Seminar of digital democracy

Privacy, surveillance and democratic challenges in the digital age

Nicolas Bocquet
bocquetnicolas@pm.me

8 December 2022

Plan

1) Context: privacy in a surveillance society, the smartphone example
2) Privacy regulation history
3) “I have nothing to hide”
4) Web-tracking
5) Conclusion and resources
6) Q&A, discussion

GAFAM users?

WHO

1) does not have a smartphone?

2) has a Google account?

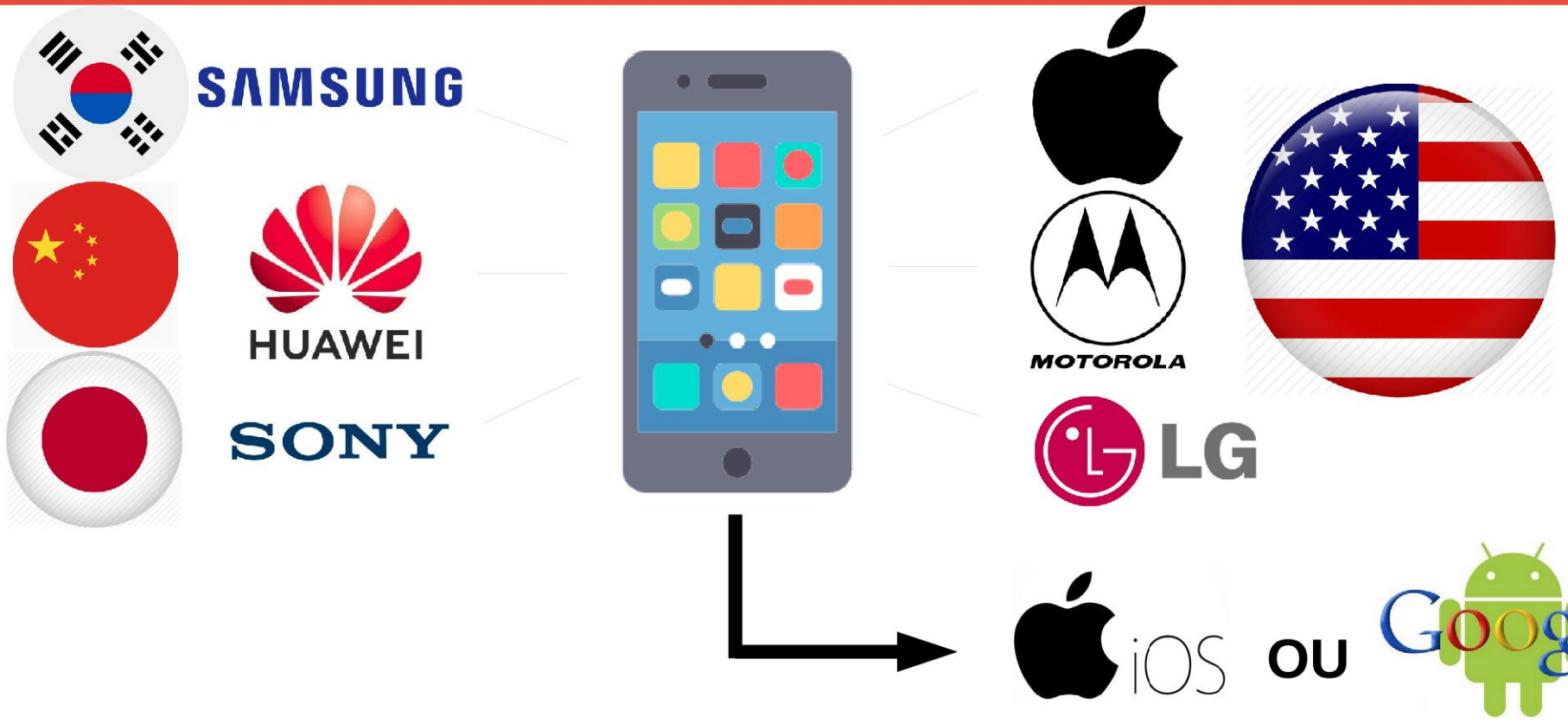
3) has a Facebook account?

4) uses other services owned by Facebook (such as WhatsApp or Instagram)?

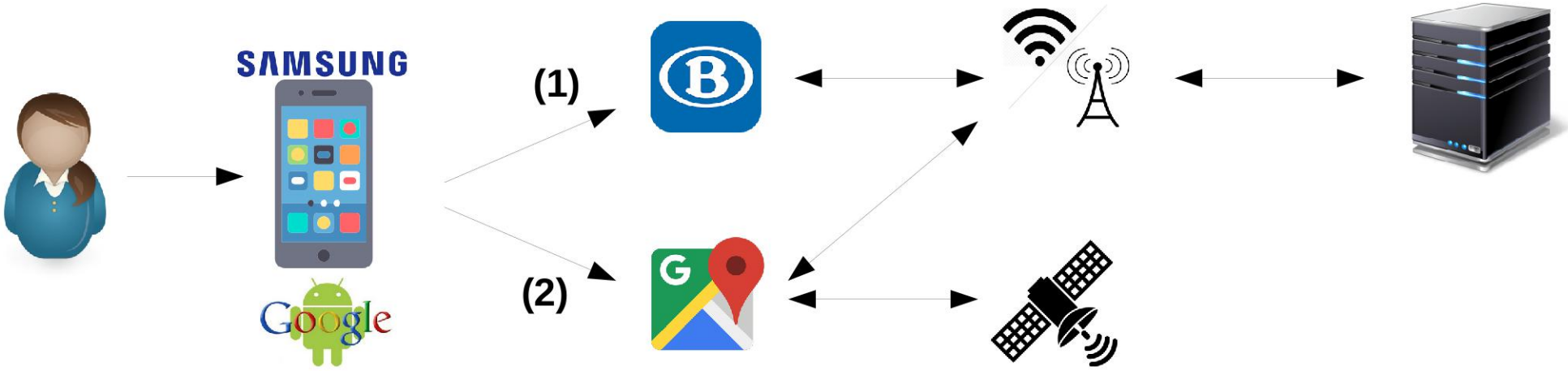
5) uses free and open source software?

6) Does anyone think he/she doesn't care about privacy because he/she has nothing to hide?

1. Context: example of the smartphone



(1) Train schedule
(2) Way to the station



ACTORS

Hardware: SAMSUNG

Software: Google

Service: SNCB Google

Infrastructure: proximus

Host: Microsoft Google

+ bonus 1: App trackers

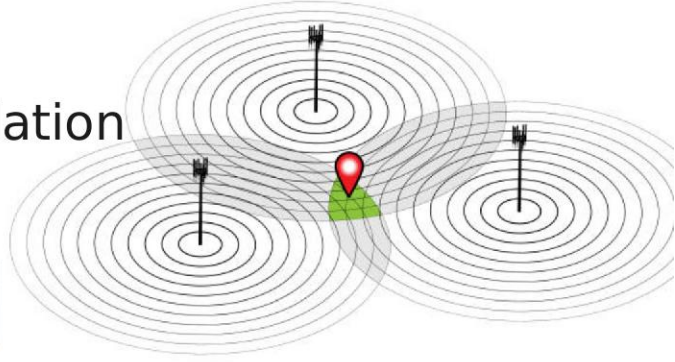
Version 9.4 of the 'SNCB International' app

- **8 trackers**
  - ✔ 4 belonging to facebook
  - ✔ 4 belonging to Google
- **13 permissions including**
  - ✔ Call log
  - ✔ Location
  - ✔ Storage

