Technology and policy proposal that enables users to opt out of tracking by websites they do not visit, including analytics services, advertising networks, and social platforms.
http://www.donottrack.us

HTTPS Everywhere Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. https://www.eff.org/https-everywhere

Maskme Beats spam, stops telemarketing and prevents unwanted charges and fraud by offering you to mask your email, phone, and credit card as you browse and shop on the web.
https://www.abine.com/maskme/

Privacy Badger Browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web. https://www.eff.org/privacybadger

Tor Widespread privacy-friendly web browser. Tor is free software and an open network that helps you defend against traffic analysis. https://www.torproject.org

Data doubles

"Data doubles" are the collection of information we leave behind, or have stored about us, which amount to a second, non-bodily image of our lives. This non-corporeal "body" of sorts, more commonly known as a "digital footprint", consists of the collection of all the different digital traces we leave behind as citizens and consumers. While the existence of information about us outside ourselves is nothing new, the data double hints at the existence of data in digital form, which has allowed the rapid growth of new ways to process, combine, and analyse this data. A relatively fully-formed data double could be composed by the association of a few discrete profiles: combining one's online purchase history, social media profile, and mobile location tracking data can yield a dense picture of one's life.

These are almost inevitable by-products of a digital age, and the use (and abuse) of data doubles – which are not always accurate representations of the self – is widespread. One of the most frequent uses of data doubles is for categorization. Some applications of categorization enable relatively harmless practices, such as advertising on social media tailored to users' tastes and habits. However, because of the association of data doubles with authenticity – data "doesn't lie" – such personal information has enabled a range of more pernicious forms of social sorting. Passenger name records generated by airlines, which are now shared internationally, can potentially be used to create a complete profile of a passenger based on flight information and even meal choice, and decisions about the trustworthiness of travellers can be derived from such information. Also, with insurance companies keen to buy individuals' registration plate tracking data from police to fine-tune the premiums they charge, and with risk-scoring methods increasingly applied for border control and online reputation tools, the use of data doubles can have very specific impacts on our daily lives in ways that we can't always control, or can potentially entrench social inequalities.

The growing reliance on data doubles comes from faith in the veracity of data, but the potential for *inaccuracy* in this data can lead to damaging social outcomes. The image that is produced when aggregating bits of information from our daily digital activities is often a caricature of the self. One of the best examples of this is how one's creditworthiness, in the case of identity theft, may not reflect one's real-life trajectory. The reliance on data doubles also reshapes the relationship between citizens and the state. But with states turning to data, and away from trust, people are recast as potentially suspicious data points rather than as citizens.

Cosas que se han dicho

Citas destacables sobre la vida en las cuevas de la vigilancia

«Un informe de la Cámara de los Lores de 2009 describía la explosión de las tecnologías de vigilancia como uno de los cambios más importantes que se han producido en Gran Bretaña desde la Segunda Guerra Mundial. [...] Este fenómeno se ha considerado un precio aceptable a cambio de una mayor seguridad, pero los estudios sobre tecnología de vigilancia no respaldan ese argumento.

Un análisis de 44 estudios independientes de cámaras de seguridad, publicado en el mismo año que el informe de la Cámara de los Lores, demostraba que los más de quinientos millones de libras esterlinas [unos 630 millones de euros] invertidos en cámaras de seguridad en Gran Bretaña en la década anterior a 2006 habían producido beneficios modestos. La conclusión más demoledora del informe fue que en la aplicación en la que más eficaces resultaban las cámaras de seguridad —para evitar delitos en los aparcamientos públicos— era posible obtener los mismos resultados simplemente mejorando la iluminación de las zonas de estacionamiento.»

James Bridle
Artista, escritor e investigador
Matter, «How Britain Exported Next Generation Surveillance»
https://medium.com/matter-archive/how-britain-exported-next-generation-surveillance-d15b5801b79e

«Resulta difícil explicar al público general lo poco que funciona la tecnología, hasta qué punto la infraestructura de nuestras vidas se sostiene con el equivalente informático de la cinta adhesiva.

Los ordenadores y la informática ya no funcionan. [...]

