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

Anonimitza't
Anonymise Yourself

Manual d'autodefensa electrònica
Electronic Self-Defence Handbook

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

iQEcBAEBAgAGBQJT+e3IAAoJEC4eInvETsq7IMkIAJ2ifrpwPO6ijHmsqWkXPczy
EDp3s98oQ8oIVVWn/IxBHDwKiJ+fpFFdG22agvNdLkyRVHPEIq0CfKXIceXXtkGI
yY9GqyLO19bt7wzu74+4iHqeVxjry4IXPIBkQhQ1VUSvELk9emAXnE6I7tYkHtEf
tSteY2chXVp3DtMHp47itIamYNYAV1KEm4MGNdEJAVs1Mi9jKzrksC7//aW9g0sQ
wx8Pjh9bro6McLSLpceTnoe6pwOS7jbDVqSUKbX4s/IWD5FDLvBLcNEvLYIDnDjc
EWN56nWLpfwme0mLKZJroEsUimTSuDArCoNbhrvkRDtbK93smRFUxk7tnY92c8Q=
=9eMM

-----END PGP SIGNATURE——

El que saben que saben

Els contorns del estat de la vigilància massiva

Intentem imaginar per un moment el vertigen que produiria treure el cap a l'abisme de la intimitat col·lectiva, als arxius de la vida quotidiana que es conserven en els Data Centers dels proveïdors d'Internet, les operadores telefòniques o les empreses de Silicon Valley: les muntanyes infinites de fotografies personals, el contingut dels missatges de correu electrònic, el nostre historial de recerques, els nostres pagaments amb targeta de crèdit, els registres de totes les trucades telefòniques que realitzem, la relació de totes les vegades que hem premut «m'agrada» en una pàgina de Facebook... Imaginem ara que tota aquesta informació, que en molts casos no voldríem compartir amb la nostra parella, els nostres amics o els nostres familiars, està lliurement a disposició d'estranys que l'emmagatzemen i l'analitzen, sense necessitat d'una justificació prèvia o supervisió judicial, sense que ni tan sols tinguis dret a saber de quina manera s'està fent servir. Imagina, a més, que el simple fet d'adoptar mesures d'autoprotecció, com, per exemple, eines per xifrar les teves comunicacions, et col·loca en una llista de sospitosos, et converteix en un objectiu que cal seguir. Imagina viure en un món en què el poder pressuposa que aquell qui vol preservar la seva intimitat fins a les últimes conseqüències deu tenir alguna cosa a amagar.

Aquesta distopia és el món en què ens vam despertar el 5 de juny del 2013, el dia que van començar a sortir a la llum les revelacions d'Edward Snowden. Snowden era un jove contractista de l'empresa de seguretat Booz Allen Hamilton que treballava per a l'Agència Nacional de Seguretat nord-americana (NSA) i que es va escapar a Hong Kong amb milers de documents classificats. Aquests documents oferien una cartografia abans impensable del món a la segona dècada del segle XXI, un món en què l'escrutini de les dades dels ciutadans i la violació de la seva privadesa estan a l'ordre del dia.

Si bé molts experts en seguretat informàtica fa anys que insisteixen en la fragilitat de les nostres comunicacions personals i en el fet que tota noció de privacitat a Internet té alguna cosa d'il·lusori, ningú podia imaginar fins a quin grau tan extrem les tecnologies digitals –les mateixes que se'ns oferien com a instruments d'alliberament i autonomia que farien possible un món més igualitari, participatiu i democràtic– facilitarien la construcció de l'estructura de control més sofisticada de la història de la humanitat.

La paradoxa és que aquest malson totalitari ha estat concebut i executat per les grans democràcies occidentals, amb la necessària col·laboració –a vegades amb resistència activa, d'altres amb resignada connivència– de la indústria tecnològica, a la qual fins ara s'adjudicaven unànimement efectes socials positius. El camí que ens ha portat fins aquí és més o menys conegut: la «guerra contra el terrorisme» iniciada pel govern nord-americà de G.W. Bush després dels atemptats l'11 de Setembre va dotar les agències d'intel·ligència i altres estructures governamentals d'amplis poders per intervenir en les comunicacions personals de qualsevol individu i emmagatzemar-les. Paral·lelament, l'explosió digital, dels mòbils a la Web 2.0, ofereix l'oportunitat de radiografiar detalladament, en un grau que no tenia precedents, la vida quotidiana i l'activitat social de la majoria dels ciutadans. Mai havia estat tan senzill interceptar dades personals; mai hi havia hagut tantes dades personals per capturar.

A més, la «intel·ligència de senyals» (*signal intelligence* o SIGINT), la branca de l'espionatge dedicada a la captura de comunicacions, viu –com una infinitat d'altres disciplines– la seva pròpia revolució Big Data. A les agències ja no els interessa interceptar un missatge concret que incrimini directament un sospitós, sinó disposar d'immensos volums de dades que els permetin reconstruir la seva esfera de contactes i moviments a través de les seves interaccions amb altres persones. El general Keith Alexander, director de la NSA fins a l'octubre del 2013, va definir aquest nou paradigma d'una manera extremament gràfica: «per trobar una agulla, es necessita un paller». El paller som tots nosaltres.

Les progressives revelacions del cas Snowden dibuixen una imatge molt clara que permet entendre fins a quin punt la nostra vida digital és transparent i accessible per a la maquinària de la societat de la vigilància massiva.

Sabem que operadores de telefonia com Verizon han lliurat a la NSA i l'FBI les metadades de milions de trucades telefòniques que permeten saber a qui ha telefonat cadascú, des d'on i durant quant de temps. Sabem que, amb el programa PRISM, la NSA pot accedir directament i sense necessitat d'una ordre judicial als servidors de companyies com Facebook, Google, Skype, Apple o Microsoft, per interceptar dades com els historials de navegació, el contingut de correus electrònics o els fitxers descarregats.

Sabem que la NSA no només ha interceptat regularment les comunicacions dels ciutadans particulars, sinó també les dels serveis diplomàtics de nombrosos països i d'organismes internacionals, amb la finalitat d'obtenir avantatge en les negociacions. Sabem que la mateixa infraestructura física d'Internet ha estat intervinguda per mitjà de programes que, com el britànic Tempura o el nord-americà Upstream, permeten «punxar» els cables de fibra òptica que canalitzen el tràfic telefònic i de dades.

Sabem de l'existència d'infraestructures paral·leles en les quals la NSA emmagatzema dades personals per indexar-les i poder investigar-les amb facilitat. El programa XKeyscore es basa en una xarxa de servidors distribuïts per tot el planeta en què els analistes poden buscar dades vinculades a adreces de correu electrònic, noms o adreces IP.

Probablement trigarem anys a comprendre les implicacions finals de les revelacions facilitades per Edward Snowden. A curt termini, mostren ben clarament que, en la configuració tecnològica d'Internet que fan servir milions d'usuaris diàriament, qualsevol sentit de la privadesa és il·lusori.

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

What We Know They Know

The outlines of the mass 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 Microscoft, intercepting data such as search histories, the contents of emails or downloaded files.

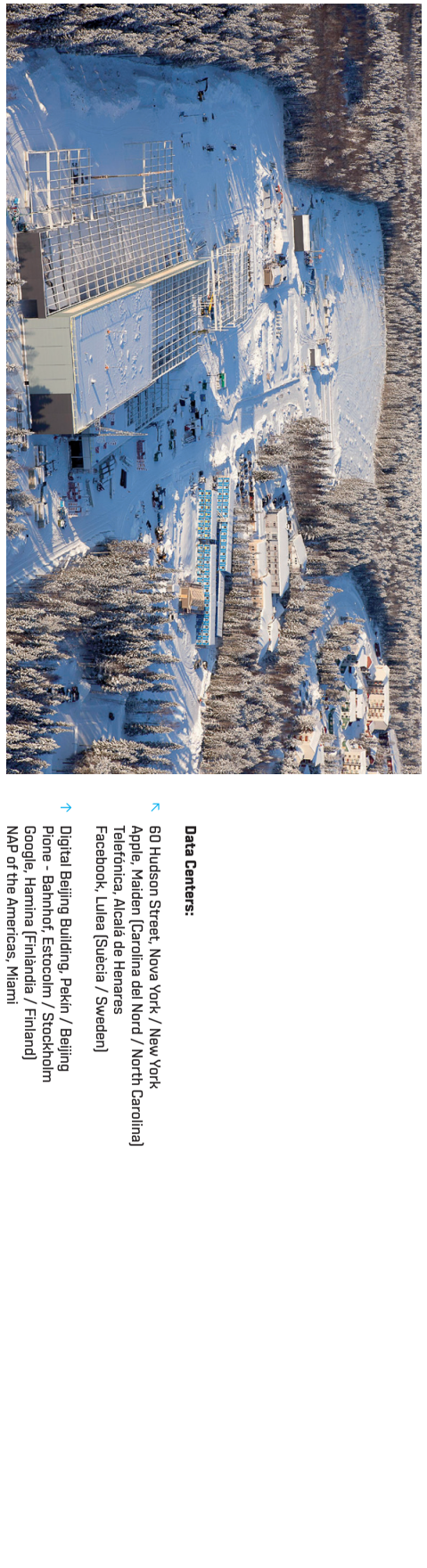
We know that in addition to private citizens, the communications of the diplomatic services of numerous countries and international organisms have been regularly intercepted by the NSA, with the aim of obtaining a competitive advantage in negotiations. We know that the very physical infrastructure of 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.

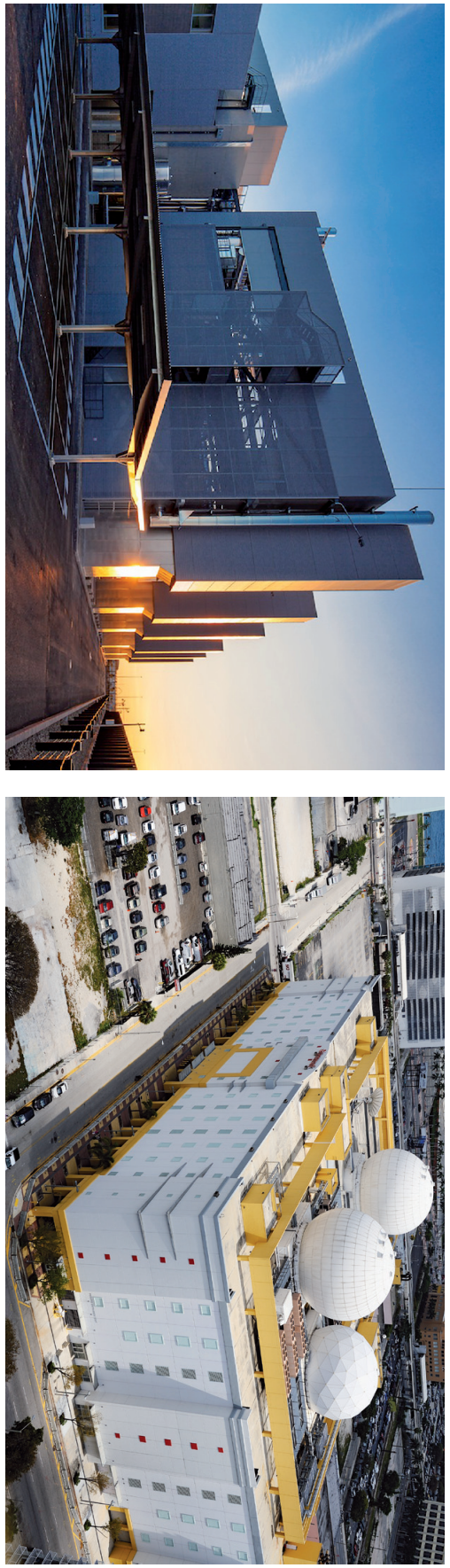
It will probably take us years to fully comprehend the ultimate implications of the revelations leaked by Edward Snowden. In the short term, they clearly establish that in the Internet technological configuration that millions of users use daily, any sense of privacy is an illusion.

