DONNER OU PAS DONNÉES ?

Dr J. NICOGOSSIAN

Anthropobiologie/ *Business Anthropology*

« CYBERSECURITE ET PROTECTION PATRIMOINE DES ENTREPRISES »

Séminaire Aristote, 1er Oct. 2018

BANKSY, *STREET ART*, BRISTOL (UK)

Amoureux à l'ère phygitale

SHOWROOM CEA TECH GRENOBLE

I. CRYPTOGRAPHIE

Sécurité & « culture entreprise »

LE CHIFFREMENT

- La cryptographie ouvre plusieurs fonctions :
- Maintien de la confidentialité (le chiffrement classique)
- Non-répudiation (la signature ne peut être remise en cause)
  - Echange HTTPS : navigateur récupère la signature du certificat et ton navigateur récupère et la vérifie(chiffrement asymétrique). En terme mathématique : il n'y a que toi qui puisse avoir signé le doc. Exemple: Impôt, premières versions de la déclaration en ligne : certificat personnel, clé privée …
- Echanges formels protégés par un protocole bien sécurisé.

LE CHIFFREMENT

- Les problèmes sont surtout dans l'utilisation qui en est faite.
- Enjeu: Former les professionnels à la bonne utilisation de ces outils
    - Une « culture de l'entreprise »
    - L' « anthroprise » une culture évolutive?

➢ Le chiffrement & l'anonymat sont indispensables à la liberté de l'information & à la promotion des droits de l'homme, pour une « liberté numérique » totale (rapport du Conseil des droits de l'homme des Nations unies). Exemple: formation RSF.

- https://rsf.org/fr/actualites/le-chiffrement-et-lanonymat-indispensables-la-liberte-de-linformation

II. QUELLES ATTAQUES ?

QUELLES ATTAQUES?

Deux types :

1. celle de l'algorithme de chiffrement lui-même (la difficulté mathématique)
2. celles des solutions (problèmes d'implémentation à plusieurs niveaux).
    a) *La faute des entreprises*
        - Ex, pour la NHS, versions de Windows obsolètes, plus au standard, pour lesquelles il n'y a a plus de sécurité.
    a) *business des failles 0D*
        - Les labos de recherche communiquent aux éditeurs (Microsoft, qui prend le temps d'implémenter la correction).
        - Francs-tireurs qui ne le communiquent pas sauf en les vendant : systèmes d'enchères, abonnements, etc.

III. L’ ANONYMAT

Et la possibilité de réidentification…

L'ANONYMAT

Chiffrement & anonymat sont indispensables à la « liberté numérique », **MAIS**

1. Le chiffrement ça marche – globalement (sauf prob d'implémentations) – mais il faut savoir l'utiliser…
2. Peut-on formaliser tous les échanges en protocole?
3. L'analyse d'un nombre massif de données à grande échelle rend l'anonymat superficiel & l'anonymisation pratiquement impossible.
4. Quand on met une donnée, on ne peut plus la retirer.

IV. LES FUITES

& le « Facteur humain »

LES FUITES

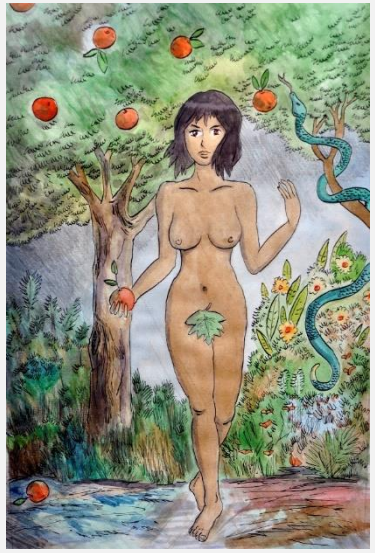
Le réflexe est de se prémunir des attaques extérieures

MAIS

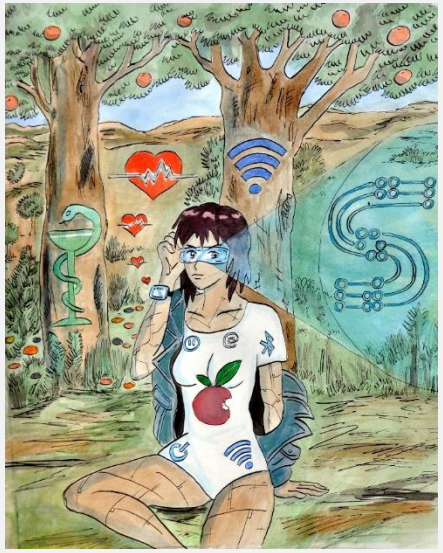
il y a aussi les risques de l'intérieur.

- Spécialiste des vieux hackeurs des réseaux sociaux faire le ménage des réseaux sociaux, faire les poubelles, les post-it, les photocopieurs enregistrent ce qu'ils scannent, la « poubelle numérique »
- L'historique Word …

DU NU…



À L’IOT.



LE « FACTEUR HUMAIN »

- Reconnaissance
- *Affairs*/ Curiosité (expérimentation Sophie Perso)…
- Argent
- Pouvoir
- Jalousie

➢ Un département de la défense avait interdit par directive à ses membres de sortir boire des cocktails avec des gens qui ne sont pas du même service: conditionnement total, uniforme?