Cada vez que descargamos una actualización de seguridad, lo que estamos actualizando lleva no se sabe cuánto tiempo estropeado, siendo vulnerable. A veces días, a veces años. Y nadie publicita esa parte de las actualizaciones. Se dice: "Debe instalar esto, es un parche esencial", pero no que es así "porque los desarrolladores la cagaron de tal manera que es probable que en este mismo momento unos críos adictos al caballo estén vendiendo las identidades de sus hijos a la mafia estonia".»

Quinn Norton
Periodista y escritora especializada en tecnología
«Everything is Broken», *Medium*
https://medium.com/message/81e5f33a24e1

«Los teléfonos móviles son dispositivos de localización que también hacen llamadas telefónicas. Triste, pero cierto. Aunque tenga una serie de herramientas seguras en el teléfono, no por ello el aparato deja de registrar todos sus pasos. Y la policía podría instalar en él actualizaciones para transformarlo en un micrófono, convirtiéndolo así en una especie de puerta trasera, y hacer otras cosas por el estilo.

La policía puede identificar a todos los participantes en una manifestación por medio de un dispositivo llamado *IMSI catcher*. Es como una antena de telefonía falsa que se puede fabricar por 1500 dólares (unos 1150 euros). Todos los teléfonos móviles que están cerca se conectan automáticamente a esa torre y, si el identificador exclusivo del teléfono queda expuesto, la policía no tiene más que acudir a la empresa de telefonía y solicitar la información del usuario.»

Jacob Applebaum
Hacker y periodista
«Leave Your Cellphone at Home», *n+1 Magazine*
https://nplusonemag.com/online-only/online-only/leave-your-cellphone-at-home/

«Todo lo que hacemos hoy en día pasa por Internet.Todo lo que hagamos mañana necesitará Internet. Si vive cerca de una central nuclear, si vuela en aviones, si viaja en coche o en tren, o si tiene un marcapasos, dinero en el banco o un teléfono móvil, su seguridad y su bienestar dependen de que la seguridad de las redes sea sólida y evolucione continuamente.

Esto es lo más alarmante de las revelaciones de Snowden: no solo que los espías nos espían a todos, sino que toda nuestra infraestructura tecnológica está sometida a un sabotaje activo para garantizar que ese espionaje pueda continuar.
No hay forma de reducir la seguridad de manera que sea posible espiar a "los malos" sin que, al mismo tiempo, todos resultemos vulnerables a "los malos".»

Cory Doctorow
Escritor
«If GCHQ wants to improve national security it must fix our technology», *The Guardian*
http://www.theguardian.com/technology/2014/mar/11/gchq-national-security-technology

«Una consecuencia indeseada de todas estas nuevas tecnologías de vigilancia es que la labor periodística resulta inmensamente más difícil que antes. Los periodistas tienen que poner especial atención a cualquier tipo de señal de red, a cualquier tipo de conexión, a cualquier tipo de dispositivo de lectura de matrículas de coches que se encuentre en su ruta hasta el punto de encuentro, a cualquier lugar en el que utilicen la tarjeta de crédito o al que lleven el teléfono móvil, a cualquier contacto de correo electrónico que tengan con la fuente, porque incluso el primer contacto que se produzca, antes de que se establezca la comunicación por un medio encriptado, es suficiente para echarlo todo a perder.

Los periodistas tienen que cerciorarse de no cometer ningún error desde el principio hasta el fin de sus relaciones con las fuentes para no poner en peligro a estas personas. Lo mismo les ocurre a los abogados. Y a los investigadores. Y a los médicos.»

Edward Snowden
Antiguo analista de inteligencia e informante
Entrevista de Alan Rusbridger, *The Guardian*
http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript

«No es suficiente con encriptarlo todo. Además de ser muy complicado, tampoco sería suficiente. Pero, además de cifrarlo todo, hay otras cosas que podemos hacer. La descentralización total sería un gran cambio.

