# Sur la piste du pistage

La revue de presse de Jonas@framasoft, qui paraît quand il a le temps. Épisode N° 3/n

## Facebook juge de ce qui est fiable ou non

Le nouvel algorithme de Facebook, qui permet de mettre en avant (ou reléguer aux oubliettes) les informations sur votre mur, cherche à faire du *fact-checking*. C'est logique : plutôt que de donner la maîtrise à l'utilisateur de ses fils de données, pourquoi ne pas rafistoler les bulles de filtre que le réseau social a lui-même créées ?

Un article à lire chez Numérama.

## Le pistage par ultrasons contribue à nous profiler et permet de repérer les utilisateurs de Tor


> *Les annonceurs et les spécialistes du marketing ont la possibilité d'identifier et de pister des individus en insérant des fréquences audio inaudibles dans une publicité*

*diffusée à la télévision, sur une radio ou en ligne. Ces ultrasons pouvant être captés à proximité par les micros des ordinateurs ou des smartphones, vont alors interpréter les instructions (…) Les annonceurs s'en servent pour lier différents dispositifs au même individu et ainsi créer de meilleurs profils marketing afin de mieux diffuser des publicités ciblées dans le futur.*

*L'année dernière, des chercheurs ont expliqué que des attaquants pourraient pirater ces ultrasons pour pirater un dispositif (ordinateur ou smartphone). Cette fois-ci, ce sont 6 chercheurs qui ont expliqué que cette technique peut également servir à désanonymiser les utilisateurs de Tor.*

Un article à lire chez Developpez.com

## Les parents allemands ne veulent pas de la poupée qui espionne leurs enfants

D'après cet article signalé par l'indispensable compte Twitter de Internet of Shit

*Les chercheurs expliquent que les pirates peuvent utiliser un dispositif Bluetooth inclus dans la poupée My Friend Cayla pour écouter les enfants et leur parler pendant qu'ils jouent.*

*La commissaire européenne à la Justice, à la Consommation et à l'Égalité des sexes, Vera Jourova, a déclaré à la BBC : » je suis inquiète de l'impact des poupées connectées sur la vie privée et la sécurité des enfants ».*

*Selon les termes de la loi allemande, il est illégal de vendre ou détenir un appareil de surveillance non-autorisé. Enfreindre la loi peut coûter jusqu'à 2 ans de prison.*

*L'Allemagne a des lois très strictes pour s'apposer à la surveillance. Sans doute parce qu'au siècle dernier le*

> *peuple allemand a subi une surveillance abusive, sous le nazisme puis sous le régime communiste de l'Allemagne de l'est.*

Euh, et en France, tout va bien ?

image par Cathie Passion (CC BY-SA 2.0)

---

# Surveillons la surve://ance

La revue de presse de Jonas@framasoft, qui paraît quand il a le temps. Épisode N° 2/n

## Effacer n’est pas supprimer : votre historique de Safari demeure longtemps dans iCloud

(Source : Forbes)

> *Si vous pensez que la suppression de votre historique de navigation sur votre iPhone ou Mac va faire disparaître définitivement vos habitudes en ligne, vous vous trompez. Lourdement. Selon le PDG d’Elcomsoft qui commercialise un outil d’extraction des données du iPhone, Apple stocke l’historique de navigation de Safari dans le iCloud, en remontant à plus d’un an, peut-être bien davantage, même lorsque l’utilisateur a demandé qu’il soit effacé de la mémoire.*


> *Jay Stanley, spécialiste de l’analyse des politiques de confidentialité à l’ACLU (Union américaine pour les libertés civiles), dit que les entreprises doivent être vigilantes et suivre les bonnes pratiques en détruisant vraiment les données des utilisateurs qui le demandent.*