+ bonus 2: telephone infrastructure

Telephone network not designed to be confidential and secure…

- **SIM card** = unique identifier linked to your **ID**
- Every call/SMS/Internet access = accessible **in clear to the operator/ intelligence services/police** → no encryption/security
- Operator knows **location in real time** (even if GPS disconnected) → triangulation of antennas to which the phone is connected
  - Precision depends on technology/environment
- **2020 CJEU decision** → unconstitutionality of the retention of telephone (meta)data of the entire population



+ bonus 3: spyware and zero-day exploit

Zero-day vulnerability

- Vulnerability in the code **unknown to developers** and **found by hackers**
- **'Black market'** of companies (like NSO) paying a lot of money for these vulnerabilities in order to compile them to **create spyware** (Pegasus, Predator)
- Spyware giving **full access to devices** without user's knowledge (camera, mic, location, msgs, calls, etc.) **sold to governments** to « fight terror and crime »
- But **big governments' abuses** and **big threat to human rights → no international regulation** so far (cyberweapons ≠ like other weapons?)

Pegasus in numbers	Targets	Confirmed NSO clients
More than 50'000 victims in more than 45 countries	Human rights activists, journalists, lawyers, political opponents, leaders, etc.	Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, UAE

1. Privacy in a surveillance society ?

Privacy = societal issue disrupted by the « digital revolution »

(1) Explosion of **means of collecting /processing**

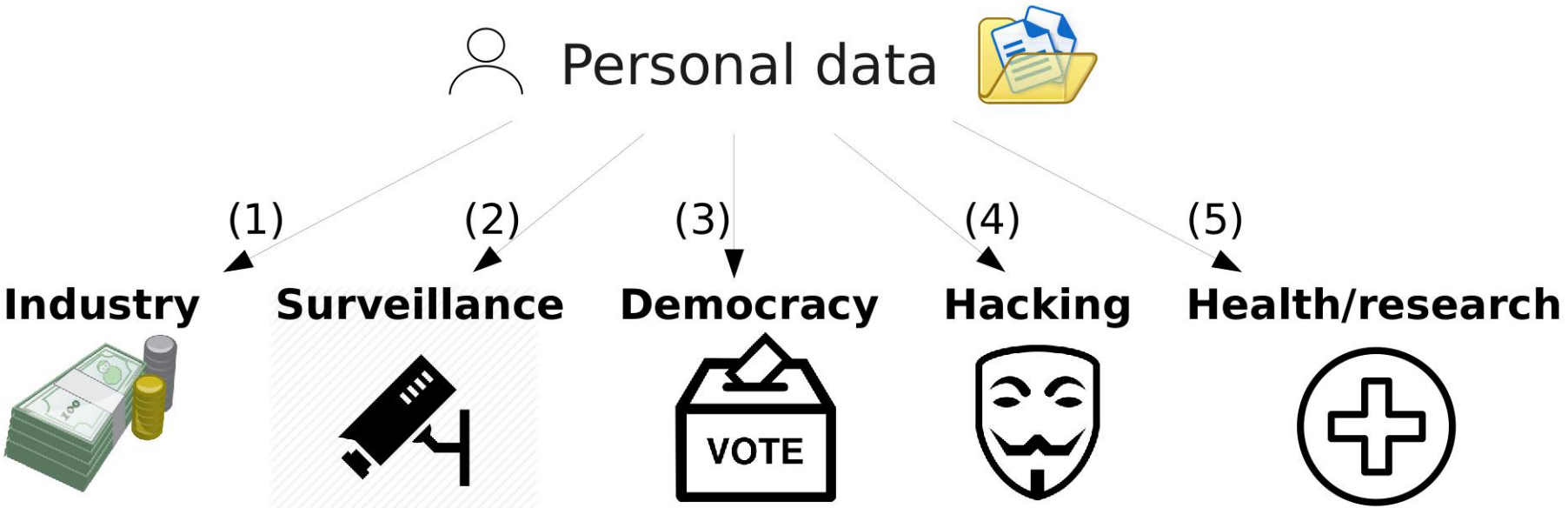
(2) Increasing **internationalisation**

(3) Increasing **technical complexity**

(4) Lack of **transparency**

1. Privacy in a surveillance society ?

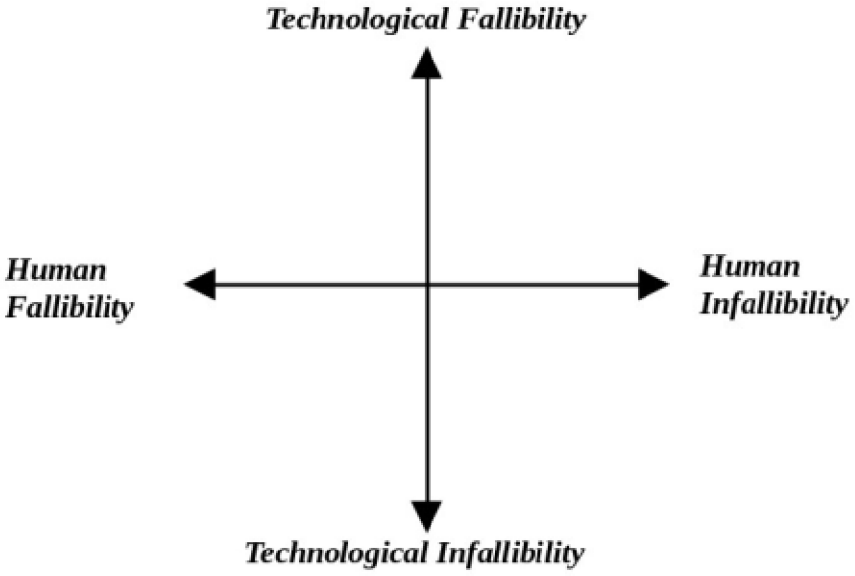
Privacy = societal issue disrupted by the « digital revolution »



1. Privacy in a surveillance society ?

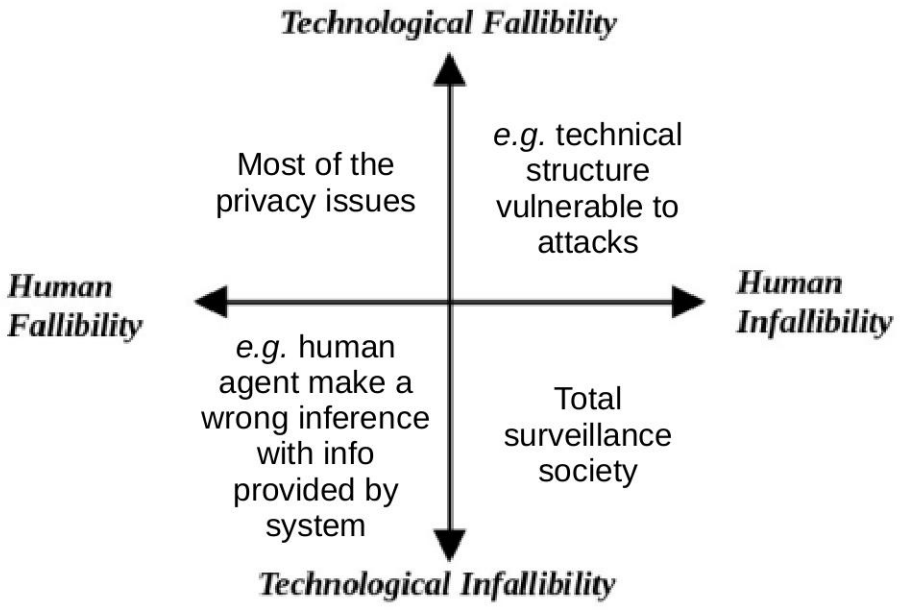
- **Technology** as a **social construct** → **never neutral** and **privacy** as a response to **surveillance**
- Privacy as an issue at the crossroads of **technological** and **human fallibility**