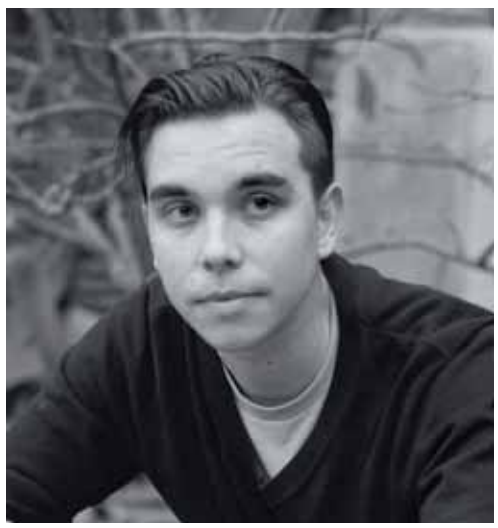
Uno de los motivos por los que la NSA [la Agencia de Seguridad Nacional de Estados Unidos] se ha salido con la suya puede resumirse en la siguiente afirmación: "si no podemos saltarnos sus sistemas de seguridad o si nos va a causar demasiados problemas pincharle las comunicaciones, nos presentamos con una carta y tendrá que hacer lo que le ordenemos". Esto también puede ocurrir en muchos otros sitios. No tenemos mucha información sobre quién más está intentando obligar a las empresas a hacer esas cosas, pero yo aseguraría que si la NSA lo está haciendo, no es la única ni mucho menos.

[...] Se acabó, ya no podemos fiarnos de los servicios centralizados, esa es la realidad; es imposible crear una Internet libre si está centralizada.»

Eleanor Saitta
Experta en seguridad informática
«Ethics and Power in the Long War», *NoisySquare*
https://noisysquare.com/ethics-and-power-in-the-long-war-eleanor-saitta-dymaxion/

«Si cree que sus problemas de seguridad se pueden solucionar con la tecnología es que no comprende ni sus problemas ni la tecnología.»

Bruce Schneier
Criptógrafo y experto en seguridad informática
Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons, 2000



→ James Bridle
Quinn Norton

This is how you should think about the News on Life in the Surveillance Wars

↑ Jacob Applebaum
Cory Doctorow

In 2009, a House of Lords report described the explosion of surveillance technologies as one of the most significant changes in Britain since the Second World War. […]. It has been contended that this is an acceptable price to pay for greater security, but studies of surveillance technology fail to support that argument.

One review of 44 separate CCTV studies, published the same year as the House of Lords report, showed that the more than £500 million ($780 million) spent on CCTV in Britain in the decade up to 2006 had produced only modest benefits. The report's most damning conclusion found that where CCTV was at its most effective – preventing vehicle crime in car parks – the same results could be achieved simply by improving lighting in the parking area.

James Bridle
Artist, writer and researcher
"How Britain Exported Next Generation Surveillance", *Matter*
https://medium.com/matter-archive/how-britain-exported-next-generation-surveillance-d15b5801b79e

It's hard to explain to regular people how much technology barely works, how much the infrastructure of our lives is held together by the IT equivalent of baling wire.

Computers, and computing, are broken. […]

Every time you get a security update, whatever is getting updated has been broken, lying there vulnerable, for who-knows-how-long. Sometimes days, sometimes years. Nobody really advertises that part of updates. People say "You should apply this, it's a critical patch!" and leave off the "…because the developers fucked up so badly, your children's identities are probably being sold to the Estonian Mafia by smack-addicted script kiddies right now."

Quinn Norton
Technology writer and journalist
"Everything is Broken", *Medium*
https://medium.com/message/81e5f33a24e1

Cell phones are tracking devices that make phone calls. It's sad, but it's true. You can have a secure set of tools on your phone, but it doesn't change the fact that your phone tracks everywhere you go. And the police can potentially push updates onto your phone that backdoor it and allow it to be turned into a microphone remotely, and do other stuff like that.

The police can identify everybody at a protest by bringing in a device called an IMSI catcher. It's a fake cell phone tower that can be built for 1500 bucks. And once nearby, everybody's cell phones will automatically jump onto the tower, and if the phone's unique identifier is exposed, all the police have to do is go to the phone company and ask for their information.