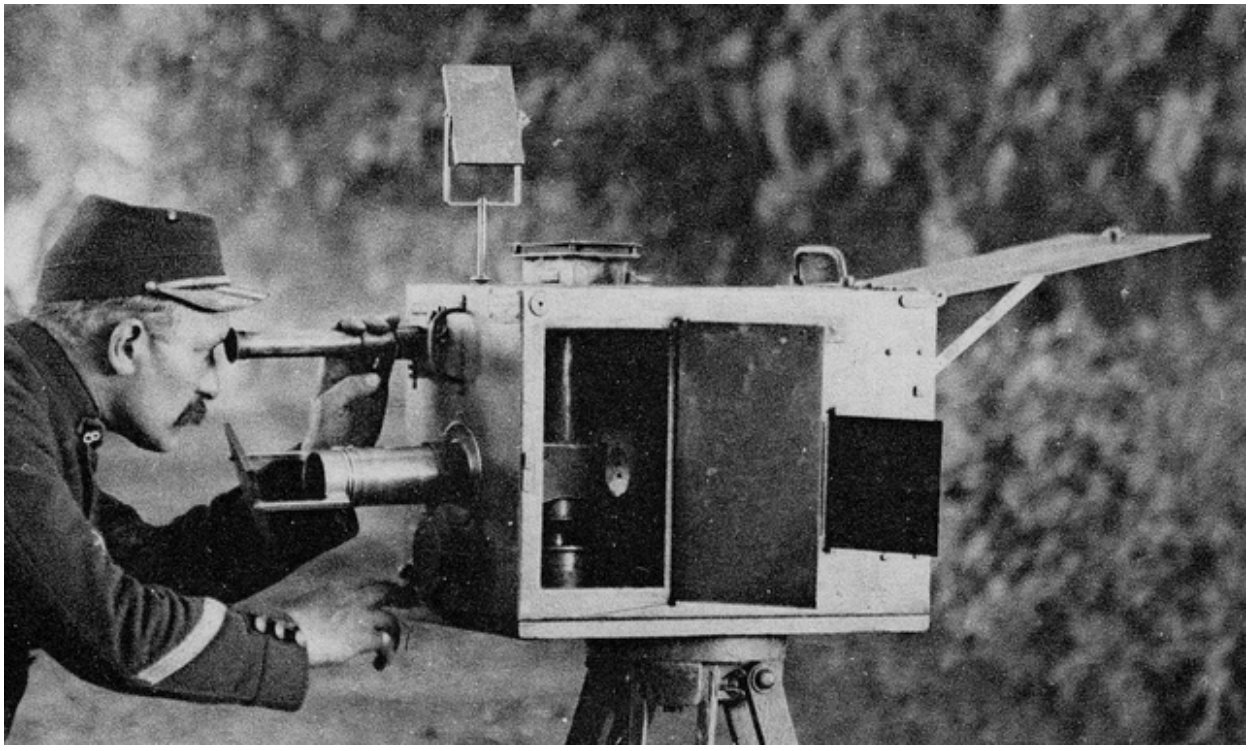
> *Il rappelle : « l’historique de navigation est un ensemble de données extrêmement sensibles. Elles révèlent les centres d’intérêt des personnes, ce qui les préoccupe, un grand nombre des pensées qui les traversent, ainsi que des informations sur leur santé et leur sexualité ».*

L'article se termine par une mise à jour rassurante : Apple semble avoir corrigé le problème dans la dernière version de son OS. Cependant il est conseillé aux utilisateurs soucieux de leurs données sensibles de désactiver la synchronisation de Safari avec  iCloud.

## Vos comptes Gmail espionnés légalement

(source : Papergeek)

> *La justice vient de statuer sur les données stockées sur les serveurs de Google, dont celles du très populaire service de messagerie Gmail. Elle a donc décidé de forcer la firme à divulguer les données de n'importe lequel de ses utilisateurs quelle que soit la nationalité, que vous résidiez ou non aux États-Unis. Même si les données en question se trouvent sur des serveurs en dehors du territoire des États-Unis.*



« Nersac, un poste optique ». Détail d'une carte postale française de 1910. Domaine public, image procurée par Signal mirror.

## Cyber-harcèlement d'état ?

(source : The New York Times)

Au Mexique, les partisans d'une taxe sur les sodas, comme des nutritionnistes ou responsables de la santé publique, sont victimes de messages électroniques inquiétants ou menaçants. La taxe est destinée à réduire la consommation de boissons sucrées et donc l'obésité, mais elle se heurte évidemment aux pressions des géants voisins des boissons gazeuses, pressions relayées semble-t-il par le gouvernement mexicain lui-même.

> *Les liens envoyés étaient accompagnés d'une forme invasive de logiciels espions développée par NSO Group, un cyber-distributeur israélien qui vend ses outils d'espionnage exclusivement aux gouvernements et qui a des contrats avec plusieurs agences à l'intérieur du Mexique, comme le révèlent des fuites publiées l'an dernier par le New York Times.*
>
> *NSO Group et les dizaines d'autres « espiogiciels » commerciaux qui sont apparus autour du globe au cours de la dernière décennie opèrent dans un marché largement non réglementé. Les fabricants de ces logiciels espions comme NSO Group, Hacking Team en Italie et Gamma Group en Grande-Bretagne assurent qu'ils vendent des outils uniquement aux gouvernements pour les enquêtes criminelles et terroristes.*
>
> *Mais les services gouvernementaux ont toute latitude pour décider qui ils veulent on non pirater avec des outils d'espionnage qui peuvent tout pister de leur cible : tous les appels téléphoniques, les textos, les courriels, les frappes au clavier, la localisation, chaque son et chaque image.*

Jonas rejeté par la baleine. Enluminure de la Bible de Jean XXII.