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

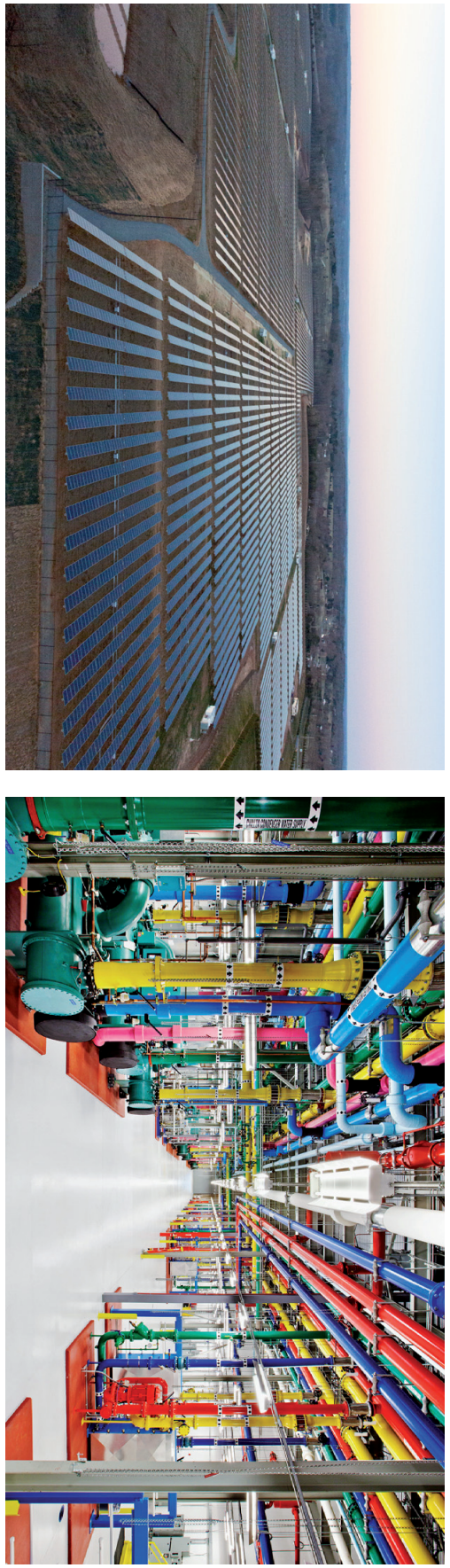
© Gunnar Svedenbäck | https://www.flickr.com



© Telefónica



© Gigaom | https://www.gigaom.com



© Beyond My Ken

Data Centers:

↗ 60 Hudson Street, Nova York / New York
Apple, Maiden (Carolina del Nord / North Carolina)
Telefónica, Alcalá de Henares
Facebook, Luleå (Suècia / Sweden)

→ Digital Beijing Building, Pekín / Beijing
Pione - Bahnhof, Estocolm / Stockholm
Google, Hamina (Finlàndia / Finland)
NAP of the Americas, Miami

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

© Connie Zhou/Google

© http://www.bahnhof.net

© Digital-dreams

Quan tu ets el producte

Dir que, quan un servei és gratuït, en realitat el que passa és que el paguem d'una altra manera (amb dades) ja comença a ser un fet acceptat per moltes de les persones que utilitzen la tecnologia de forma quotidiana i que tenen una certa consciència del rastre de dades que van deixant amb cadascuna de les activitats que realitzen.

Tanmateix, més enllà del «tu ets el producte», poques persones coneixen de forma detallada en què consisteix o com funciona aquest pagament amb dades. De fet, la qüestió no és senzilla. L'àmbit amb el qual potser és més fàcil introduir el tema és el de la navegació per Internet: les empreses i prestadors de serveis ens ofereixen de forma gratuïta les seves pàgines web, i sovint serveis associats, com la possibilitat de tenir contacte amb altres persones a través de xarxes socials, fòrums, etc. Ara bé, tal com mostra l'eina Disconnect, cada vegada que entrem en una pàgina web, una sèrie de microprogrames coneguts com a *cookies* (galetes) s'instal·len al nostre dispositiu i envien al propietari del lloc web informació sobre la nostra IP o MAC (la «matrícula» del nostre dispositiu), el temps que utilitzem el lloc web i com l'utilitzem, i sovint també sobre els altres llocs web que consultem mentre tenim una web concreta oberta. Addicionalment, és habitual que diferents empreses paguin a la web que estem visitant per poder instal·lar-nos galetes de tercers.

De fet, cada vegada que obrim un lloc web, el nostre ordinador pot rebre entre desenes i centenars de peticions d'instal·lació de galetes. Quan naveguem per Internet, doncs, som el producte, perquè a canvi de la visita proporcionem informació sobre la nostra activitat virtual i, sovint, dades personals que han estat prepagades per les empreses que han contractat amb un lloc web en particular la possibilitat d'espiar-nos.

Però si l'exemple de la navegació web és el més habitual, cada cop és el menys protagonista. El mateix desplegament de connexions no aparents ni fàcilment controlables es produeix també quan utilitzem, per exemple, una targeta client, que relaciona el nostre patró de consum amb un nom, una adreça, targeta de crèdit i sovint també amb les respostes al petit qüestionari que se'ns demana que omplim quan fem la sol·licitud.

Un altre àmbit de recollida de dades cada vegada més important és l'ús de l'espai públic. Com mostra la infografia de les pàgines 6-7, el nostre deambular incaut per la ciutat cada vegada té menys d'anònim: els escàners d'adreces MAC, les càmeres tèrmiques i de videovigilància, les xarxes Wi-Fi, els fanals «intel·ligents» o els sensors de lectura automàtica de matrícules ens incorporen de forma rutinària a bases de dades que en algun lloc serveixen a algú per treure'n un profit que ni coneixem ni controlem.

En l'àmbit domèstic és potser on augmenta de forma més preocupant aquest monitoratge dels nostres moviments i rutines per elaborar-ne patrons vendibles: tots els electrodomèstics «intel·ligents», del comptador a la televisió, passant per la nevera, construeixen una xarxa d'extracció de dades que mira de perfeccionar la imatge de qui som i què volem o podem voler, per tal d'avançar-se a les nostres necessitats i temptar-nos a adquirir productes o serveis addicionals. Paguem, doncs, dues vegades: quan adquirim l'electrodomèstic i quan aquest ens converteix en producte revenent les nostres dades.

Si fer el mapa de la sèrie de mecanismes i processos que ens converteixen en producte és relativament senzill, no ho és tant establir quin és el model de negoci ni el benefici concret que creem amb les nostres dades. L'empresa Datacoup, per exemple, permet a l'usuari escollir quines dades vol vendre (des de l'ús de xarxes socials a dades bancàries) a canvi de fins a 8 dòlars al mes. De forma similar, en una denúncia col·lectiva presentada als EUA contra Facebook per apropiar-se indegudament dels noms i preferències dels usuaris, l'empresa va acabar accedint a pagar 10 dòlars a cada usuari. No ens farem rics, doncs.

Els veritables diners de la mercantilització de les dades personals no són encara en aquesta interfície concreta entre l'usuari i les empreses que recullen dades. Qui guanya diners amb la nostra despreocupada cessió de dades personals són aquells que es col·loquen en les primeres posicions de la carrera per emmagatzemar dades a l'espera que la promesa de la monetarització es realitzi. De moment, aquesta promesa només ha omplert les butxaques dels fundadors i accionistes d'empreses amb un model de negoci centrat en la compra i venda de perfils de dades (com l'esmentada Facebook o Tuenti, Google, Foursquare, YouTube, etc.) i ha creat un submercat de «corredors de dades» *(data brokers)*, companyies dedicades a l'encreuament de diferents bases de dades d'activitat *online* i *offline* per tal d'augmentar el preu de venda dels perfils generats d'aquesta manera.

És possible que a determinades persones aquest panorama no els generi inquietuds, ja que pagar amb dades també obre la porta a la promesa de serveis personalitzats i atenció individualitzada. Ara bé, els corredors de dades no es limiten a encreuar les dades del que comprem, amb qui interactuem i què ens agrada. El comerç de dades inclou també, i cada vegada més, expedients mèdics, dades fiscals i de renda o dades bancàries, és a dir, el tipus d'informació que pot determinar si se'ns dóna un crèdit, si se'ns ofereix una assegurança mèdica més o menys cara o si aconseguim un lloc de treball. De cop, el preu pagat en dades es revela desproporcionat.

Quan acceptem ser el producte, doncs, convé no oblidar que acceptem també que se'ns pugui acabar deixant al fons de la prestatgeria, amagats i ignorats perquè el nostre perfil no promet la solvència, la salut o l'obediència que ofereixen els altres.

↑ https://disconnect.me/disconnect

We 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.

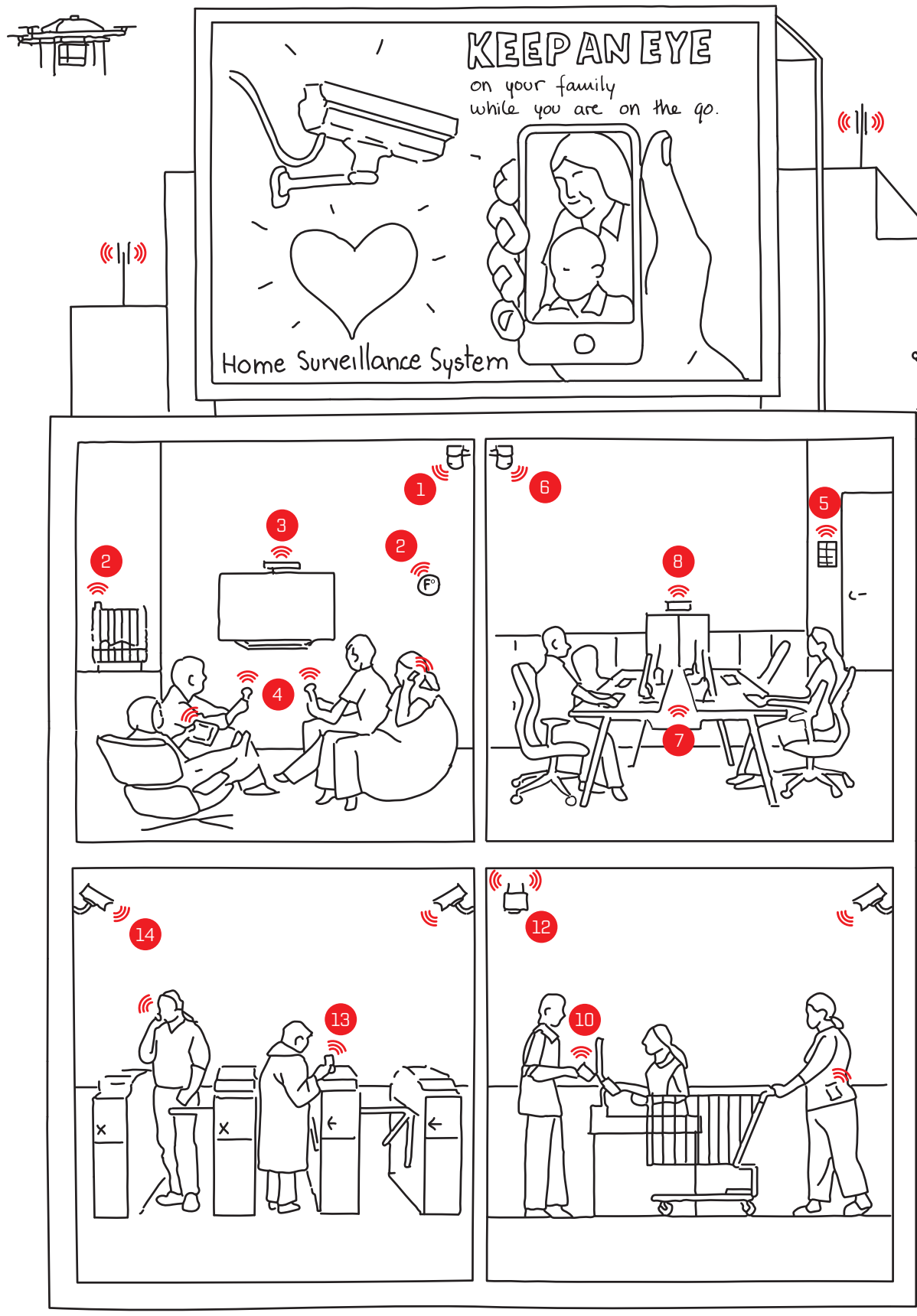
The real money from the commercialisation of personal data is not yet in this specific interface between the user and the companies that collect data... The people who earn money from our carefree surrender of personal data are those who position themselves at the front of the race to store data while 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.