Figure 1: A matrix of privacy problem (according to Bennett & Raab 2006)



1. Privacy in a surveillance society ?

Figure 1: A matrix of privacy problem (according to Bennett & Raab 2006)



2. Privacy regulation history

The success story of a paradigm of which we are now “prisoners”

The « **privacy paradigm** » as:

- Result of an **international consensus of experts** (OECD)
- Coming from **liberal tradition** → atomistic conception of society (Locke, Mill)
- Privacy as a **prerequisite for democracy**
  - Counter-powers (civil society, independence media + protection sources, …)
  - Secret ballot
  - Source of other fundamental freedoms (opinion, expression, assembly, movement, innocence)

2. Privacy regulation history

- Permanent fear of an **authoritarian shift** (context of cold war)
- **State** (and police) = **main threat**
- **Problem-framing: bureaucratic tendency** to collect more and more personal data
- **Policy goal: give the individual back control** over personal data that state (and then private) organisations collect and process about him/her

3. Nothing to hide?

3. Nothing to hide?

Persistent myths:

- Eric Schmidt (Google) in 2009 : "*Only miscreants worry about net privacy*"
- Marc Zuckerberg (Facebook) in 2010 : "*Privacy is no longer a social norm*"
- "*We do not live in a dictatorship*"
- **"I have nothing to hide"**

3. Nothing to hide?

- Privacy = source of **individual well-being and development:**
  - Need to exist **outside the social gaze**
  - Intimacy necessary for the **construction of the "self"** and of your own ideas → develop **autonomous thinking** potentially at odds with the majority / dominant norms → otherwise risk of 'pack mentality'
  - Right to **make mistakes**, otherwise self-censorship, paranoia
- **Surveillance = loss of individual BUT also collective freedom…**

3. Nothing to hide?

- It is not you who **decides what you can be blamed for**, but those who monitor
- Very little information about you ⇒ **unsuspected correlations**
- ≠ doing something **illegal** (keys, passwords, etc.)
- **Social norms change**: behaviour considered acceptable today ≠ tomorrow
- **Other people** may have something to hide in a more immediate way

3. Nothing to hide?

Collective dimension of privacy:

- Protect yourself…
- But the PRIORITY IS TO **PROTECT OTHERS**, the weakest, those who are less in line with the dominant social norms, those who have less privileges (minorities, political opponents, etc.)

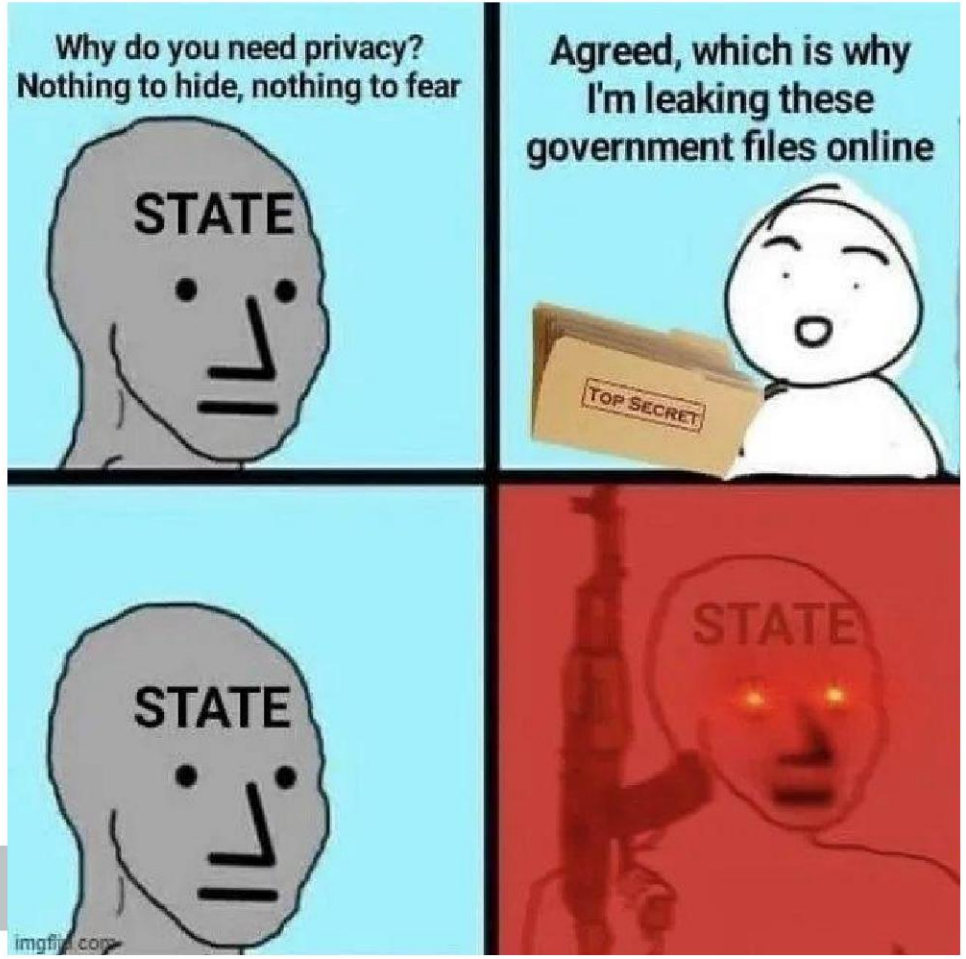
"Arguing that you don't care about the right to privacy because you have nothing to hide, is no different than saying you don't care about free speech because you have nothing to say."

Edward Snowden

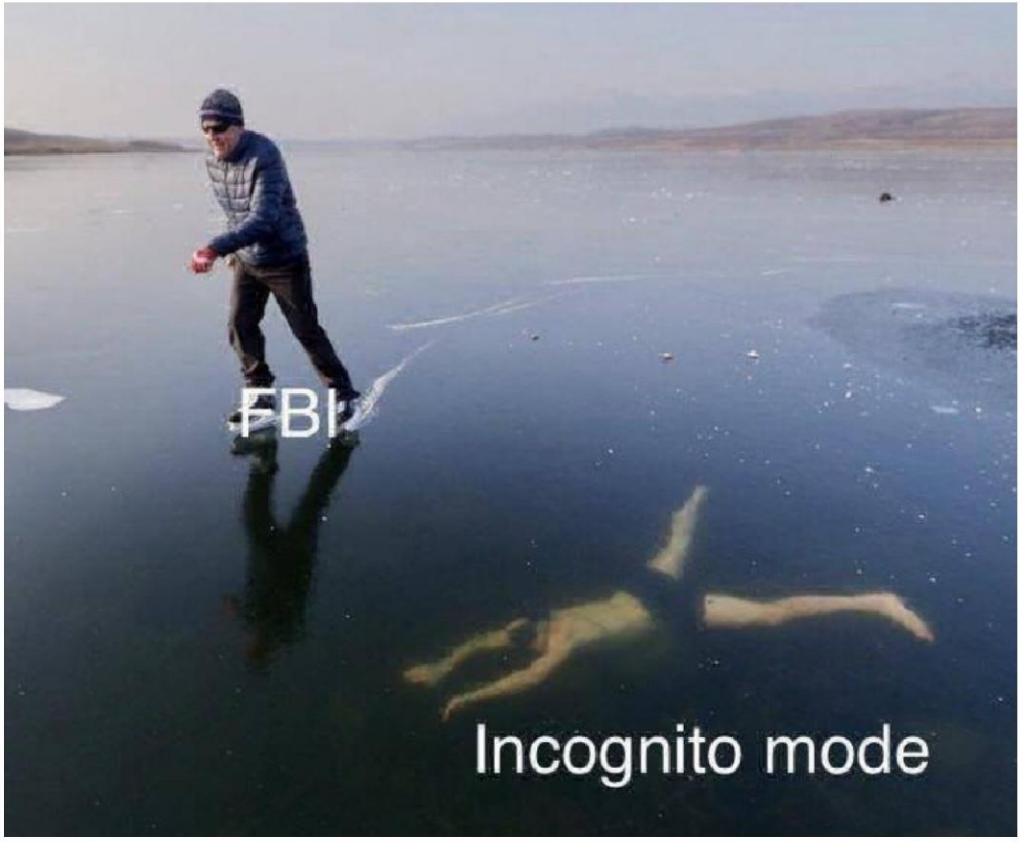
3. Nothing to hide?