École française du XIVe siècle — Domaine public (via Wikimédia Commons)

---

# Chroniques du Léviathan

La revue de presse de Jonas@framasoft, qui paraît quand il a le temps

MOTHERBOARD

## « Un cerveau de substitution »

Dans une interview sur les chances qu'a Qwant de rivaliser avec le moteur de recherche de Google, Éric Léandri, co-fondateur de Qwant, déclare :

> *Vous devez penser à l'Internet non seulement comme un moyen de communication, mais de plus en plus comme à un cerveau de substitution. Les choses qui auraient été gardées dans les limites impénétrables de votre propre esprit, ou dans le sanctuaire de votre maison, sont maintenant envoyées sur des serveurs pour que le monde ou quelques entreprises les voient. Tout ce que nous faisons est de plus en plus stocké et peut être récupéré sur demande.*

The Atlantic

## « Votre historique de navigation suffit à dévoiler votre identité »

D'après un article de The Atlantic, une équipe de chercheurs de Stanford et Princeton a développé un système qui peut connecter votre profil Twitter avec votre nom et votre identité, en examinant seulement votre historique de recherche.

> *Cela signifie que conserver la confidentialité tout en utilisant Twitter est impossible sans renoncer à ce qui constitue le marqueur du réseau social : sa nature publique et gratuite pour tous.*

L'article explique comment l'expérience a été menée et mentionne au passage quelles parades on peut éventuellement utiliser : Privacy Badger et Ghostery
Mais voici la fin de l'article :

> *Le conseil de sagesse qu'on nous donne généralement est qu'il faut être prudent avec ce que l'on partage. Mais ici, nous montrons que vous pouvez être dés-anonymisé simplement en naviguant et en suivant des comptes, même si vous ne partagez rien.*

la Repubblica

## « Une fois vos informations stockées, on peut les modifier et en faire ce qu'on veut »

Dans l'hebdomadaire italien La Repubblica, la journaliste Stefania Maurizi interviewe le lanceur d'alerte William Binney. Celui-ci évoque entre autres un programme pour la NSA nommé ThinThread, qu'il avait développé avec son équipe et qui permettait de cibler avec précision la surveillance en visant les activités délictueuses, tout en laissant de côté les données privées.

Quelques extraits de la conversation :

> *Stefania Maurizi – Après le 11 septembre, la NSA a détourné votre système, supprimé les dispositifs protégeant la vie privée et a utilisé ThinThread pour espionner la population tout entière ?*
> *William Binney – La première chose qu'ils ont faite a été le programme « Stellar Wind » qui visait l'espionnage domestique (…) ils ont supprimé trois fonctionnalités de ThinThread dont l'une était la protection de la vie privée. Au lieu de prendre seulement les données pertinentes ou celles qui étaient très probablement pertinentes, ils ont absolument tout pris et ils ont étendu la surveillance à l'échelle de la planète.*
> *SM – Nous avons constaté dans les seize dernière années que la surveillance de la NSA avait échoué à prévenir des attaques terroristes. Pensez-vous que ce n'est qu'une*

*question de temps avant que la NSA ne soit capable de le faire effectivement, ou bien qu'ils n'en auront jamais les capacités ?*
*WB – Je pense qu'ils sont condamnés à l'échec, parce qu'ils sont enfermés dans la conviction qu'ils doivent tout collecter (…) Ils sont très bons pour collecter des données, mais ils n'ont fait aucun progrès pour essayer de savoir ce qu'ils peuvent avoir dans les données qu'ils ont collectées.[…]*
*Ce genre de pouvoir ne devrait pas exister pour aucun gouvernement, parce qu'il crée vraiment un état totalitaire. C'est comme la Stasi dopée aux amphétamines ; au lieu de détenir des dossiers avec des documents sur tout le monde, ils archivent tout ce que vous faites de façon électronique, si bien que le jeu d'informations est beaucoup plus complet, à jour et exploitable, et ils peuvent le manipuler, et faire de vous tout ce qu'ils veulent […]*
*SM – Donc le problème n'est pas seulement la collecte, mais aussi la manipulation des données ?*
*WB – Oui. une fois qu'on a stocké les informations, on peut les modifier et en faire ce que l'on veut.*

Léviathan dans la fresque « Le Jugement dernier » de Giacomo Rossignolo – CC-BY-

SA