Escenes quotidianes d'una ciutat sota vigilància

Everyday Scenes of a City under Surveillance



Probablement no som conscients de la quantitat de vegades al llarg del dia que entrem en contacte amb una tecnologia que produeix dades en què es reflecteixen els nostres actes. Ja sigui a peu de carrer, a casa, a la feina o als espais comercials, la ciutat del segle XXI és una ciutat sota vigilància. Totes aquestes dades poden ser una amenaça en potència per a la nostra privacitat. No és exagerat dir que avui dia són pocs els moments en què som autènticament anònims.

A casa

1 **VIDEOVIGILÀNCIA DOMÈSTICA:** els dispositius que transmeten vídeo sense fil, com ara els monitors de vigilància de nadons, poden ser interceptats i el seu senyal pot ser capturat des de l'exterior de l'habitatge.

2 **COMPTADORS DE LA LLUM I TERMÒSTATS INTEL·LIGENTS:** permeten identificar el comportament quotidià dels habitants de cada llar, ja que el registre del consum mostra quan s'activa la dutxa, la torradora o la cafetera.

3 **TELEVISORS INTEL·LIGENTS:** en el futur immediat, els televisors connectats a Internet, amb càmera web incorporada, monitoraran els hàbits familiars de consum de televisió i fins i tot l'ús dels espais comuns de l'habitatge.

4 **CONSOLES DE VIDEOJOCS:** les últimes generacions de consoles incorporen càmeres de vídeo i infrarojos que poden captar i transmetre imatges i so de la sala d'estar sense que l'usuari ho sàpiga.

A la feina

5 **CONTROL BIOMÈTRIC D'ENTRADES I SORTIDES:** cada vegada més, els sistemes per registrar el moment en què els treballadors accedeixen al lloc de treball i en surten incorporen sistemes d'identificació biomètrica, com ara empremtes dactilars o reconeixement ocular.

6 **VIDEOVIGILÀNCIA:** les càmeres col·locades al recinte del lloc de treball i les seves gravacions es poden utilitzar per reconstruir els moviments dels treballadors o per comprovar el lloc en què es troben en un moment determinat.

7 **MONITORATGE REMOT DE LA PANTALLA DE TREBALL:** diversos sistemes de control de la productivitat arxiven regularment captures de la pantalla del treballador i l'envien a superiors o clients per comprovar-ne l'activitat.

8 **BASES DE DADES PERSONALS:** en un gran nombre d'empreses, les bases de dades personals dels seus clients són una eina de treball essencial diàriament. Aquestes bases de dades poden incloure historials financers, de salut o de riscos, entre d'altres.

Als espais comercials

9 **SENSORS DE COMPTATGE DE PERSONES:** s'utilitzen per monitorar el trànsit de compradors en espais comercials, així com per registrar el temps que passen contemplant els aparadors.

10 **TARGETES DE FIDELITZACIÓ:** a canvi d'oferir descomptes i avantatges, s'utilitzen per crear un perfil del consumidor basats en els seus hàbits de compra i conèixer millor els seus costums com a consumidor.

11 **IBEACONS:** aquest sistema permet als comerços enviar anuncis i ofertes als mòbils que es trobin físicament a prop, si tenen instal·lada l'aplicació corresponent. Es tem que es pugui utilitzar per rastrejar els moviments dels compradors de la zona.

12 **WI-FI GRATUÏT:** a canvi d'oferir accés gratuït a Internet, diversos serveis comercials exigeixen les dades d'identificació en xarxes socials com Facebook o Twitter i accedeixen al nostre perfil en aquests serveis.

En el transport urbà

13 **BITLLETS DE TRANSPORT PÚBLIC:** les targetes recarregables que s'utilitzen a cada vegada més xarxes d'autobús i metro produeixen dades sobre els desplaçaments dels seus usuaris.

14 **VIDEOVIGILÀNCIA A ANDANES I VAGONS DE TREN I METRO:** tant les andanes de les estacions com l'interior dels vagons estan equipats en molts casos amb càmeres de videovigilància.

15 **XARXES DE BICICLETES PÚBLIQUES:** les targetes d'usuari registren el trajecte realitzat i les hores de sortida i arribada de l'usuari.

16 **AUTOMÒBILS:** les matrícules dels vehicles poden ser registrades per sistemes ANPR de reconeixement de matrícules, tant al carrer com als aparcaments. També es registren els trajectes dels cotxes que tenen incorporats sistemes de pagament de telepeatge (Teletac).

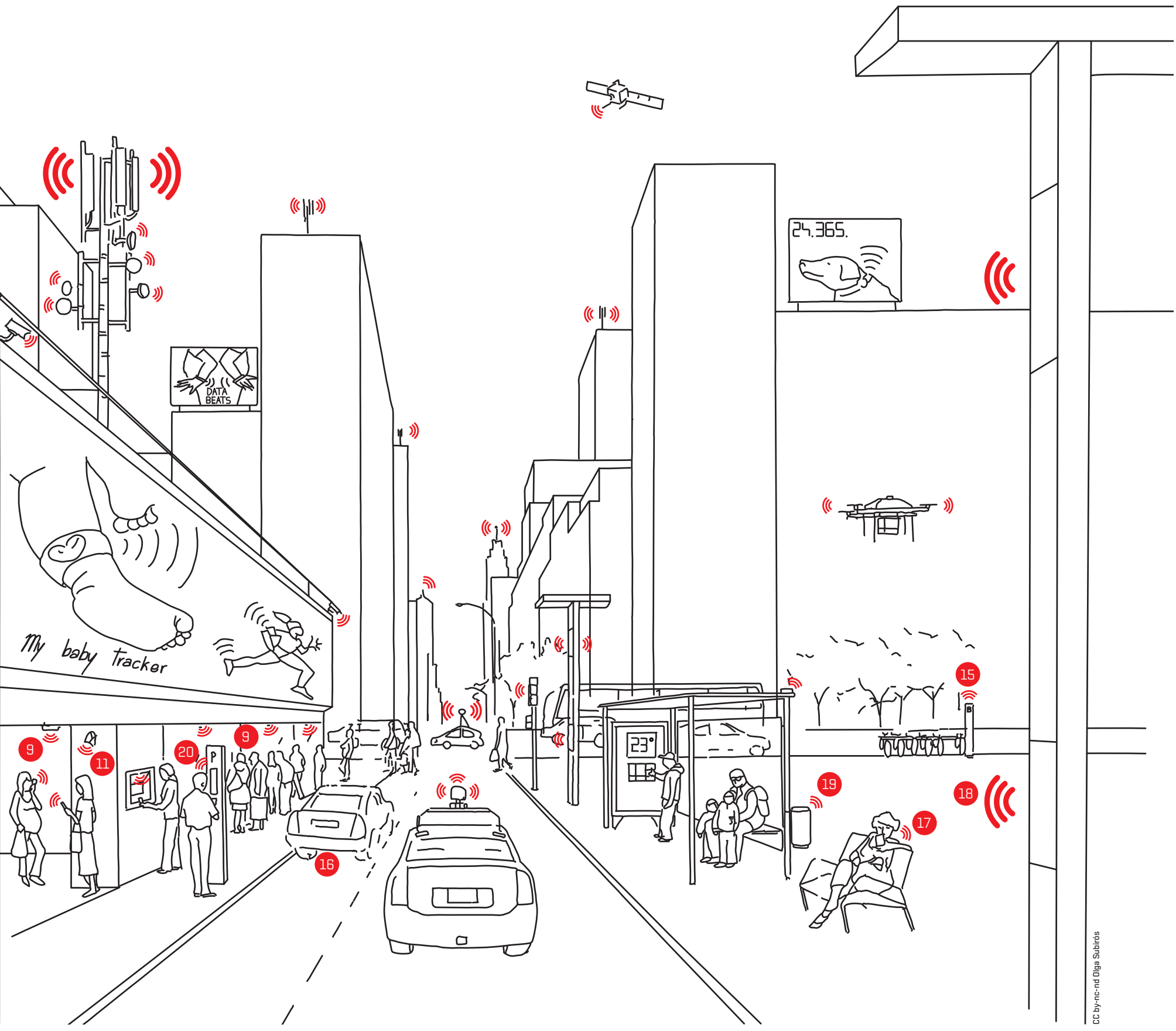
Al carrer

17 **TELEFONIA MÒBIL:** permet a les operadores i a serveis d'intel·ligència determinar –per triangulació del senyal, o GPS– la posició aproximada de l'usuari i activar remotament l'auricular per utilitzar-lo com a micròfon.

18 **CÀMERES TÈRMIQUES I SENSORS SONORS:** presents a molts espais públics de les grans ciutats contemporànies, es fan servir per mesurar el flux de vianants o registrar els nivells de soroll.

19 **MOBILIARI URBÀ INTEL·LIGENT:** la incorporació progressiva de sensors a parades d'autobús, fanals o papereres té com a finalitat detectar la presència de vianants a prop, però aquests sensors també poden identificar-los captant informació dels seus telèfons intel·ligents.

20 **SISTEMES D'APARCAMENT:** el pagament amb targeta a zones blaves i verdes genera dades sobre l'usuari. Les places estan incorporant progressivament sensors que determinen si estan lliures o ocupades.



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: gairebé els grans èxits

Com a resposta a la videovigilància, activistes i artistes han creat tot un ventall de mètodes per pertorbar-ne el funcionament, així com per protestar contra altres formes de visibilitat i traçabilitat. La majoria de les primeres formes de resistència anaven dirigides a les càmeres de televisió de circuits tancats, ja fos escenificant missatges polítics de *contestació* davant la càmera (com feien els Surveillance Camera Players als anys noranta) o senzillament fent-hi pintades o reorientant-les.

A mesura que la videovigilància s'ha fet més i més omnipresent i automatitzada, també s'hi han tornat les eines i els mitjans de resistència. Les càmeres de televisió de circuits tancats han anat evolucionant per passar del circuit tancat a mètodes de videovigilància en xarxa, alhora que formes de resistència com ara *Life: A User's Manual* han explotat els nous mitjans emprats per la videovigilància –per exemple, l'espectre sense fil– per posar de manifest les noves relacions socials creades per aquesta vigilància. Com més en xarxa es connecta la vigilància, més s'hi connecten les formes de coneixement creades per resistir a la vigilància, com ara les bases de dades de càmeres de videovigilància, i els mètodes d'elusió s'han barrejat cada vegada més amb la moda (com palesa el projecte CV Dazzle) a mesura que s'han anat ampliant les capacitats d'abast i de reconeixement de la videovigilància, i de les ciutats que la despleguen.

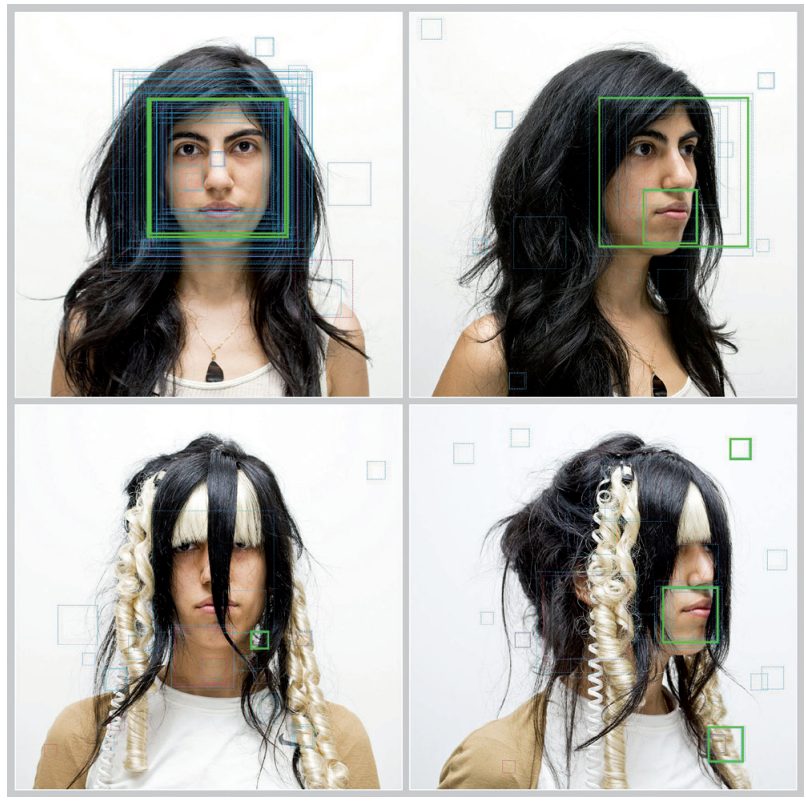
Surveillance Camera Players (1998)
Els Surveillance Camera Players (SCP) són un grup format el 1996 que va plantar cara de manera directa a les càmeres de videovigilància mitjançant performances públiques. Els SCP s'inspiren en el moviment situacionista, que utilitzava l'espectacle disruptiu i la performance pública com a mitjà per destacar o criticar les relacions socials. Han escenificat versions adaptades de diverses obres davant de càmeres de videovigilància a Nova York, entre elles una interpretació en públic a Manhattan de *Re-Elect Big Brother* (basada en el *1984* d'Orwell) –amb vestuari inclòs– el dia de les eleccions nord-americanes, el novembre del 1998. A més de quedar enregistrada per la càmera de videovigilància, la performance també va ser enregistrada per equips de filmació per poder-la emetre per televisions per cable locals i independents. Amb les seves actuacions davant la càmera, els SCP lluiten de manera efectiva contra la idea que les persones vigilades s'han de resignar a la seva sort.