- "I have nothing to hide" → **socially privileged position**
- Claim of **neutrality → power of surveillance**
- **Political function** of surveillance: monitoring, classifying and sorting all our behaviours to exclude or eliminate the undesirable, the subversive and thus **maintain the dominant order**
- Documentary "*Nothing to hide*" (2017) available for free access

3. Nothing to hide?



4. Web-tracking



4. How did we get from that...

Un article très très intéressant

Les origines de la surveillance globale remontent à la fin des années 1940, à la signature de l'accord secret UKUSA adopté conjointement par le Royaume-Uni et les États-Unis, qui aboutira en 1971 à la création du réseau de surveillance globale du nom de code « Echelon ».
Dans les années 1970, à la suite de l'affaire du Watergate et d'une enquête du Congrès des États-Unis qui suivit, on découvrit que la NSA, en collaboration avec son homologue britannique GCHQ, avait régulièrement intercepté les communications internationales d'importants militants et chefs de file de l'opposition à la guerre au Viêt Nam, tels que Jane Fonda et le Dr Benjamin Spock. Des décennies plus tard, une enquête conduite pendant plusieurs années par le Parlement européen mit en évidence le rôle de la NSA dans l'espionnage économique, dans un rapport intitulé Development of Surveillance Technology and Risk of Abuse of Economic Information (Développement des technologies de surveillance et risque d'abus dans l'information économique) et publié en 19993.
Toutefois, pour le grand public, c'est la série de divulgations détaillées de documents internes à la NSA, en juin 2013, qui révéla pour la première fois l'échelle considérable de l'espionnage de la NSA, aussi bien à l'intérieur qu'à l'extérieur des frontières des États-Unis. La plupart de ces documents furent divulgués par un ancien sous-traitant de la CIA et de la NSA, Edward Snowden.
Ainsi, nombre des programmes de surveillance globale plus anciens comme PRISM, XKeyscore et Tempora ont été cités dans les milliers de documents publiés en 2013. De nombreux pays, y compris des alliés occidentaux des États-Unis et des États membres de l'OTAN, ont été ciblés par l'alliance stratégique des « Five Eyes » (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis) – cinq démocraties occidentales et anglophones cherchant à atteindre la connaissance totale de l'information (Total Information Awareness) grâce au contrôle d'Internet, via des outils d'analyse comme le Boundless Informant (l'informateur sans limite).
Comme l'a confirmé le directeur de la NSA Keith Alexander le 26 septembre 2013, la NSA collecte et stocke toutes les données téléphoniques de tous les citoyens américains. La majorité des données sont conservées dans de grandes installations de stockage comme le centre de données de l'Utah, un énorme projet de 1,5 milliard de dollars qualifié par le Wall Street Journal de « symbole des prouesses en surveillance de l'agence d'espionnage ».
Les révélations d'Edward Snowden sur les activités de surveillance de la NSA sont dans la continuité de fuites dans la presse qui ont commencé au début des années 2000. Un an après les attentats du 11 septembre, l'ancien fonctionnaire du renseignement américain William Binney critiqua publiquement la NSA pour son espionnage des citoyens des États-Unis.
D'autres révélations ont suivi. Le 16 décembre 2005, le New York Times publia un reportage sous le titre « Bush laisse les États-Unis espionner les appels téléphoniques sans mandat ». En 2006, une nouvelle preuve de la surveillance intérieure exercée par la NSA sur les citoyens américains fut produite par USA Today. Le journal publia le 11 mai 2006 un rapport sur « l'énorme base de données » de la NSA, constituée des données d'appels téléphoniques de « dizaines de millions » de citoyens américains. Selon USA Today, ces données d'appels provenaient de plusieurs opérateurs de téléphonie tels que AT&T, Verizon et BellSouth.
En 2008, le spécialiste en sécurité Babak Pasdar révéla l'existence de ce qui fut appelé le « circuit Quantico », que lui et son équipe avait mis en place en 2003. Ce circuit fournissait au gouvernement fédéral américain une porte dérobée dans le réseau d'un opérateur de téléphonie mobile, dont le nom ne fut pas divulgué mais qui fut plus tard identifié comme étant Verizon.
Les premiers contacts établis par Snowden avec Glenn Greenwald, journaliste du quotidien The Guardian, datent de fin 2012. Depuis, les révélations de Snowden sur la surveillance de masse ont continué tout au long de l'année 2013 et se poursuivent en 2015.
Le 6 juin 2013, le quotidien britannique The Guardian commença la publication d'une série de révélations provenant d'un lanceur d'alerte américain jusqu'alors inconnu, qui s'est révélé quelques jours plus tard être Edward Snowden, un ancien administrateur systèmes sous-traitant de la CIA et de la NSA.
Snowden avait confié un ensemble de documents à deux journalistes : Glenn Greenwald et Laura Poitras ; Greenwald estimera plus tard qu'il contenait entre 15 000 et 20 000 documents, certains très longs et détaillés et d'autres très courts. Après plus de deux mois de publication, il apparut clairement que la NSA gérait un réseau complexe de programmes d'espionnage qui lui permettait d'intercepter les conversations téléphoniques et numériques de plus d'un milliard d'utilisateurs, situés dans des dizaines de pays à travers le monde. En particulier, certaines révélations concernaient la Chine, l'Union européenne, l'Amérique latine, l'Iran, le Pakistan, l'Australie et la Nouvelle-Zélande. Cependant, la documentation publiée révéla que de nombreux programmes collectaient en vrac et indistinctement de l'information directement depuis les serveurs centraux et les dorsales Internet qui transportent et routent le trafic de pays éloignés.
À cause de cette surveillance des serveurs centraux et des dorsales Internet, de nombreux programmes se chevauchent et sont en corrélation les uns avec les autres. Ces programmes ont souvent été réalisés avec l'aide d'entités fédérales comme le département de la Justice et le FBI. Ils ont été ratifiés par des lois telles que le FISA Amendments Act, et les ordonnances judiciaires nécessaires ont été signées par un tribunal secret, le Foreign Intelligence Surveillance Court. Certains des programmes

… to this?