Jacob Applebaum
Hacker and journalist
"Leave Your Cellphone at Home", *n+1 Magazine*
https://nplusonemag.com/online-only/online-only/leave-your-cellphone-at-home/

Everything we do today involves the internet. Everything we do tomorrow will require the internet. If you live near a nuclear power plant, fly in airplanes, ride in cars or trains, have an implanted pacemaker, keep money in the bank, or carry a phone, your safety and well-being depend on a robust, evolving, practice of network security.

This is the most alarming part of the Snowden revelations: not just that spies are spying on all of us, but that they are actively sabotaging all of our technical infrastructure to ensure that they can continue to spy on us.

There is no way to weaken security in a way that makes it possible to spy on "bad guys" without making all of us vulnerable to bad guys, too.

Cory Doctorow
Writer
"If GCHQ wants to improve national security it must fix our technology", *The Guardian*
http://www.theguardian.com/technology/2014/mar/11/gchq-national-security-technology

An unfortunate side effect of the development of all these new surveillance technologies is that the work of journalism has become immeasurably harder than it ever has been in the past. Journalists have to be particularly conscious about any sort of network signalling, any sort of connection, any sort of licence plate reading device that they pass on their way to a meeting point, any place they use their credit card, any place they take their phone, any email contact they have with the source because that very first contact, before encrypted communications are established, is enough to give it all away.

Journalists have to be sure that they make no mistakes at all from the very beginning to the very end of a source relationship or they're placing people actively at risk. Lawyers are in the same position. And investigators. And doctors.

Edward Snowden
Former intelligence analyst and whistleblower
Interview by Alan Rusbridger, *The Guardian*
http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript

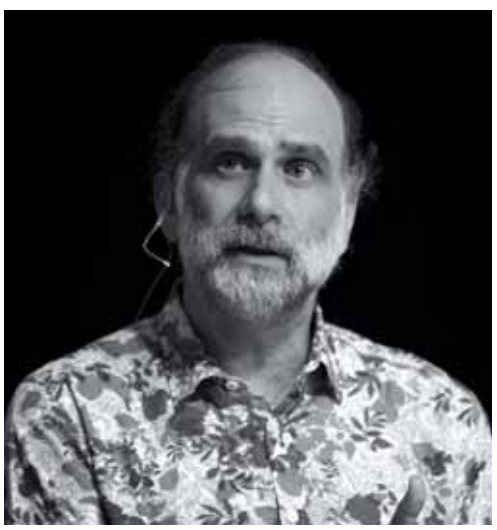
Encrypting all the things isn't enough. Encrypting all the things will be hard, but it isn't actually enough. However, there are things that we can do that will actually make a difference in addition to encrypting all the things. If we start decentralizing all the things, that makes a real difference.

One of the reasons why NSA has been so successful is that, "well, if we can't break your security or if it's going to be too inconvenient to tap this on the wire, we just show up with a letter and now you have to do what we say." There are lots of other places where this can happen too, we don't know that much about who else is trying to compel companies to do that, but I would guarantee that if NSA is doing it, then lots of other people are doing it as well.

[…] It's over, we need to stop relying on central services, we just can't do it anymore, it's impossible to build a free internet that is centralized.

↓ Edward Snowden

↓ Eleanor Saitta
Bruce Schneier



Eleanor Saitta
Computer security expert
"Ethics and Power in the Long War",
NoisySquare
https://noisysquare.com/ethics-and-power-in-the-long-war-eleanor-saitta-dymaxion/

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

Bruce Schneier
Cryptographer and computer security expert
Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons, 2000

Exposición / Exhibition «Big Bang Data»

© Gunnar Knechtel Photography

Exposición «Big Bang Data»

El Centro de Cultura Contemporánea de Barcelona (CCCB) presenta «Big Bang Data», una exposición sobre la emergencia de los datos y sus efectos culturales, políticos y artísticos comisariada por José Luis de Vicente y Olga Subirós.

La exposición trata varias dimensiones de los actuales discursos y estrategias centrados en los datos: desde el emergente y discutido paradigma científico del Big Data hasta la instrumentalización del mundo y la multiplicación de los dispositivos de detección, pasando por la mercantilización de la identidad en los medios sociales y las industrias del *quantified self*. La exposición también aborda la cultura de la vigilancia en el mundo post-Snowden y los riesgos de una política y una ética cuantitativas, gobernadas por los datos.