Institute of Applied Autonomy, *iSee* (2001)
El projecte iSee, de l'Institute of Applied Autonomy, és una base de dades geogràfica de proveïment participatiu que exemplifica perfectament la tàctica de la *sousveillance* o vigilància des de sota. Amb aquesta eina els usuaris poden facilitar la localització geogràfica de càmeres de videovigilància i, al seu torn, consultar la base de dades per saber on es troben les càmeres. En comptes d'enfrontar-se directament a les càmeres mateixes, l'iSee ajuda els usuaris a seguir una «ruta menys vigilada» per la ciutat. L'iSee per a Manhattan, per exemple, es basa en part en dades d'un «cens de circuits tancats de televisió» fet entre 1998 i 2002 i permet que els usuaris creïn els seus itineraris evitant tantes càmeres com sigui possible. Malgrat que és una eina de resistència a la videovigilància, el que fa és reduir, més que no pas anular totalment, l'exposició a les càmeres de vigilància.

Michelle Teran, *Life: A User's Manual* (2003-2006)
Aquest projecte de Michelle Teran juga amb la juxtaposició de mons virtuals i físics mitjançant un receptor sense fil que utilitza les transmissions sense fil accessibles públicament de les càmeres de videovigilància que siguin a prop. L'artefacte en si és una maleta amb rodes arrossegada per un personatge femení nòmada i equipada amb una petita pantalla negra circular en què es mostren enregistraments de videovigilància. Basat en la novel·la epònima de Georges Perec del 1978, en què es narren les històries entrecreuades dels habitants d'un edifici de pisos de París, el projecte de Teran entreteixeix l'espai físic del carrer amb l'espai virtual dels enregistraments de videovigilància. *Life: A User's Manual* utilitza l'espectre sense fil accessible públicament (per tal que no esdevingui en si mateix una tecnologia de vigilància intrusiva) i posa de relleu fins a quin punt les imatges de les vides dels habitants de la ciutat emeses per ells mateixos fan possible la vigilància.

Adam Harvey, *CV Dazzle* (2010)
A mesura que les càmeres de videovigilància proliferen i adquireixen capacitats de reconeixement facial, la necessitat de defensar el rostre de cadascú ha passat a estar lligada a la necessitat de mantenir la identitat i les emocions de cadascú en l'anonimat. Entreu a CV Dazzle, una eina que dóna consells de maquillatge i moda per eludir els sistemes de reconeixement facial. El nom d'aquesta eina és una adaptació en clau d'humor de Dazzle, el camuflatge cubista utilitzat pels cuirassats de la Primera Guerra Mundial, i es basa en unes investigacions que demostren que el maquillatge o les obstruccions en el rostre poden confondre o inutilitzar els sistemes de reconeixement facial. A més d'un *book* de maquillatges i pentinats, CV Dazzle ofereix consells –basats en la investigació– per recuperar la privacitat, incloent-hi mètodes per enfosquir-se els ulls o el nas i, així, desdibuixar els trets comuns que busquen els sistemes de reconeixement facial.

Veïns de Lavapiés, *Un barrio feliz* (2010)
Quan l'any 2010 l'Ajuntament de Madrid va instal·lar càmeres de videovigilància al barri de Lavapiés, molts veïns van oposar resistència activa a les premisses i les promeses del sistema. Part del to crític d'*Un barrio feliz* es proposava posar de relleu la justificació que es va fer de la videovigilància: davant la davallada de la delinqüència i les insinuacions del coordinador de seguretat de l'Ajuntament sobre la presència d'«altres persones», es denunciava que el sistema era un instrument de fragmentació social. La resposta dels activistes va consistir a parodiar el discurs oficial sobre la videovigilància mitjançant pòsters crítics, alguns amb la inscripció «Lavapiés 1984». La mesura més controvertida del grup va posar de manifest el doble criteri de la videovigilància: quan el grup va instal·lar una càmera pròpia a la zona, imitant el projecte municipal, va ser penalitzat amb una multa de 10.000 euros de l'Agència de Protecció de Dades.



© Adam Harvey

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

Electronic Self-Defence: How to Resist Surveillance

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.

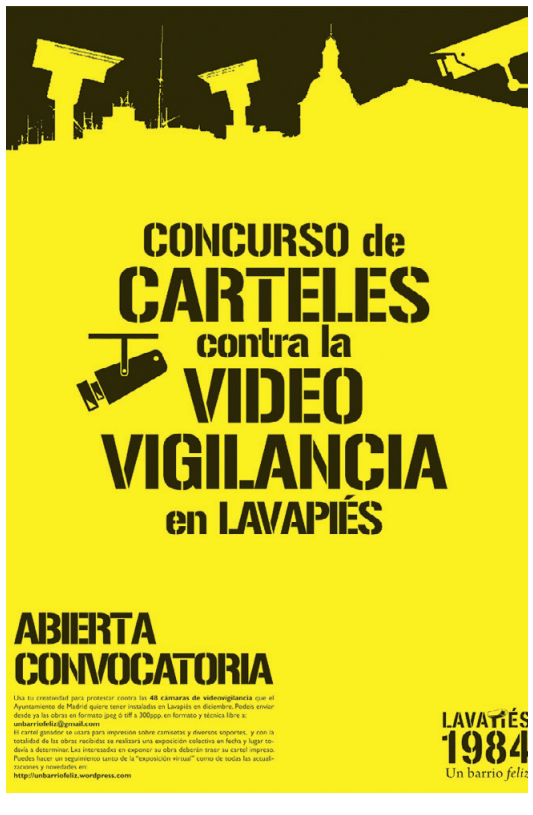
The Surveillance Camera Players (1998)
The Surveillance Camera Players are a group formed in 1996 that directly confront video surveillance cameras through public performance. The SCP are inspired by the situationist movement which used disruptive spectacle and public performance as a mode of highlighting 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 costumes – 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.

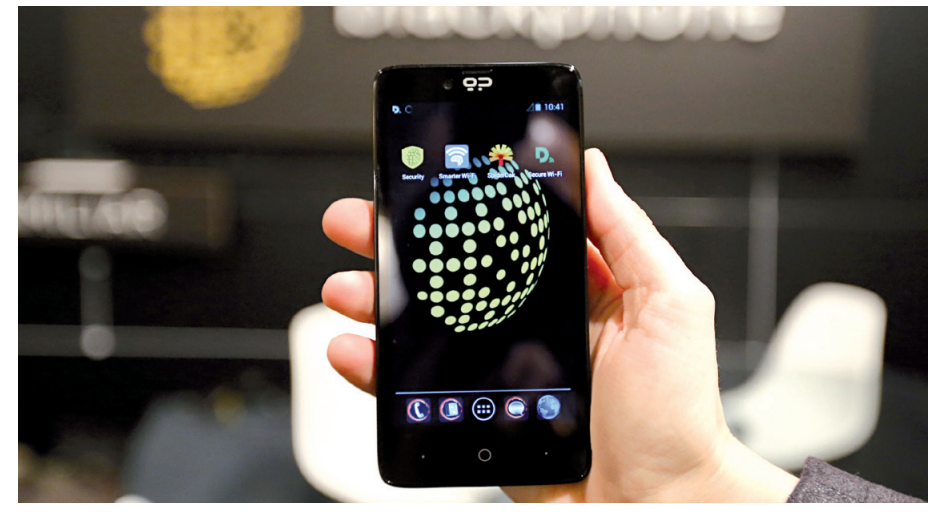
Michelle Teran, *Life: A User's Manual* (2003-2006)
Michelle Teran's project plays with the juxtaposition of virtual and physical worlds by using a wireless receiver to draw on publicly-accessible wireless transmissions from surveillance cameras in proximity. The artefact itself is a wheeled suitcase, 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

Cryptobotiga
Cryptostore

Adam Harvey, membre del col·lectiu Undisclosed de Nova York, vol dur a terme una tasca de conscienciació de l'auge de la Societat de la Vigilància mitjançant un original projecte artístic que intenta combinar privacitat i moda. Es tracta de diverses peces «anti-drone» creades amb un material que evita la detecció per part de les càmeres tèrmiques amb què estan equipats els avions no tripulats. L'inevitable color platejat que el material protector dóna a aquests dissenys recorda, sens dubte, la imatgeria futurista pròpia de dècades anteriors.

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

L'Off Pocket és una funda per a telèfons intel·ligents amb protecció d'ones d'entre 500 MHz i 5 GHz. Prevé l'intercanvi no desitjat d'informació creant l'efecte gàbia de Faraday, amb la qual cosa evita la revelació accidental de qualsevol dada o metadada provinent dels senyals emesos pels dispositius Wi-Fi, Bluetooth o GPS, o pel mateix telèfon. Funciona a tots els països i amb tots els operadors. Aquest complement està fabricat amb un material flexible que permet que el seu pes no arribi als cent grams. Està disponible en tres mides diferents i, a més, és resistent a l'aigua. Si el preu no és a l'abast de la nostra butxaca, podem optar per la versió «fes-t'ho-tu-mateix» que ofereix killyourphone.com, potser amb menys glamur però més autèntica i assequible.

No només de vigilància electrònica viu el panòptic. Biogenfutur ens ofereix una solució per a tots aquells petits rastres de saliva, pèls, ungles i escates de pell amb els quals anem geolocalitzant la nostra presència allà on anem i donant pistes sobre les nostres accions. Amb tan sols 0,5 nanograms d'ADN ja és possible fer una anàlisi forense del nostre «DNI biogenètic». Gràcies al líquid Erase es pot eliminar el 99,5% del rastre d'ADN i completant l'acció amb Replace s'aconsegueix crear confusió sobre el 0,5% restant. Pot semblar exagerat, però el 2013 Heather Dewey-Hagborg va aconseguir crear retrats realistes a partir de les mostres d'ADN encara presents en les burilles, pèls i xiclets que va recol·lectar als carrers de Nova York.

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

Si volem una alternativa molt més pràctica i operativa a l'Off Pocket que no ens impedeixi utilitzar el telèfon mentre garantim la privacitat, el Blackphone és un telèfon dissenyat específicament per evitar el rastreig per part de tercers. Disposa d'una versió d'Android creada expressament per a aquest telèfon, el PrivatOS, i diverses eines per a la comunicació segura i anònima: Silent Phone, Silent Text, Silent Contacts, cerca i navegació anònima, i l'ús de VPN que ofereix Disconnect; a més, ofereix emmagatzematge segur al núvol mitjançant SpiderOak, sistema antirobatori i el servei d'atenció de Blackphone 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 sabotatge

Defensar la nostra intimitat i les nostres dades no sempre requereix un gran coneixement de tecnologies alternatives. No cal saber com funciona Tor ni com muntar un servidor domèstic segur per desbaratar els plans dels que construeixen models de negoci opacs amb dades personals. De fet, amb un coneixement bastant rudimentari de com funcionen els mercats secundaris de dades i els mecanismes de creació de perfils a partir de càlculs algorítmics és possible subvertir la major part d'esperances de monetarització de la nostra activitat quotidiana.

La primera opció de qualsevol que vulgui protegir la seva identitat *online* i *offline*, doncs, és el sabotatge. En les pàgines d'aquest manual trobareu diferents experiències de sabotatge, des dels Surveillance Camera Players al CV Dazzle: exemples de sabotatge premeditat, organitzat i amb l'objectiu de conscienciar.