Register
to get a free article
Email
Password
REGISTER


Do you have some splines that need reticulating?
YES
WHAT?


DOWNLOAD NOW
DOWNLOAD NOW
DOWNLOAD NOW


Mon site web préféré
Un article très très intéressant
Les origines de la surveillance globale remontent à la fin des années 1940, à la signature de l'accord secret UKUSA adopté conjointement par le Royaume-Uni et les États-Unis, qui aboutira en 1971 à la création du réseau de surveillance globale du nom de code « Echelon ».
Dans les années 1970, à la suite de l'affaire du Watergate et d'une enquête du Congrès des États-Unis qui suivit, on découvrit que la NSA, en collaboration avec son homologue britannique GCHQ, avait régulièrement intercepté les communications internationales d'importants militants et chefs de file de l'opposition à la guerre au Viêt Nam, tels que Jane Fonda et le Dr Benjamin Spock. Des décennies plus tard, une enquête conduite pendant plusieurs années par le Parlement européen mit en évidence le rôle de la NSA dans l'espionnage économique, dans un rapport intitulé Development of Surveillance Technology and Risk of Abuse of Economic Information (Développement des technologies de surveillance et risque d'abus dans l'information économique) et publié en 19993.
Toutefois, pour le grand public, c'est la série de divulgations détaillées de documents internes à la NSA, en juin 2013, qui révéla pour la première fois l'échelle considérable de l'espionnage de la NSA, aussi bien à l'intérieur qu'à l'extérieur des frontières des États-Unis. La plupart de ces documents furent divulgués par un ancien sous-traitant de la CIA et de la NSA, Edward Snowden.
Ainsi, nombre des programmes de surveillance globale plus anciens comme PRISM, XKeyscore et Tempora ont été cités dans les milliers de documents publiés en 2013. De nombreux pays, y compris des alliés occidentaux des États-Unis et des États membres de l'OTAN, ont été ciblés par l'alliance stratégique des « Five Eyes » (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis) – cinq démocraties occidentales et anglophones cherchant à atteindre la connaissance totale de l'information (Total Information Awareness) grâce au contrôle d'Internet, via des outils d'analyse comme le Boundless Informant (l'informateur sans limite).
Comme l'a confirmé le directeur de la NSA Keith Alexander le 26 septembre 2013, la NSA collecte et stocke toutes les données téléphoniques de tous les citoyens américains. La majorité des données sont conservées dans de grandes installations de stockage comme le centre de données de l'Utah, un énorme projet de 1,5 milliard de dollars qualifié par le Wall Street Journal de « symbole des prouesses en surveillance de l'agence d'espionnage ».
Les révélations d'Ed
2000. Un an après l
espionnage des citoy
D'autres révélations
téléphoniques sans
journal publia le 11 m
citoyens américains
En 2008, le spécialis
circuit fournissait au
fut plus tard identifi
Les premiers contact
la surveillance de m
Le 6 juin 2013, le qu
inconnu, qui s'est ré
Snowden avait confi
20 000 documents,
complexe de progra
des dizaines de pays
l'Australie et la Nouv
directement depuis
A cause de cette surveillance des serveurs centraux et des dorsales Internet, de nombreux programmes se chevauchent et sont en corrélation les uns avec les autres.
Ces programmes ont souvent été réalisés avec l'aide d'entités fédérales comme le département de la Justice et le FBI. Ils ont été ratifiés par des lois telles que le FISA Amendments Act, et les ordonnances judiciaires nécessaires ont été signées par un tribunal secret, le Foreign Intelligence Surveillance Court. Certains des programmes
Is it okay if we track you?
OK
NO


Man devastated to find all his work replaced with “content”


This man learned 12 languages but nobody wants to speak to him

4. Web-tracking

How can I be tracked online?

1) Browser tracking

2) IP address

3) Cookies

4) Fingerprinting

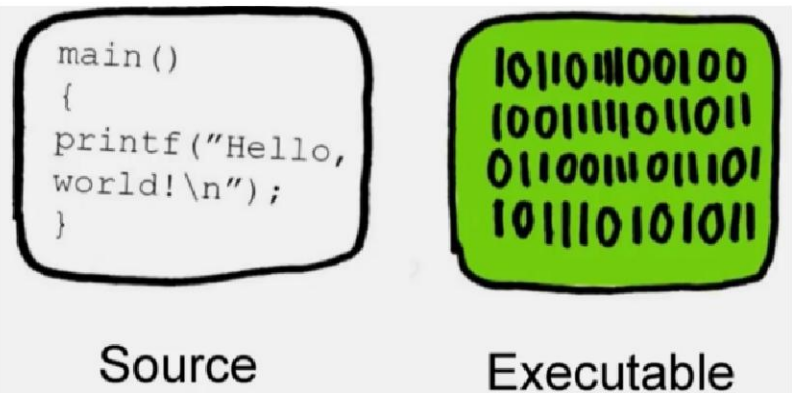
4. Browser tracking

What is software source code?

- Computer software has two forms:

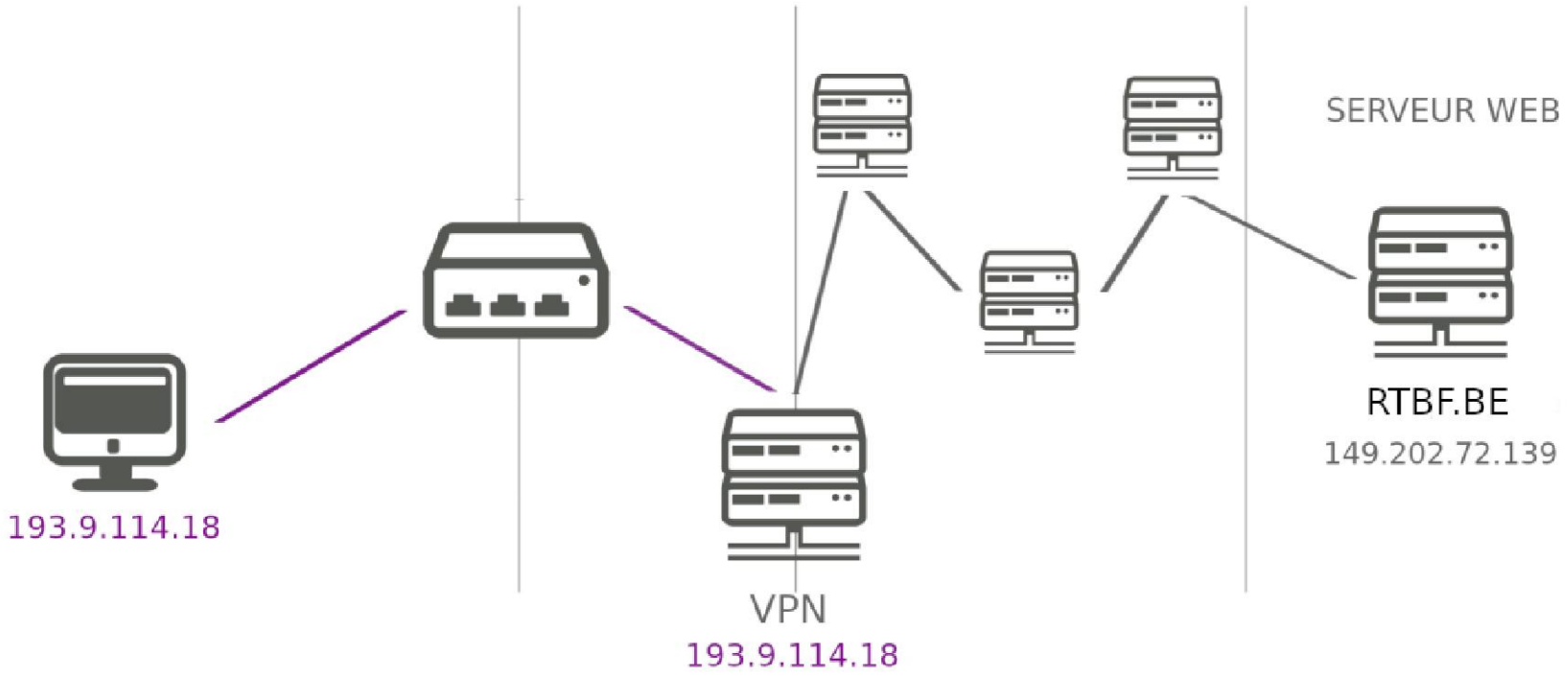
  1) Executable file: just machine instructions (in binary) → *proprietary software* → **Google Chrome or Safari**