«Big Bang Data» ofrece una amplia exploración de este campo cultural combinando el arte contemporáneo y proyectos de diseño, documentación histórica, vídeos de entrevistas y prototipos de nuevas tecnologías y servicios, e incluye también un laboratorio activo que aloja proyectos y actividades participativas todos los días de la exposición.

La nómina de artistas y diseñadores participantes incluye, entre otros muchos nombres, los de Mark Lombardi, Diller and Scofidio, David Bowen, Ingo Gunther, Aaron Koblin, Fernanda Viegas y Paolo Cirio.

Esta publicación, *Anonimízate. Manual de protección electrónica*, ofrece un conjunto de recomendaciones, herramientas y prácticas para preservar nuestro sentido de la privacidad en el mundo post-Snowden.

La exposición se presenta en el CCCB entre el 9 de mayo y el 16 noviembre de 2014. En 2015 itinerará a la Fundación Telefónica de Madrid, antes de embarcarse en una gira internacional.

Exhibition «Big Bang Data»

The Centre de Cultura Contemporània de Barcelona (CCCB) presents "Big Bang Data": an exhibition on the Data Explosion and its cultural, political and artistic consequences, curated by José Luis de Vicente and Olga Subirós.

The exhibition touches on numerous aspects of data-centric discourses and strategies today: from the emerging and contested scientific paradigm of Big Data, to the instrumentation of the world and the multiplication of sensing devices, through the commodification of the self in the social media and quantified self industries. The exhibition also deals with the culture of surveillance in the world post-Snowden world and with the risks of quantitative, data driven politics and ethics.

"Big Bang Data" offers a wide exploration of this cultural field combining contemporary art and design projects, historical documentation, video interviews and prototypes for new technologies and services, as well as including a full active laboratory that hosts participatory projects and activities every single day of the exhibition run.

Artists and designers participating include among many others names like Mark Lombardi, Diller and Scofidio, David Bowen, Ingo Gunther, Aaron Koblin, Fernanda Viegas and Paolo Cirio.

This current issue *Anonymise Yourself-Electronic Self-Defence Handbook* offers a set of recommendations, tools, and practices to preserve our sense of privacy in the post-Snowden world.

The show has been presented at CCCB between 9 May and 16 November 2014. In 2015 it will also travel to Madrid's Telefónica Foundation, followed by an international tour.

Dirección y coordinación del proyecto / *Project direction and coordination*
Servicio de Exposiciones del CCCB
CCCB Exhibitions Service

Comisariado / *Curatorship*
José Luis de Vicente
Olga Subirós

Dirección de las actividades
Activities direction
ZZINC

Anonimízate.
Manual de autodefensa electrónica
Anonymise Yourself. Electronic Self-Defence Handbook

Dirección / *Direction*
José Luis de Vicente
Gemma Galdón

Textos / *Texts*
José Luis de Vicente
[www.zzzinc.net]
Gemma Galdon Clavell
[eticasconsulting.com]
Philippe M. Frowd
[eticasconsulting.com]
José María Zavala
[eticasconsulting.com]

Idea y realización de la infografía / *Idea and production of infographics*
Olga Subirós

Diseño gráfico y maquetación / *Graphic design and layout*
David Torrents
Silvia Míguez

Coordinación y edición de textos / *Text editing and coordination*
Marina Palà
Rosa Puig

Traducción y corrección
Translation and proofreading
Marc Jiménez Buzzi
Bernat Pujadas
Blanca Rodríguez
Debbie Smirthwaite

D.L. B 20599-2014

FOTO: Ingo Günther, *WorldProcessor* © 1989 - 2014 Courtesy IngoGunther.com & NovaRico.com

EXPOSICIÓN

BIG BANG DATA

Del 14 de marzo al 24 de mayo de 2015

Espacio Fundación Telefónica
Fuencarral 3, Madrid

espacio.fundaciontelefonica.com
Despertando ideas se despierta el futuro

Telefónica FUNDACIÓN

Coproducida con:
CCCB Centre de Cultura Contemporània de Barcelona

Colaborador tecnológico:
LG Life's Good