El sabotatge, però, també pot ser una estratègia personal i quotidiana, orientada a distorsionar el perfil que les empreses i els prestadors de serveis pretenen fer de nosaltres. Si distorsionem el nostre *dada double*, el valor de la informació recollida i agregada disminueix, i així podem recuperar un cert control sobre el procés.

Sabotatge a xarxes socials: L'única referència certa que cal donar a les xarxes socials per poder-se comunicar amb amics i coneguts és el nom. Tota la resta es pot sabotejar: data de naixement, correu electrònic, estat civil, gustos i preferències, etc. Pots jugar amb aquests sistemes per veure com el tipus d'anuncis que reps canvien segons si estàs soltera o casada, o si tens 18 o 68 anys. Diverteix-te!

Sabotatge a les targetes client: El descompte que t'ofereixen se't fa tan irresistible que vols tenir targeta client però no convertir-te en un perfil comercial? Molt senzill: identifica quina dada personal és imprescindible per accedir al preuat descompte (si t'envien cupons, el correu electrònic o l'adreça postal; si són descomptes a caixa, el nom) i utilitza-la, però distorsiona la resta. Facilitar el teu telèfon mòbil, per exemple, no t'aportarà cap descompte, i és una dada que ben segur que regales a canvi de res. En molts casos, la dada personal clau n'és una de sola, i la resta te la pots inventar sense renunciar als descomptes.

Sabotatge en el comerç en línia: La llista de les nostres compres a Internet és un bé preuat per a les empreses de publicitat i corredors de dades personals, ja que se'n pot inferir informació sobre els nostres desitjos futurs. Així, coses tan senzilles com comprar un regal o comprar coses per a una altra persona poden deformar aquesta fotografia. ¿Un home de mitjana edat que compra revistes per a adolescents? ¿Una noia jove adquirint llibres de Corín Tellado un dia, i les obres completes de Thomas Mann l'endemà? Els algoritmes, que viuen dels perfils fàcils i sense matisos, suaran la gota negra. A més a més, també podem seleccionar una adreça d'entrega que no correspongui a la nostra residència.

Sabotatge a les càmeres de vigilància: Als països amb més presència de videovigilància ja fa temps que els jerseis amb caputxa s'han convertit en un element habitual del vestuari urbà. Les persones que volen cometre actes delictius tendeixen a decantar-se per deixar-se el casc de la moto posat. Potser no cal arribar tan lluny, o potser en el futur tots anirem amb pentinats i maquillatge antivigilància, com suggereix Adam Harvey. O és possible que, com fan els Surveillance Camera Players, acabem buscant les càmeres per sortir-hi. De moment, però, una bona manera de sabotejar la videovigilància consisteix a identificar les càmeres i no normalitzar els espais públics sota vigilància.

Sabotatge a la *smart city*: Si els somnis humits d'una part de la indústria d'andròmines intel·ligents es compleixen, la Internet de les coses i les capacitats d'identificació i reidentificació de la infraestructura urbana, sincronitzada amb els *wearables*, pot fer que tota la nostra existència acabi registrada i processada. Per evitar-ho, el sabotatge més evident consisteix a no comprar mecanismes intel·ligents que cobren en diners i en dades (com els televisors intel·ligents o els *wearables*), a comprar telèfons mòbils que anonimitzin les adreces MAC i a apagar el detector de xarxes Wi-Fi que permet la lectura del nostre dispositiu sense que ens en adonem.

De la mateixa manera que per protegir les nostres dades podem sabotejar sistemes i processos, la consciència de què es fa amb les nostres dades, com es fa i qui ho fa pot portar-nos a gestionar la nostra informació de forma responsable i conseqüent: cedint-la quan ens sembla procedent i proporcionat, amagant-la o emmascarant-la quan no sigui així, i fins i tot regalant-la voluntàriament com una forma de contribució no monetària a projectes o productes que ens inspiren simpatia.

El sabotatge com a estratègia d'autodefensa electrònica, de fet, combina el millor de la consciència ciutadana (i els drets relacionats) amb les possibilitats del consum responsable. I tu, què has sabotejat avui?

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 Corín 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?

Guia de l'autodefensa

Vivint com estem vivint –en paraules de Mark Zuckerberg– l'era de la fi de la privacitat, és sorprenent la quantitat d'alternatives als sistemes i solucions més habituals per compartir dades en línia que estan apareixent. De les xarxes socials al correu electrònic, passant pels cercadors, els serveis al núvol o la veu per Internet, els darrers anys han estat testimonis d'una eclosió d'alternatives als estàndards desenvolupats per les grans empreses, que sovint creen aquests serveis només com a esquers per aconseguir dades («tu ets el producte»). La taula que reproduïm, orientativa i no pas exhaustiva ni definitiva, recull algunes de les alternatives de major impacte en àmbits avui dia encara controlats per les grans corporacions, així com solucions que ajuden a adquirir consciència de com es (mal) gestionen les dades personals en el món digital. Amb nivells diferents de facilitat d'ús, de protecció de la privacitat i d'implantació, dibuixen un mapa del que pot ser el futur de l'autodefensa electrònica: un món en què el client-producte s'afirma com a ciutadà i exigeix tenir el control sobre les dades que genera i la informació que se'n deriva.

Categoria	Descripció/Productes convencionals	Alternatives
Àudio/ Vídeo/ VoIP	L'extensió de l'ús d'alternatives a la telefonia convencional a través de serveis de Veu sobre IP (VoIP) no està relacionada amb les revelacions realitzades per Edward Snowden, les quals van deixar més que clar que les trucades telefòniques no s'escapen de ser interceptades. En realitat, el recurs a programes com Skype (Microsoft), Hangouts (Google) i VoIPbuster (Betamax GmbH & Co KG) té a veure amb tarifes més competitives que inclouen serveis similars i fins i tot avantatges addicionals sense cap cost (missatgeria instantània, videoconferència, trucades entre múltiples usuaris). L'alternativa que ofereixen els serveis de VoIP no aporta cap garantia de privacitat, sinó més aviat al contrari. Ja el 2012, Skype va ser acusat de canviar la seva infraestructura per poder facilitar la intercepció de les converses entre usuaris. Per això sorgeixen programes específics que fan de la privacitat la seva bandera i prometen una encriptació de les comunicacions molt més meticulosa.	**Jitsi** Aplicació multiplataforma de veu (VoIP), videoconferències i missatgeria instantània lliure i de codi obert per a Windows, Linux i Mac OS X amb llicència GPL. Admet diversos protocols populars de missatgeria instantània i telefonia i també permet compartir l'escriptori. https://jitsi.org/ **Redphone** És una aplicació de codi obert amb llicència GPL que ofereix trucades amb encriptació d'extrem a extrem per a usuaris que la tinguin instal·lada per garantir que ningú més pugui escoltar les seves converses. https://whispersystems.org **Tox** Programa que permet realitzar videoconferències, trucades i missatgeria de text prioritzant la privacitat i sense cap cost afegit ni continguts publicitaris. http://tox.im
Emmagatzematge al núvol	La conjunció entre les creixents necessitats d'emmagatzematge i les tendències en el terreny de la mobilitat va donar com a resultat l'arribada del «núvol»: solucions d'emmagatzematge remot fàcilment accessibles des de qualsevol dispositiu connectat a la xarxa. Hi ha veritables «granges» de servidors interconnectats destinats simplement a oferir còpies de seguretat i serveis d'emmagatzematge. Avui dia, serveis com Google Drive, iCloud i Dropbox encapçalen les solucions d'emmagatzematge al núvol per als usuaris petits i mitjans. No obstant això, deixar una còpia de la nostra informació en mans alienes, emmagatzemada en llocs desconeguts dels quals ignorem els marcs legals i sense saber qui hi té accés, no pot ser el més tranquil·litzador, sobretot si es tracta de documents que contenen informació confidencial o que revelen secrets al públic (i han de ser dipositats d'una manera totalment anònima). En el cas del servei ofert per Google, un dels principals riscos és que l'accés està vinculat amb la resta de serveis que ofereix a través del seu identificador únic d'usuari, de manera que, si no es té especial cura de tancar la sessió, l'accés als arxius queda exposat. La necessitat de serveis d'emmagatzematge al núvol amb una protecció especial de la privacitat és una demanda que de mica en mica és cada vegada més atesa. És clar que el més segur sempre serà emmagatzemar els arxius en qualsevol dispositiu sense cap tipus de connexió a la xarxa.	**DocumentCloud** Alternativa a scribd respectuosa amb la privacitat. DocumentCloud processa tots els documents que es pengin mitjançant OpenCalais i dóna accés a informació extensa sobre les persones, els llocs i les organitzacions que s'esmenten en aquests documents. https://www.documentcloud.org/home **SecureDrop** És una plataforma de programari de codi obert per a la comunicació segura entre periodistes i fonts d'informació (informants). Originàriament dissenyada i desenvolupada per Aaron Swartz i Kevin Poulsen amb el nom de *DeadDrop*. https://pressfreedomfoundation.org/securedrop **SpiderOak** Permet emmagatzemar, sincronitzar, compartir i accedir privadament a les pròpies dades des de qualsevol lloc, a partir d'un entorn «coneixement zero». https://spideroak.com/ **Tresorit** Emmagatzematge d'objectes digitals de valor, accessible des de qualsevol lloc i compartible de manera segura. El grau més elevat d'encriptació protegeix tots els aspectes de la gestió de continguts al núvol. https://tresorit.com
Encriptació d'unitats	Encara que un dispositiu d'emmagatzematge no estigui connectat a la xarxa, si el roben o el confisquen el podran examinar sense cap problema en cas que no disposi d'una bona encriptació. Un mecanisme addicional de seguretat consisteix a codificar no només els intercanvis d'informació, sinó també la informació en si, disponible a la nostra unitat d'emmagatzematge local. Els discs durs no vénen per defecte amb un sistema d'encriptació, de manera que si en volem augmentar la seguretat, haurem de configurar-lo nosaltres mateixos.	**Bitlocker** Funció d'encriptació total d'unitats inclosa en certes versions de Windows, dissenyada per protegir dades mitjançant l'encriptació de volums sencers. http://www.microsoft.com/en-us/download/details.aspx?id=7806
Correu electrònic	La majoria dels particulars utilitzen comptes de correu electrònic basats en sistemes de correu web, és a dir, que confien l'accés, la gestió i l'emmagatzematge de la seva correspondència virtual a grans empreses que ofereixen aquests serveis: MSN (Microsoft), Gmail (Google), Yahoo!, etc. Com que són productes gratuïts, la rendibilitat del correu web es basa en la vigilància anonimitzada de caràcter comercial, de cara a adaptar la publicitat resultant a les característiques de l'usuari. D'altra banda, les pràctiques demostrades d'espionatge massiu per part d'agències públiques d'intel·ligència han fet palès que, si es vol defensar la privacitat de les comunicacions electròniques, els nivells de seguretat convencionals no són mai suficients i cal anar més enllà. Les alternatives requereixen claus d'encriptació, projectes de correu web amb garanties i fins i tot adreces de correu electrònic «d'un sol ús».	**Enigmail** És una extensió de seguretat per a Mozilla Thunderbird i Seamonkey. Permet redactar i rebre missatges de correu electrònic signats o encriptats amb l'estàndard OpenPGP. https://www.enigmail.net **GnuPG (GPG)** GNU Privacy Guard o GPG és una eina d'encriptació i signatures digitals que substitueix el sistema PGP (Pretty Good Privacy) amb l'avantatge de ser programari lliure amb llicència GPL. GPG utilitza l'estàndard de l'IETF denominat OpenPGP. https://www.gnupg.org **MailPile** Un projecte de «correu web» que permet triar entre fer servir l'ordinador propi com a servidor, per poder controlar les dades i la privacitat pròpies, o bé executar Mailpile en un ordinador al núvol. https://www.mailpile.is **RiseUp** Un projecte per crear alternatives democràtiques i practicar l'autodeterminació mitjançant la promoció de mitjans de comunicació segurs. Ofereix correu web respectuós amb la privacitat: trànsit encriptat, ubicació anònima, adreça IP anònima, etc. https://www.riseup.net/
IM (Missatgeria instantània)	La missatgeria instantània permet la comunicació en temps real a través de text i es va popularitzar ja fa uns quants anys gràcies als clients oferts per MSN Messenger, ICQ o AIM. Avui dia, hi ha desenes d'opcions disponibles, algunes d'elles basades en el protocol obert XMPP. L'ús del sistema d'IM s'ha estès àmpliament a través de terminals mòbils. Destaquen programes com Line, Hangouts (Google), WhatsApp o Facebook Messenger i es tendeix cap a l'intercanvi multimèdia, que completa la comunicació a través de text amb imatges, sons i vídeos. Algunes d'aquestes opcions per comunicar-se han mostrat greus vulnerabilitats; no obstant això, no hi ha cap dubte que, en el cas d'aquestes eines, els que més curiositat mostren per espiar-nos són precisament persones del nostre entorn: només cal una ullada ràpida a Internet per comprovar la gran demanda i oferta d'eines per interceptar converses. És precisament en l'àmbit de la missatgeria instantània on ha sorgit un ampli ventall d'alternatives que asseguren protegir la privacitat de l'usuari.	**Chatsecure** És un client de xat encriptat lliure i de codi obert per a iPhone i Android que admet encriptació «Off-the-record» (OTR) per XMPP. https://chatsecure.org **Cryptocat** Una aplicació de codi obert, de programari gratuït i accessible, desenvolupada per professionals de l'encriptació, que ofereix un xat encriptat en el navegador o en el mòbil. Ni tan sols la mateixa xarxa de Cryptocat no pot llegir els missatges. https://crypto.cat **Telegram** Telegram Messenger és un servei de missatgeria multiplataforma amb clients de codi obert. Els usuaris de Telegram poden intercanviar missatges, fotos, vídeos i documents (admet tots els tipus d'arxius) encriptats i autodestruïbles. https://telegram.org **TextSecure** Encripta els missatges de text i de xat amb connexió sense fil i al telèfon. Tots els missatges s'encripten localment, de manera que si l'usuari perd el telèfon, els missatges no es perdran. https://whispersystems.org/#encrypted_texts
Gestió de contrasenyes	Quan se'ns adverteix que triem una clau segura, no s'exagera en absolut. La capacitat per esbrinar i predir contrasenyes ha adquirit nivells de sofisticació terrorífics. Un dels errors i riscos més grans és utilitzar una mateixa contrasenya per a tot o gairebé tot. SplashData publica cada any la seva llista de les 25 claus més comunes, que a més fan gala de la seva inseguretat. El 2013 el rànquing estava encapçalat per «password» i «123456». Davant la idea d'haver de recordar centenars de noms d'usuari i contrasenyes, molt sovint es recorre a un gestor de claus; la fragilitat de centralitzar tota la informació d'accés en un mateix lloc fa que sigui fonamental triar un gestor en què puguem confiar. Tanmateix, per molt segura que sigui una contrasenya, gran part de la responsabilitat recau en les organitzacions a les quals accedim, ja que s'han donat múltiples casos en què s'ha piratejat directament la base de dades i s'ha aconseguit accedir massivament a les contrasenyes dels usuaris.	**Encrypter** Gestor de contrasenyes, magatzem de tipus clau-valor i cartera electrònica de codi obert, de «coneixement zero» i basat en el núvol. https://encryptr.crypton.io/ **KeePassX** Desa una gran diversitat d'informació –com ara noms d'usuari, contrasenyes, URL, fitxers adjunts i comentaris– en una sola base de dades i ofereix una petita utilitat per generar contrasenyes segures. https://www.keepassx.org **LastPass** El guardonat gestor de contrasenyes LastPass desa les contrasenyes i proporciona accés segur des de qualsevol ordinador i dispositiu mòbil. https://lastpass.com
Votacions	Les aplicacions per coordinar esdeveniments i votar electrònicament com Doodle poden desvelar informació personal sobre les preferències o la disponibilitat d'un usuari, manipular les seves respostes i fins i tot poden conduir a processos de reidentificació.	**Dudle** Generador de votacions que millora la privacitat. L'accés i l'edició estan més ben controlats i les votacions s'eliminen automàticament si no s'hi accedeix durant més de tres mesos. https://dudle.inf.tu-dresden.de/