  2) Source code: a text that can be read and understood (if you master the language) → *free and open source software* → **Firefox (or TOR)**

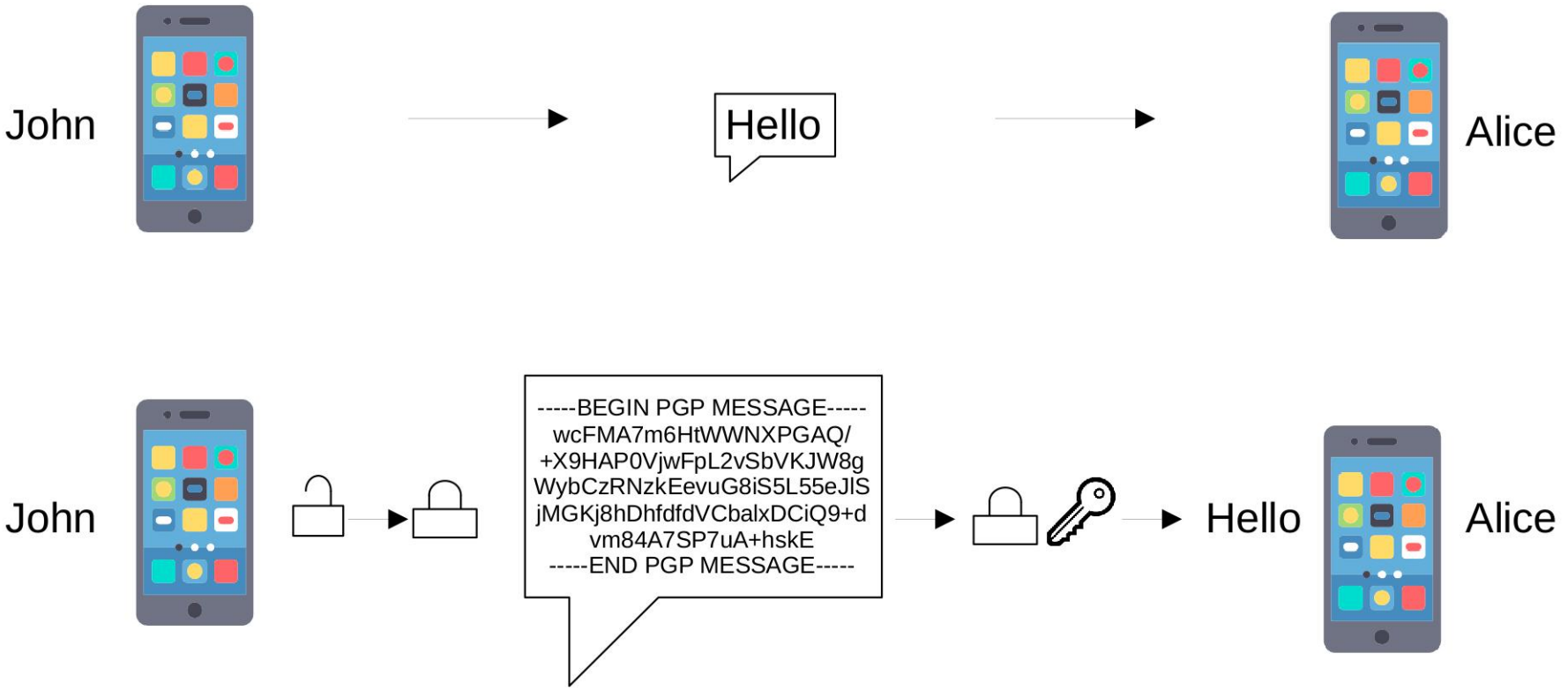


4. IP address

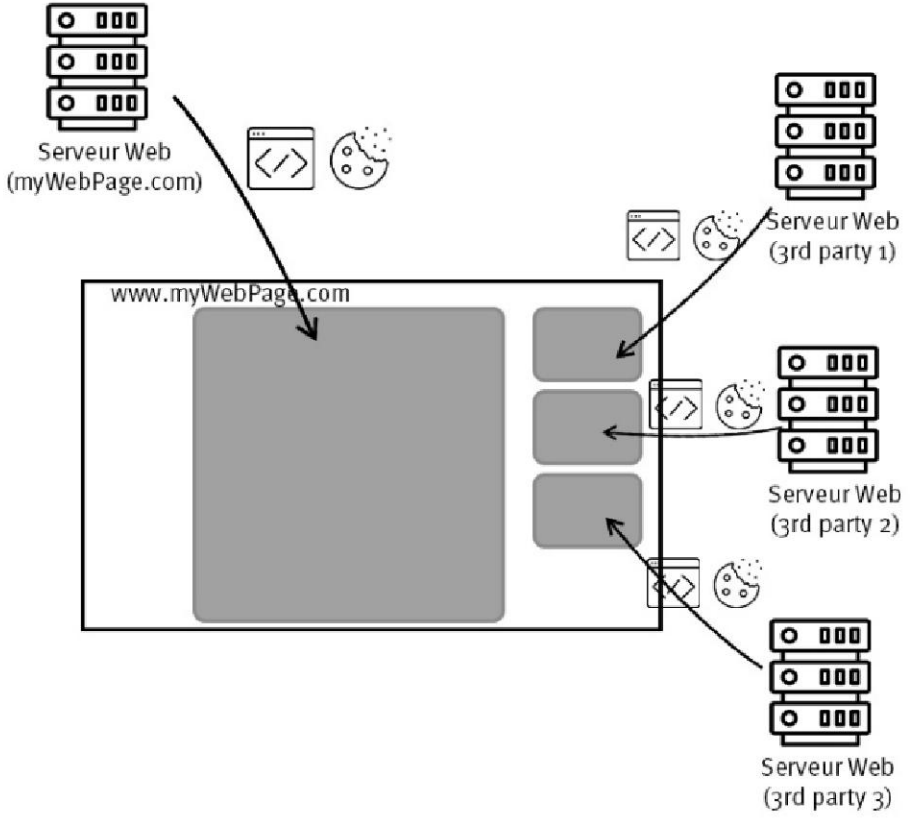
Using a VPN that is open source (or TOR)



4. Encryption

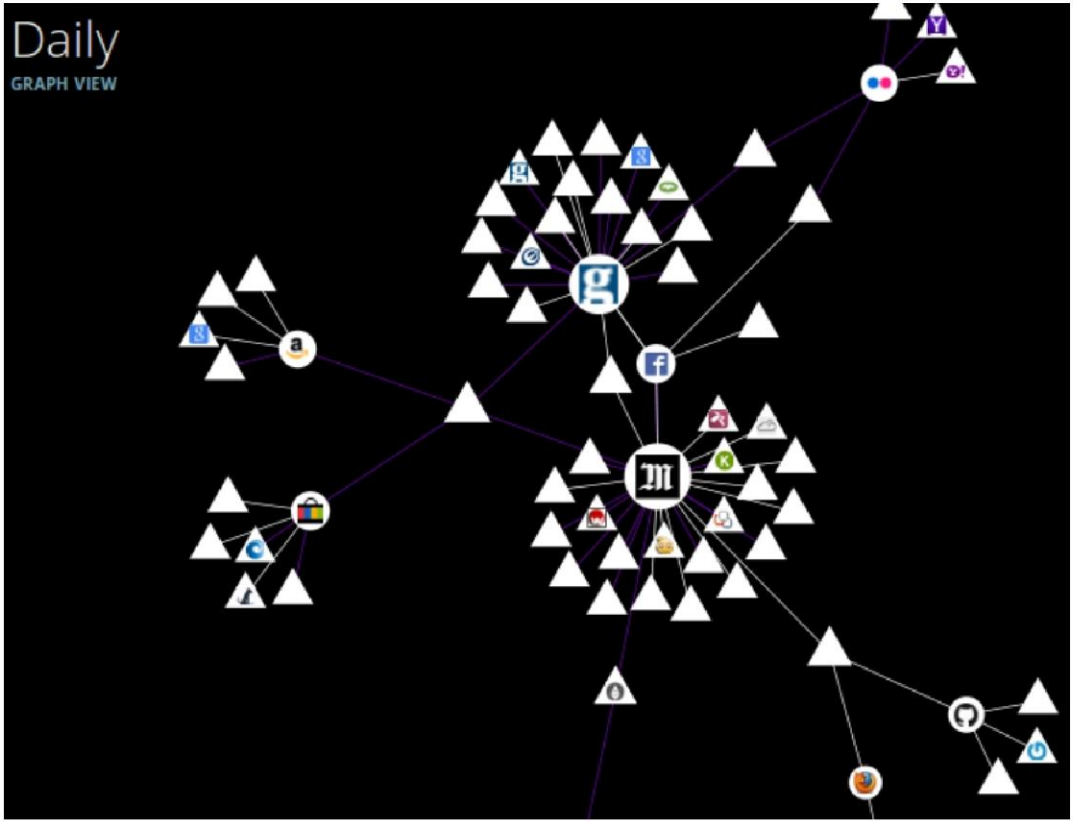


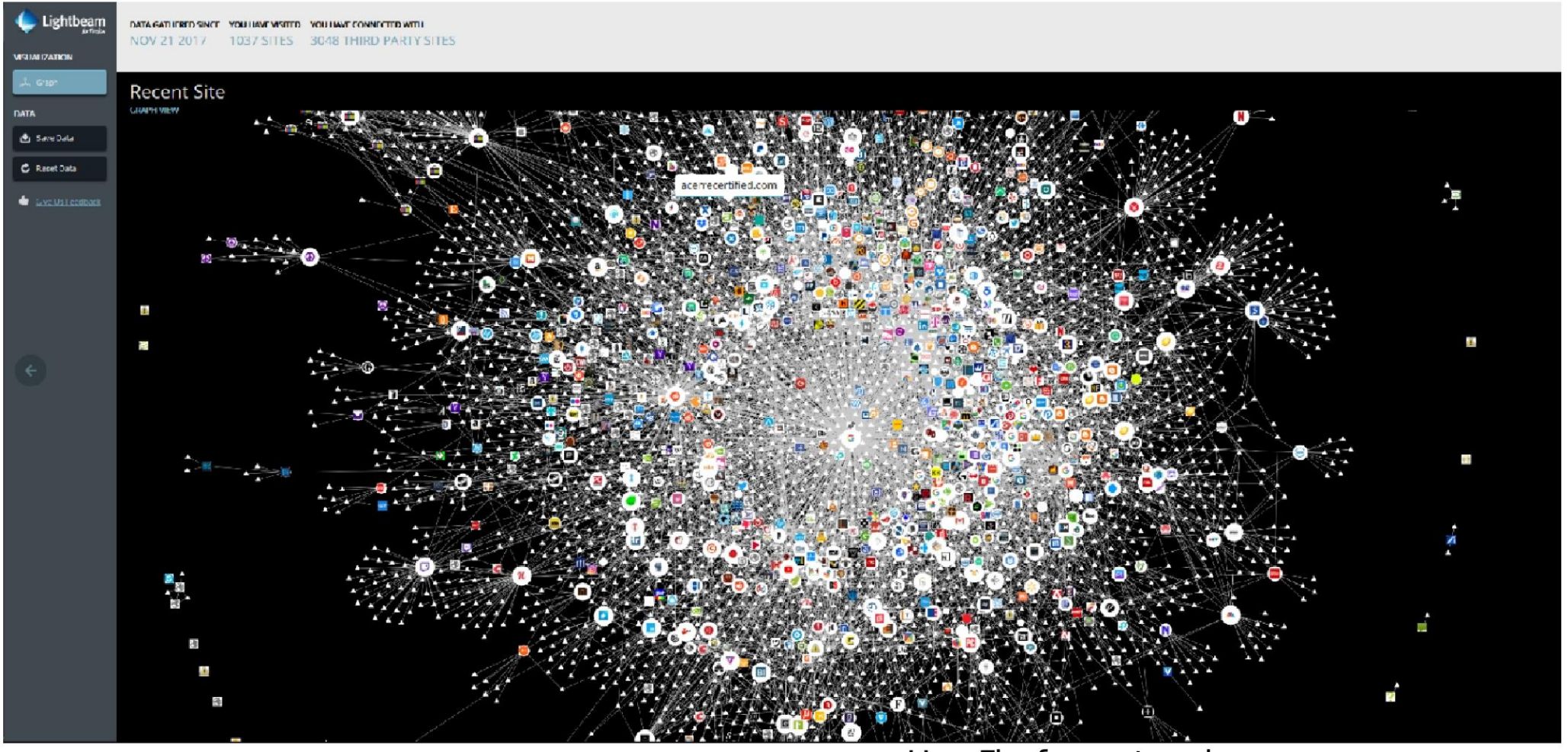
4. Cookies tracking



4. Cookies tracking

Lightbeam extension

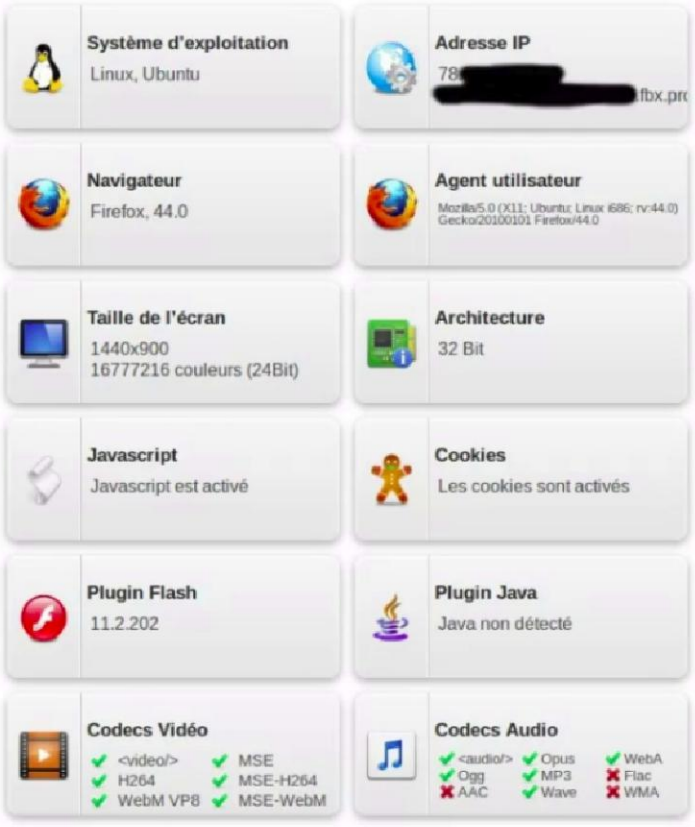




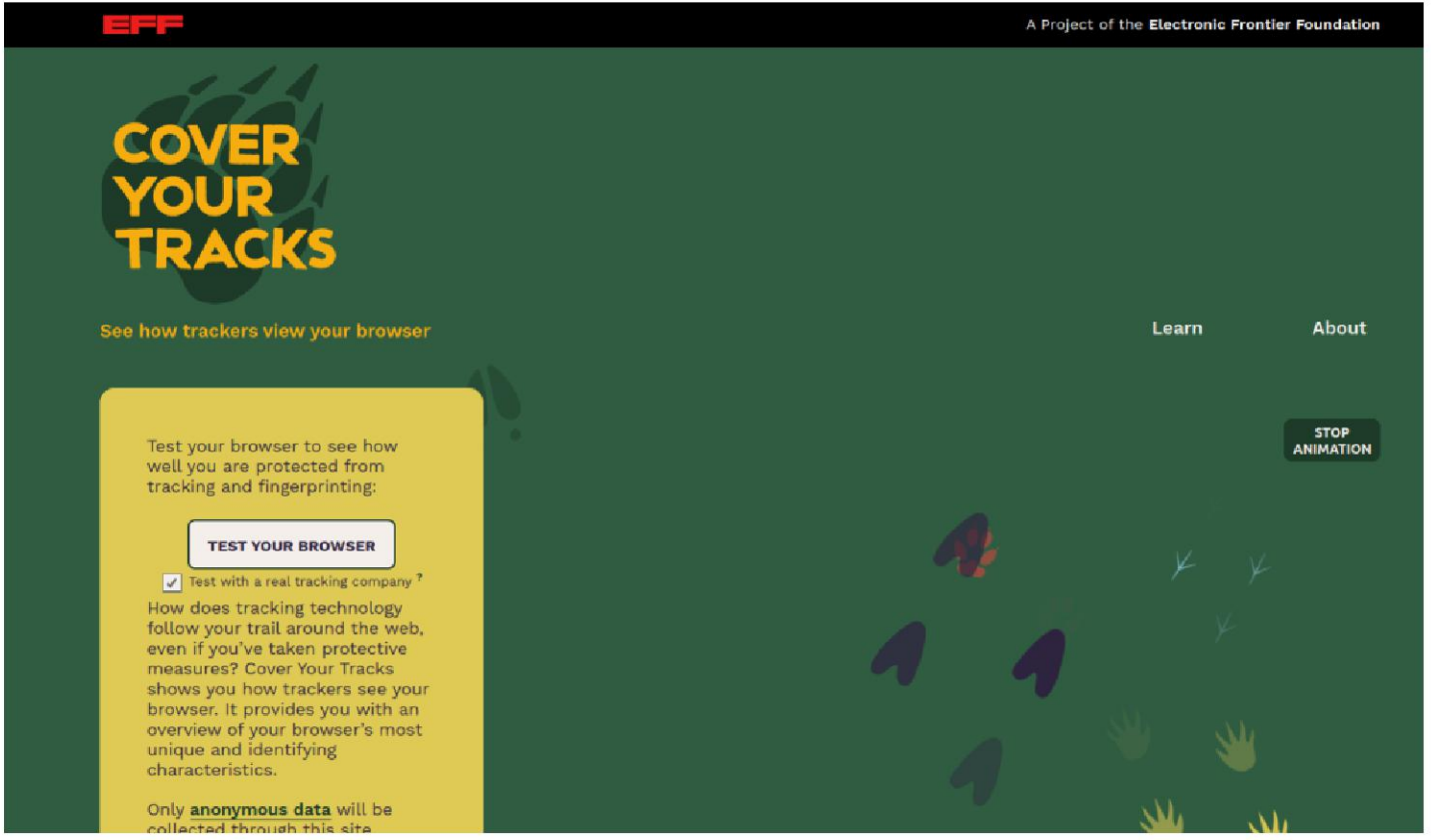
Firefox settings:
- Delete cookies when you close your browser
- Reject third-party cookies

Use Firefox extensions:
- uBlock origin
- Decentraleye
- Cookie AutoDelete

4. Fingerprinting



4. Fingerprinting



5. Conclusion and ressources

- Stable conception of ‘privacy’ over time → **continuity of regimes and tools**
- **Small community → same experts** who draft the OECD guidelines and national laws
- Data privacy regulation as a symbol of the **limit of the liberal conception** of the state and of the regulation → “consent”…
- **EU = a decade behind the Chinese surveillance model** but moving in the same direction… (facial recognition, etc.)
- **Selling personal data** as the next solution?
- Inability to understand that what was allowed to be used for commercial purposes for more than two decades **could be used for other purposes**

5. Conclusion and ressources

- Cambridge Analytica = **electroshock for politics**
- **Antitrust law** for regulating the GAFAM?
- **Boundary** between **public** and **private** is becoming increasingly thin