Paquet de privacitat

Alguns entorns en línia i sistemes operatius donen una certa sensació de fragilitat en termes de privacitat. La usabilitat, la compatibilitat i la interoperabilitat que ofereixen (entre programes, serveis, dispositius, etc.) és possible en molts casos gràcies a la cessió d'informació personal (totalment o parcialment anonimitzada). Aquesta és en gran mesura la base per rendibilitzar aquestes empreses, ja que el pagament directe pel servei no és tan atractiu per al consumidor. Ja sigui en entorns de Windows, Apple o Android, la idea d'anar deixant un rastre informacional pot resultar molt inquietant, de manera que alguns desenvolupadors han creat eines complexes d'acció múltiple que ajuden a contrarestar simultàniament diversos dels problemes plantejats aquí i, així, no haver d'estar pendent de mantenir una llarga llista d'aplicacions.

Disconnect Joc d'eines amb navegació privada, cerca privada, previsualització de política de privacitat de llocs web, privacitat per a nens i connexió sense fil segura. https://disconnect.me

Freedome Paquet de seguretat i privacitat per a dispositius mòbils: navegació segura, màscara d'adreça IP, irrastrejabilitat, seguretat Wi-Fi, antipesca (*anti-phishing*), antivirus...
http://freedome.f-secure.com

Tails «TheAmnesicIncognitoLiveSystem» és un sistema operatiu en directe que es pot iniciar en quasi qualsevol ordinador a partir d'un DVD, una memòria USB o una targeta SD. Utilitza la xarxa Tor, no deixa cap traça a l'ordinador i fa servir les últimes eines criptogràfiques per encriptar els arxius, els correus electrònics i la missatgeria instantània. https://tails.boum.org

Cercador

Mentre que molts dels nostres correus electrònics o trucades poden resultar avorrits i mancats absolutament d'interès, per als experts en mineria de dades les nostres cerques per Internet a través de cercadors com ara Google o Bing (Microsoft) diuen què ens inquieta o què busquem en cada moment: autèntic or digital. Si resulta ser alguna cosa que es pugui vendre (ja sigui una bicicleta, un remei per a la calvície o la nostra mitja taronja), sempre hi haurà un anunciant desitjós de saber qui són els seus clients potencials per estampar-los un bàner que els orienti. Així mateix, si el que busquem en els oracles d'Internet és comprar grans quantitats de fertilitzant, adquirir una còpia de l'Alcorà o entrar en un fòrum on compartir el nostre descontentament envers les autoritats, més aviat cridarem l'atenció dels serveis d'intel·ligència i obrirem la possibilitat de ser classificats com a delinqüents potencials i que la vigilància a la qual ens sotmeten sigui encara més intensiva.

DuckDuckGo Posa l'èmfasi en la privacitat de l'usuari que cerca evitant els resultats de cerca personalitzats. Genera els resultats a partir de llocs web clau de proveïment participatiu, com ara la Viquipèdia, i de partenariats amb altres cercadors, com ara Yandex, Yahoo!, Bing i WolframAlpha.
https://duckduckgo.com

Ixquick És un potent cercador que no compila ni comparteix cap informació personal i ofereix una Guia Telefònica Internacional i accés a 18 milions d'hores de vídeo amb el seu cercador de vídeos.
https://ixquick.com

Startpage Cercador anònim que presenta la mateixa política de privacitat que Ixquick. No registra l'adreça IP de l'usuari ni en rastreja les cerques. Guardonat amb el Segell Europeu de Privacitat.
https://startpage.com

Xarxa social

Els Serveis de Xarxa Social (SXS) com ara Facebook, Twitter, Tuenti o MySpace no es paguen amb diners, es paguen amb dades. Sens dubte, per aprofitar al màxim aquests serveis, el millor és ajustar la identitat virtual a la real (a fi de poder ser trobar i donar-se a conèixer); això permet a aquestes empreses fer perfils més ajustats, però en termes de privacitat els usuaris s'exposen a uns nivells de transparència no sempre desitjables. Davant del fals mite que el que s'exposi en un SXS és informació «pública», es pot fer un ús d'aquests entorns limitant-lo a cercles més propers, de manera que parlar de privacitat en xarxes socials no hauria de ser cap paradoxa. Si bé la circulació en una xarxa és més eficient quan ha de creuar el mínim nombre possible de nodes, algunes iniciatives pretenen oferir SXS menys jerarquitzats, més distribuïts i descentralitzats, lliures de vigilància comercial i sense cap «porta del darrere» per a mirades indiscretes.

Diaspora Sorgeix el 2010 com a alternativa a Facebook. Ofereix la primera xarxa social gestionada per la comunitat, distribuïda, descentralitzada i respectuosa amb la privacitat, que permet als usuaris tenir el control de les seves dades.
https://joindiaspora.com

N-1 És un «dispositiu tecnopolític» sense ànim de lucre que promou l'ús d'eines lliures, desenvolupades i autogestionades amb una ètica horitzontal i antagonista. És una de les xarxes de Lorea, un projecte que engloba diverses xarxes socials i té com a objectiu la seva federació. També està connectat amb Rhizomatik Labs.
https://n-1.cc

Navegació web

https://

La navegació web és la porta d'entrada per a l'intercanvi d'un ampli volum d'informació en línia. Per poder utilitzar-la moltes aplicacions utilitzen directament com a interfície el navegador, el qual emmagatzema infinitat d'informació que diu moltíssim sobre nosaltres: galetes, historial de navegació, adreces d'interès, noms d'usuari i contrasenyes i fins i tot dades introduïdes prèviament en formularis. L'opció de navegació privada (*private browsing*) no garanteix que no es produeixi un rastreig de la nostra sessió. La navegació en si està plena de riscos encara que siguem prudents: captures de pantalla il·legítimes, pesca (*phishing*), *spambots*... Fins i tot hi ha troians que poden prendre el control de la nostra càmera web. El protocol més comú per a la navegació segura és l'HTTPS, que evita les punxades informàtiques i les intercepcions (*man-in-the-middle*), però tota precaució és poca: antivirus, tallafocs, detectors de programari maliciós, anonimitzadors...

Anonymizer Un ordinador que fa de servidor intermediari i d'escut de la privacitat entre un client i la resta d'Internet. Accedeix a Internet en nom de l'usuari i protegeix la informació personal ocultant la informació identificativa del client.
http://www.livinginternet.com/i/is_anon_work.htm

Bleachbit Allibera memòria cau ràpidament, elimina galetes, esborra l'historial de navegació, destrueix arxius temporals per evitar que es puguin recuperar, elimina registres i descarta brossa que no sabíem que hi era.
http://bleachbit.sourceforge.net

Do Not Track És una tecnologia i proposta de política que permet als usuaris donar-se de baixa voluntàriament del seguiment de llocs web que no visiten, com ara serveis d'analítiques, xarxes de publicitat i plataformes socials.
http://www.donottrack.us

HTTPS Everywhere És una extensió de Firefox, Chrome i Opera que encripta les comunicacions amb molts llocs web importants i, així, fa més segura la navegació.
https://www.eff.org/https-everywhere

Maskme Derrota el correu brossa, atura el telemàrqueting i evita els cobraments no desitjats i el frau oferint la possibilitat d'emmascarar el correu electrònic, el telèfon i la targeta de crèdit quan es navega i es fan compres per Internet.
https://www.abine.com/maskme/

Privacy Badger És un complement del navegador que evita que els anunciants i altres rastrejadors rastregin secretament què visita l'usuari i quines pàgines web mira.
https://www.eff.org/privacybadger

Tor Un navegador web respectuós amb la privacitat molt estès. Tor és un programari lliure i una xarxa oberta que ajuda l'usuari a defensar-se de les anàlisis de trànsit. https://www.torproject.org

Data double

El *data double* és el conjunt d'informació que anem deixant o que hem emmagatzemat al voltant nostre, i constitueix una segona imatge incorpòria de la nostra vida. Aquest «cos» incorpori, més comunament conegut com a «petjada digital», està format per les diverses traces digitals que anem deixant com a ciutadans i consumidors. Si bé l'existència d'informació sobre nosaltres fora de nosaltres no és res nou, el *data double* indica l'existència de dades en format digital, la qual cosa ha permès el ràpid creixement de noves maneres de processar, combinar i analitzar aquestes dades. Es podria generar un *data double* relativament complet associant diversos perfils diferenciats: si es combina l'historial de compres per Internet d'una persona, el seu perfil en mitjans socials i les dades de seguiment de la seva geolocalització, es pot obtenir un retrat de la seva vida força dens.

Es tracta de conseqüències gairebé inevitables en una era digital, i l'ús [i abús] de *data doubles* –que no sempre són representacions acurades de l'individu– està molt estès. Un dels usos més freqüents que tenen els *data doubles* és la categorització. Algunes aplicacions de la categorització permeten unes pràctiques relativament inofensives, com ara adaptar la publicitat dels mitjans socials als gustos i els costums dels usuaris. Tanmateix, a causa de l'associació dels *data doubles* amb l'autenticitat –les dades «no menteixen»–, aquesta informació personal ha permès un seguit de formes més pernicioses de classificació social. Els registres de noms de passatgers generats per les companyies aèries, ara compartits en l'àmbit internacional, es poden fer servir potencialment per crear un perfil complet d'un passatger a partir de la informació dels vols i fins i tot de la tria del menú, i partint d'aquesta informació es poden prendre decisions sobre la fiabilitat dels viatgers. Així mateix, davant del gran interès de les asseguradores per comprar a la policia les dades de seguiment de les matrícules dels vehicles per tal d'afinar les primes que cobren, i davant dels mètodes de puntuació de risc que s'apliquen cada vegada més en el control de les fronteres i en les eines de reputació a Internet, l'ús de *data doubles* pot tenir efectes molt concrets en la nostra vida quotidiana d'una manera que no sempre podem controlar, o bé pot arribar a consolidar les desigualtats socials.

La creixent confiança dipositada en els *data doubles* prové de la fe en la veracitat de les dades, però la *inexactitud* potencial d'aquestes dades pot tenir conseqüències socials nocives. El retrat que es genera quan s'agreguen bits d'informació de les nostres activitats digitals quotidianes sovint és una caricatura de la persona en qüestió. Un dels millors exemples d'això el trobem quan, en cas de robatori d'identitat, la solvència d'un individu pot no reflectir la seva trajectòria vital real. La confiança dipositada en els *data doubles* també modifica la relació entre els ciutadans i l'Estat: els estats recorren cada cop més a les dades i es tornen més desconfiats, de manera que les persones són tractades com a punts de dades potencialment sospitoses més que no pas com a ciutadans.

Guide to Self Defence Tools

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.

Coses que s'han dit

Citacions destacables sobre la vida en les Guerres de la vigilància

«Un informe de la Càmera dels Lords de 2009 descrivia l'explosió de les tecnologies de vigilància com un dels canvis més importants que s'han produït a la Gran Bretanya des de la Segona Guerra Mundial. [...] Aquest fenomen s'ha considerat un preu acceptable a canvi d'una major seguretat, però els estudis sobre tecnologia de vigilància no recolzen aquest argument.

Una anàlisi de 44 estudis independents de càmeres de seguretat, publicat el mateix any que l'informe de la Càmera dels Lords, demostrava que els més de cinc-cents milions de lliures esterlines (uns 630 milions d'euros) invertits en càmeres de seguretat a la Gran Bretanya durant la dècada anterior al 2006 havien produït uns beneficis modestos. La conclusió més demolidora de l'informe era que en l'aplicació en què les càmeres de seguretat resultaven més eficaces –la d'evitar delictes en els aparcaments públics– era possible obtenir els mateixos resultats simplement millorant la il·luminació de les zones d'aparcament.»

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

«És difícil explicar al públic general l'escàs rendiment de la tecnologia, fins a quin punt la infraestructura de les nostres vides se sosté amb l'equivalent informàtic de la cinta adhesiva. Els ordinadors i la informàtica ja no funcionen. [...]

Cada vegada que descarreguem una actualització de seguretat, el que estem actualitzant no se sap quant de temps fa que està espatllat, que és vulnerable. De vegades són dies, de vegades són anys. I ningú dóna publicitat a aquesta part de les actualitzacions. Ens diuen: "Heu d'instal·lar això, és un pegat essencial", però no que és així "perquè els desenvolupadors la van espifiar de tal manera que és probable que en aquest precís instant uns nens addictes al cavall estiguin venent les identitats dels vostres fills a la màfia estoniana".»

Quinn Norton
Periodista i escriptora especialitzada en tecnologia
«Everything is Broken», *Medium*
https://medium.com/message/81e5f33a24e1

«Els telèfons mòbils són dispositius de localització que també fan trucades telefòniques. És trist, però és cert. Encara que tingueu una sèrie d'eines segures al telèfon, això no canvia el fet que l'aparell registra tots els vostres passos. I que la policia podria instal·lar-hi actualitzacions per transformar-lo en un micròfon, convertint-lo en una mena de porta del darrere, i fer altres coses semblants.

La policia pot identificar tots els participants en una manifestació per mitjà d'un dispositiu anomenat *IMSI catcher*. És com una antena de telefonia falsa que es pot fabricar per 1.500 dòlars (uns 1.150 euros). Tots els telèfons mòbils que estan a prop es connecten automàticament a aquesta torre i, si l'identificador exclusiu del telèfon queda exposat, la policia no ha de fer res més que acudir a l'empresa de telefonia i sol·licitar la informació de l'usuari.»

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

«Tot el que fem avui en dia passa per Internet. Tot el que farem demà necessitarà Internet. Si viviu a prop d'una central nuclear, si voleu en avions, si viatgeu en cotxe o en tren, o si teniu un marcapassos, diners al banc o un telèfon mòbil, la vostra seguretat i el vostre benestar depenen d'unes xarxes segures que evolucionin contínuament.

Això és el més alarmant de les revelacions de Snowden: no solament que els espies ens espien a tots, sinó que tota la nostra infraestructura tecnològica està sotmesa a un sabotatge actiu per garantir que aquest espionatge continuï.

No és possible reduir la seguretat de manera que es pugui espiar "els dolents" sense que, alhora, tots siguem vulnerables "als dolents".»

Cory Doctorow
Escriptor
«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 conseqüència no desitjada de totes aquestes noves tecnologies de vigilància és que la tasca periodística és immensament més difícil que abans. Els periodistes han de parar especial atenció a qualsevol tipus de senyal de xarxa, a qualsevol tipus de connexió, a qualsevol tipus de dispositiu de lectura de matrícules de cotxes que es trobi en el seu camí fins al punt de trobada, a qualsevol lloc en què utilitzin la targeta de crèdit o portin el telèfon mòbil, a qualsevol contacte de correu electrònic que tinguin amb la font, perquè fins i tot el primer contacte que es produeixi, abans que s'estableixi la comunicació per un mitjà encriptat, és suficient per espatllar-ho tot.

Els periodistes han d'anar amb molt de compte de no cometre cap errada des del començament fins a la fi de les seves relacions amb les fonts per no posar en perill a aquestes persones. Els advocats es troben en la mateixa situació. I els investigadors. I els metges.»

Edward Snowden
Antic analista d'intel·ligència i informant
Entrevista d'Alan Rusbridger, *The Guardian*
http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript

«No n'hi ha prou amb encriptar-ho tot. A part de ser molt complicat, no seria suficient. A més d'encriptar-ho tot, però, podem fer altres coses. La descentralització total seria un gran canvi.

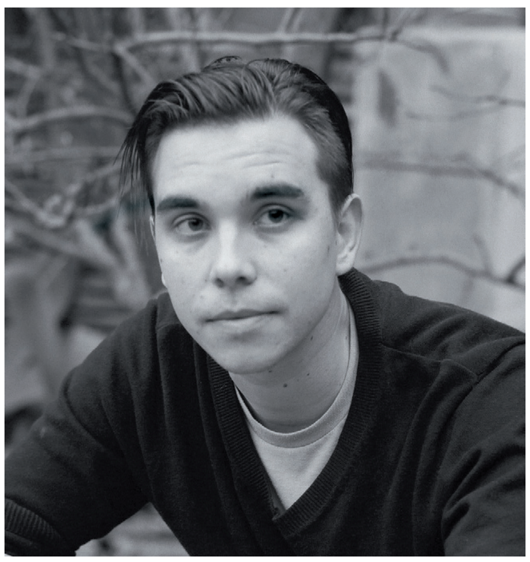
Una de les raons que expliquen l'èxit de la NSA (l'Agència de Seguretat Nacional dels Estats Units) es pot resumir en l'afirmació següent: "si no podem saltar-nos els vostres sistemes de seguretat, o si punxar les comunicacions ens causarà massa problemes, ens presentarem amb una carta i haureu de fer el que us ordenem". Això també pot passar en molts altres llocs. No tenim gaire informació sobre qui més intenta obligar les empreses a fer aquestes coses, però posaria la mà al foc que, si la NSA ho està fent, no és ni de bon tros l'única.

[...] S'ha acabat, ja no podem fiar-nos dels serveis centralitzats, aquesta és la realitat; és impossible crear una Internet lliure si està centralitzada.»

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

«Si creieu que els vostres problemes de seguretat es poden solucionar amb la tecnologia és que no enteneu ni els vostres problemes ni la tecnologia.»

Bruce Schneier
Criptògraf i expert en seguretat informàtica
Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons, 2000




→ James Bridle
Quinn Norton

Things They've Said

Quotes from 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 whoknows-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.

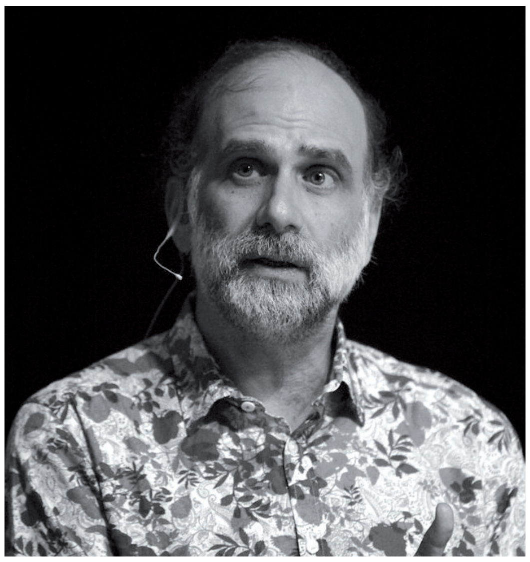
Eleanor Saitta
Computer security expert
"Ethics and Power in the Long War", *NoisySquare*
https://noisysquare.com/ethics-and-power-in-the-long-war-eleanor-saitta-dymaxion/

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

↓ Edward Snowden

↓ Eleanor Saitta
Bruce Schneier



Exposició / Exhibition «Big Bang Data»

© Gunnar Knechtel Photography

Exposició «Big Bang Data»

El Centre de Cultura Contemporània de Barcelona (CCCB) presenta «Big Bang Data», una exposició sobre l'emergència de les dades i els seus efectes culturals, polítics i artístics comissariada per José Luis de Vicente i Olga Subirós.

L'exposició tracta diverses dimensions dels actuals discursos i estratègies centrats en les dades: des de l'emergent i discutit paradigma científic del Big Data fins a la instrumentalització del món i la multiplicació dels dispositius de detecció, passant per la mercantilització de la identitat als mitjans socials i les indústries del *quantified self*. L'exposició també aborda la cultura de la vigilància en el món post-Snowden i els riscos d'una política i una ètica quantitatives, governades per les dades.

«Big Bang Data» ofereix una àmplia exploració d'aquest camp cultural combinant l'art contemporani i projectes de disseny, documentació històrica, vídeos d'entrevistes i prototips de noves tecnologies i serveis, i inclou també un laboratori actiu que allotja projectes i activitats participatives diàries mentre duri l'exposició.

La nòmina d'artistes i dissenyadors participants inclou, entre molts altres noms, els de Mark Lombardi, Diller and Scofidio, David Bowen, Ingo Gunther, Aaron Koblin, Fernanda Viegas i Paolo Ciri.

Aquesta publicació, *Anonimitza't. Manual d'Autodefensa electrònica*, ofereix un conjunt de recomanacions, eines i pràctiques per preservar el nostre sentit de la privacitat en el món post-Snowden.

L'exposició es presenta al CCCB entre el 9 de maig i el 16 de novembre del 2014. El 2015 itinerarà a la Fundació Telefónica de Madrid, abans de començar una gira internacional.

Big Bang Data" Exhibition

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.