- Privacy as an **answer to resolve political** (representative democracy) and **capitalistic contradictions** (surveillance capitalism)... until when?
- **Mass surveillance** becoming increasingly diffuse, but **powerful tools (FOSS+encryption)** to protect against it collectively becoming more and more accessible...

5. Conclusion and ressources

À oublier	Outils libres	Ordinateur	Smartphone
Windows, iOS, Android	Système d'exploitation	GNU/Linux	Lineage, Divest, Graphene, UbuntuTouch...
Google Play, AppStore	Applications	Logithèque	F-Droid ou AuroraStore
Edge, Opera, Chrome	Navigateur internet	Firefox ou Tor	Mull ou Tor
Outlook	Client mail	Thunderbird	K9-Mail ou FairEmail
Google Maps	Carte, trajets	OpenStreetMap	OSMand, Organic Maps, Transportr
OneDrive, Dropbox	Sauvegarde, partage	NextCloud	

5. Conclusion and ressources

Chiffrement	Ordinateur	Smartphone
Disque	LUKS (à l'install) ou VeraCrypt (après)	Souvent automatique
Dossiers	Cryptomator ou VeraCrypt	Turtl
Mail	PGP avec Thunderbird ou Mailvelope	PGP avec OpenKeychain + K9-Mail ou FairEmail
Messagerie	Silence (SMS), Signal, Tox, Element, XMPP	
VPN	Neutrinet (local, prix libre, une seule IP), Riseup (prix libre), Proton (Freemium), Mullvad (5€/mois)	
Notes	Standard Notes	
Mots de passe	KeePass	

5. Conclusion and ressources

	Privacy Tools	
degooglisons-internet.org	privacytools.io	prism-break.org

6. Q&A, discussion

Thank you for your attention!