Direcció i coordinació del projecte / *Project direction and coordination*
Servei d'Exposicions del CCCB
CCCB Exhibitions Service

Comissariat / *Curatorship*
José Luis de Vicente
Olga Subirós

Direcció de les activitats
Activities direction
ZZINC

Anonimitza't. Manual d'autodefensa electrònica
Anonymise Yourself. Electronic Self-Defence Handbook

Direcció / *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 i realització de la infografia / *Idea and production of infographics*
Olga Subirós

Disseny gràfic i maquetació / *Graphic design and layout*
David Torrents
Silvia Míguez

Coordinació i edició de textos / *Text editing and coordination*
Marina Palà
Rosa Puig

Traducció i correcció
Translation and proofreading
Marc Jiménez Buzzi
Bernat Pujadas
Blanca Rodríguez
Debbie Smirthwaite

D.L. B 20599-2014

Una coproducció
Coproduction

CCCB Centre de Cultura Contemporània de Barcelona
Telefónica Fundación

Amb el patrocini de
Sponsored by

Generalitat de Catalunya
Fundació BancSabadell
hp
FUJIFILM
FOTOPRIX
FOR A GOOD REASON GRUNDIG

Mitjans col·laboradors
Collaborating media

EL PAÍS
3
CATALUNYA RÀDIO

El CCCB és un consorci de
CCCB is a consortium of

Diputació Barcelona
Ajuntament de Barcelona

I la col·laboració de
With the collaboration of

Telefónica Investigación y Desarrollo
bcnlab ciència ciutadana
MEDIAPRO
IAAC FAB LAB BARCELONA
FAB 10
LOOP BARCELONA
sónar 2014 +D
MORITZ BARCELONA

ACTIVITATS DE L'EXPOSICIÓ **BIG BANG DATA - ESTACIÓ BETA**

Big Bang Data és la primera edició de Beta, una sèrie de projectes que analitzen la cultura del segle XXI i les grans transformacions del nostre present, explorant les interseccions entre la cultura, la tecnologia i la societat. Cada edició de Beta inclou una exposició i un espai laboratori integrat, l'Estació Beta, que acull processos de producció, recerca i divulgació.

Lloc: Estació Beta, l'espai taller de l'exposició «Big Bang Data», Sala 3 del CCCB, llevat que s'indiqui un altre lloc.
Entrada: Lliure fins a completar l'aforament. Inscripció prèvia: http://bigbangdata.cccb.org/inscripcio-espai-beta/, llevat que s'indiqui el contrari.

■ Activitats familiars ■ Debats i trobades ■ Festivals i seminaris ■ Tallers i *hackatons*

SETEMBRE

■ **Dm. 9, 19-21 h**
Tertúlia Recerca i Big Data
«La tecnologia darrere del Big Data»
A càrrec de **Mario Macías** (enginyer en Informàtica per la UAB i doctor en Arquitectura de Computadors per la UPC)
Entrada lliure amb inscripció prèvia

■ **Dc. 17, 16-20 h**
Taller Open Data
Anàlisi de dades
A càrrec de **Julià Minguillón** (professor agregat de la UOC i membre de Catalunya Dades)

■ **Dj. 18, 18.30-21 h**
Data Jam
A càrrec del col·lectiu d'artistes audiovisuals **Telenoika** i **Óscar Marín** (estudi de visualització Outliers)

■ **Dv. 19 - ds. 20**
Taller amb l'Institut de Govern i Polítiques Públiques (IGOP)
«Ús del Big Data en la investigació social i política»
Dv. 19, 18-20 h Presentació del taller i debat / Ds. 20, 11-20 h Taller
A càrrec de l'IGOP, amb la participació de **Jorge Luis Salcedo Maldonado**, **Mayo Fuster** i **Rubén Martínez**
Entrada lliure amb inscripció prèvia

■ **Dj. 25, 19-21 h**
Trobada Ciència ciutadana: les dades a les nostres mans
«Riu.net» i «Flora urbana i al·lèrgia, cooperes?»
A càrrec de **Freshwater Ecology Management Research** (UB) i **Punt d'Informació Aerobiològica** (XAC-UAB)

■ **Ds. 27, 12 h**
Visita comentada a l'exposició «Big Bang Data» a càrrec de la **Societat Catalana d'Estadística**.
Activitat exclusiva per als Amics del CCCB i els subscriptors de l'*Ara*

■ **Dg. 28, 11-13 h**
Taller en família
«Nosaltres al ciberespai»
A càrrec de **La Mandarina de Newton**
A partir de 6 anys
Entrada: 6 € / Gratuïta per als Amics del CCCB. Places limitades. Inscripció prèvia a les taquilles del CCCB

■ **Dm. 30, 11-14 h**
Taller Recerca i Big Data
«Ens ajudes a desxifrar el cervell? Projectes a gran escala per desxifrar el cervell»
A càrrec de **Jaime de la Rocha** i **Albert Compte** (investigadors principals de l'IDIBAPS)
Entrada lliure amb inscripció prèvia

■ **Dm. 30, 19-21 h**
Tertúlia Recerca i Big Data
«Supercomputació i cardiologia»
A càrrec de **Mariano Vázquez** i **Fernando Cucchietti** (investigadors del Barcelona Supercomputing Center) i **Francesc Carreras** (cardiòleg i investigador a l'Hospital de Sant Pau)
Entrada lliure amb inscripció prèvia

OCTUBRE

■ **Dc. 1, 16-20 h**
Taller Open Data
Visualització de dades, finalització del curs de quatre sessions
A càrrec de **Julià Minguillón** (professor agregat de la UOC i membre de Catalunya Dades)

■ **Dj. 2, 17-21 h**
Jornada sobre Big Data en els estudis d'Humanitats
17 h Presentació de ponències / 19.30 h Taula rodona
«Com utilitzar PhiloBiblon? Tecnologies per estudiar els manuscrits ibèrics medievals», a càrrec de **Gemma Avenoza** (UB); «Laboratorio de Innovación en Humanidades Digitales (LINHD)», a càrrec d'**Elena González-Blanco** (UNED); «Centro de Competencias en recursos y tecnologías lingüísticas IULA-UPF-CC-CLARIN», a càrrec de **Núria Bel** (UPF) i «La història digital de l'art i les humanitats digitals», a càrrec de **Núria Rodríguez** (Universidad de Málaga)
Organitzada per **María Morrás** i **Antonio Rojas** (Departament d'Humanitats de la UPF)
Entrada lliure amb inscripció prèvia

■ **Dv. 3, 19-21 h**
Trobada de programació creativa: Visualització de dades
A càrrec de **Telenoika**, **MIRA** i **ZZZINC**

■ **Dg. 5, 11-13 h**
Taller en família
«Geolocalitzem!»
A càrrec de **La Mandarina de Newton**
A partir de 6 anys
Entrada: 6 € / Gratuïta per als Amics del CCCB. Places limitades. Inscripció prèvia a les taquilles del CCCB

■ **Dm. 7, 19-21 h**
Tertúlia Recerca i Big Data
«EPNet: Big Data en història»
A càrrec de **José Remesal** (catedràtic d'Història Antiga a la Facultat de Geografia i Història de la UB), **Albert Diaz-Guilera** (coordinador de la xarxa d'investigadors en sistemes complexos a Catalunya), **Xavier Rubio Campillo** (investigador del Barcelona Supercomputing Center) i **Alessandro Mosca** (investigador del SIRIS Lab de SIRIS Academic SL)
Entrada lliure amb inscripció prèvia

■ **Dc . 8, 19-21 h**
Tertúlia Recerca i Big Data
«Big Data Analytics i geolocalització aplicats al màrqueting de clients»
A càrrec de **Pau Agulló** (director general i cofundador de Kernel Analytics) i **Manuel Bruscas** (cofundador de Bcn Analytics i cap d'Analytics & Insights de Desigual)
Entrada lliure amb inscripció prèvia

■ **Dj. 9, 17-20 h**
Periodisme de dades. Sessió de treball (VI)
«Observant les dades del meu municipi»
Amb la participació de **Karme Peiró** i **Carlos Alonso**
Entrada: 3 € / Gratuïta per als Amics del CCCB, els aturats i amb el carnet del Col·legi de Periodistes

■ **Ds. 11, 11-20 h**
Hackató Astronòmica
«Un univers de dades»
A càrrec de: **ZZZINC** i **Outliers**, amb la col·laboració del **CCCB LAB** i **Sebastián Pérez** (doctor en Astrofísica i investigador postdoctoral de la Universitat de Xile), en el marc del projecte **Anilla Cultural Latinoamérica-Europa**
Entrada lliure amb inscripció prèvia

■ **Dm. 14, 19-21 h**
Tertúlia Recerca i Big Data
«Big Data en l'estudi del cervell»
A càrrec de **Joan Guàrdia** (catedràtic de Metodologia de la Facultat de Psicologia de la UB i investigador de l'Institut de Recerca en Cervell, Cognició i Conducta, IR3C) i **Albert Barqué** (investigador doctorand en Ciències Cognitives i autor de «Neurocàpsules» a El Periódico)
Entrada lliure amb inscripció prèvia

■ **Dc. 15, 19-21 h**
Tertúlia Recerca i Big Data
«Big Data i genòmica»
A càrrec de **Modesto Orozco** i **Cédric Notredame** (Centre de Regulació Genòmica)
Entrada lliure amb inscripció prèvia

■ **Dj. 16, 18.30-21 h**
Data Jam
A càrrec del col·lectiu d'artistes audiovisuals **Telenoika** i **Óscar Marín** (estudi de visualització Outliers)

■ **Dg. 19, 11-13 h**
Taller en família
«Satèl·lits i petjades!»
A càrrec de **La Mandarina de Newton**
A partir de 6 anys
Entrada: 6 € / Gratuïta per als Amics del CCCB. Places limitades. Inscripció prèvia a les taquilles del CCCB

■ **Dm. 21, 19-21 h**
Tertúlia Recerca i Big Data
«Open Data a la UPF»
A càrrec de **Jordi Campos** (cap de la unitat d'Organització i Processos de la UPF)
Entrada lliure amb inscripció prèvia

■ **Dc. 22, 11.30-19h**
Jornada «El Big Data en la innovació de Telefónica I+D»
Amb la participació de **Rafael Pellón**, **Enrique Frías**, **José Luis Agúndezi** i **Alexandros Karatzoglou** (investigadors de Telefónica I+D)
Entrada lliure amb inscripció prèvia

■ **Dj. 23, 18-21 h**
Trobada **Barcelona Urban Beers**

■ **Dv. 24, 19-21 h**
Trobada Ciència ciutadana: les dades a les nostres mans
«Mobilitat humana i altres experiments de comportament humà»
A càrrec de **ComplexitatLab** (UB), **OpenSystemsUB** i **ICREA-Movement Ecology Laboratory** (CEAB-CSIC, CREAF)

■ **Dc. 29, 19-21 h**
Tertúlia Recerca i Big Data
«Cultural Data. Open Data i xarxes socials a les institucions culturals»
Presentació de l'Estudi sobre les xarxes socials de les institucions culturals a Espanya, a càrrec d'**Encarna Segura** (directora de Social Win), i presentació de les últimes novetats del projecte GLAM-WIKI, a càrrec d'**Àlex Hinojo**.
Moderada per **Olga Subirós** (comissària de l'exposició)
Entrada lliure amb inscripció prèvia

NOVEMBRE

JORNADES «THE COLD WEB»

Dj. 6 - dv. 7
Com a cloenda de les activitats presentades en el marc del projecte Big Bang Data, l'Obra Social "La Caixa", en col·laboració amb el CCCB, organitza les jornades «The Cold Web. Autoprotecció i defensa de la privacitat en l'era de la vigilància massiva» al Palau Macaya, amb l'objectiu d'aprofundir i amplificar els temes que aborda aquesta publicació. Les jornades consistiran en una sèrie de sessions de debat amb experts internacionals i un taller pràctic per aprendre a utilitzar eines d'encriptació informàtica.
Entrada lliure amb inscripció prèvia: http://bigbangdata.cccb.org/inscripcio-espai-beta

Consulteu la programació més detallada a: www.cccb.org/ca/exposicio-big_bang_data-45167

Check the programme in English at: http://www.cccb.org/en/exposicio-big_bang_data-45167

Descobriu a **www.bdigitalglobalcongress.com** tot el contingut i les conclusions de **The Big Digital Bang**, la 16a edició del BDigital Global Congress 2014, focalitzada a explorar les tendències tecnològiques que han revolucionat diferents sectors del mercat (Big Data, Wearable Technologies i Innovació i tendències de futur).

Exposició «Big Bang Data»
Del 9 de maig al 16 de novembre de 2014
De dm. a dg. - d'11 h a 20 h
www.bigbangdata.cccb.org
@_BigBangData #BBData

CCCB
Montalegre, 5 - 08001 Barcelona
T. 93 306 41 00. www.cccb.org