LE « FACTEUR HUMAIN »

Préconisations:

- Du curatif : changer les mots de passe, se désinscrire de badoo, ou si c'est trop dur demander à la personne de ne pas utiliser son mail pro pour aller sur badoo !
- Tout le temps sur VPN (*Virtual Private Network*)
- Pas de réseaux sociaux.
- Compte Google vestigial!

LE « FACTEUR HUMAIN »

1. Ne pas laisser traîner ses données
2. Choisir ses mots de passe
3. ~~Ne pas avoir de relation à l'extérieur de son service~~

Les erreurs reconnues sont l'occasion d'améliorer le *process*, en tirer une leçon, anticiper pour ne pas que ça se reproduise!

V. LE CONSENTEMENT

Une absurdité?

LE « CONSENTEMENT »

« Avant même le piratage, le mec qui se trouve au bon endroit au bon moment, c'est surtout qu'avant tout ça, TU donnes tout! »

Z, membre d'un service de cybersécurité, Département de la Défense

LE « CONSENTEMENT »

« La donnée est devenue une infrastructure […] Peut-être que nous pouvons mieux protéger la vie privée, ou mettre en place de meilleures façon de protéger les données. L'expérience nous dit que tous les mécanismes fondés sur le consentement de l'utilisateur échouent : on a déjà 25 ans d'expérience et on accepte toujours les conditions générales d'utilisation sans les lire. »

R. Stallman, 64 ans, 2017 adoubé « Pape du logiciel libre »

LE « CONSENTEMENT »

Espèce de consensus

« Je suis prêt à tout donner pour avoir un service gratuit », **MEME SI**
« quand c'est gratuit le produit c'est toi ». (Z)

LE « CONSENTEMENT »

- Privilégier des comptes mails (sur un autre *Business Plan*) qui ne dépendent pas de la législation américaine?

« J'ai un compte mail que je paie sécurisé, gérée par des serveurs qui se retrouvent sous une montagne en Suisse. » (Z)

❖ Quel est le prix qu'on donne à sa vie privée?

VI. SRATEGIES DE DÉTOURNEMENT

DÉTOURNEMENT

- Les données peuvent:
- venir d'une fuite (ex *Wikileaks*);
- être instrumentalisées, altérées modifiées avant d'être remise en circulation (ex *Clearstream*).

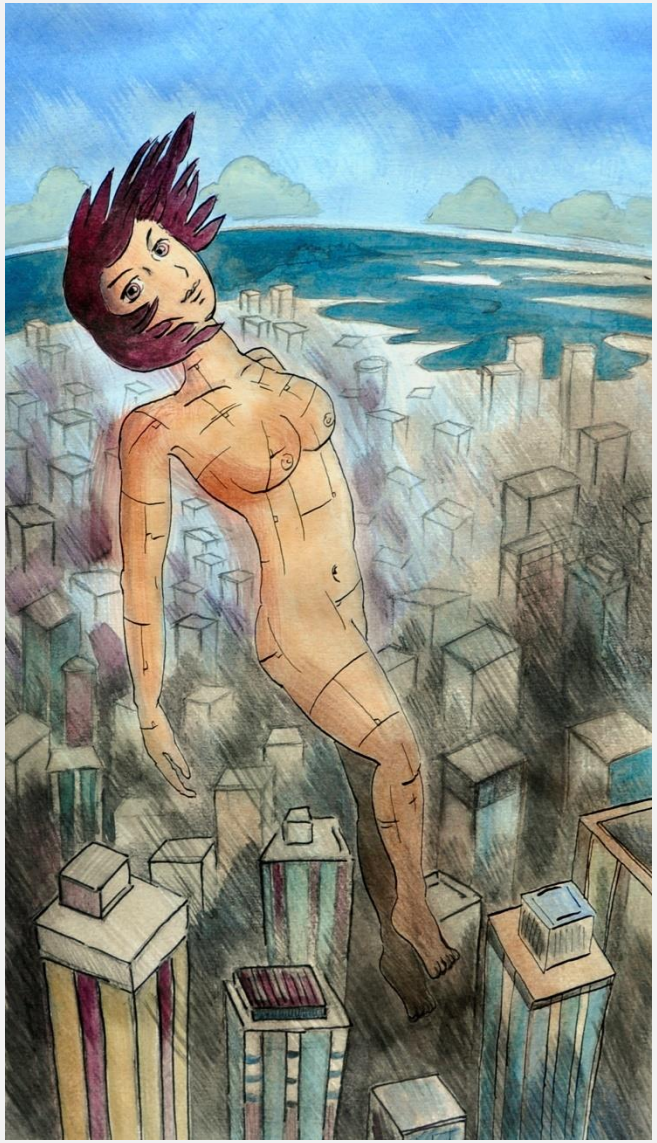
OBFUSCATION, *FÉMININ*

- = masquage, opacification, **assombrissement**, **obscurcissement, offuscation** est une stratégie de protection de la vie privée, intentionnelle ou involontaire, sur internet qui consiste à publier des informations fausses ou imprécises de manière à dissimuler les informations pertinentes.

  - *(Programmation informatique)* Technique qui consiste à rendre illisible pour un humain un programme, tout en le gardant pleinement fonctionnel.

CAMOUFLAGE THERMO-OPTIQUE

Ghost in the Shell, Oshii (1995)



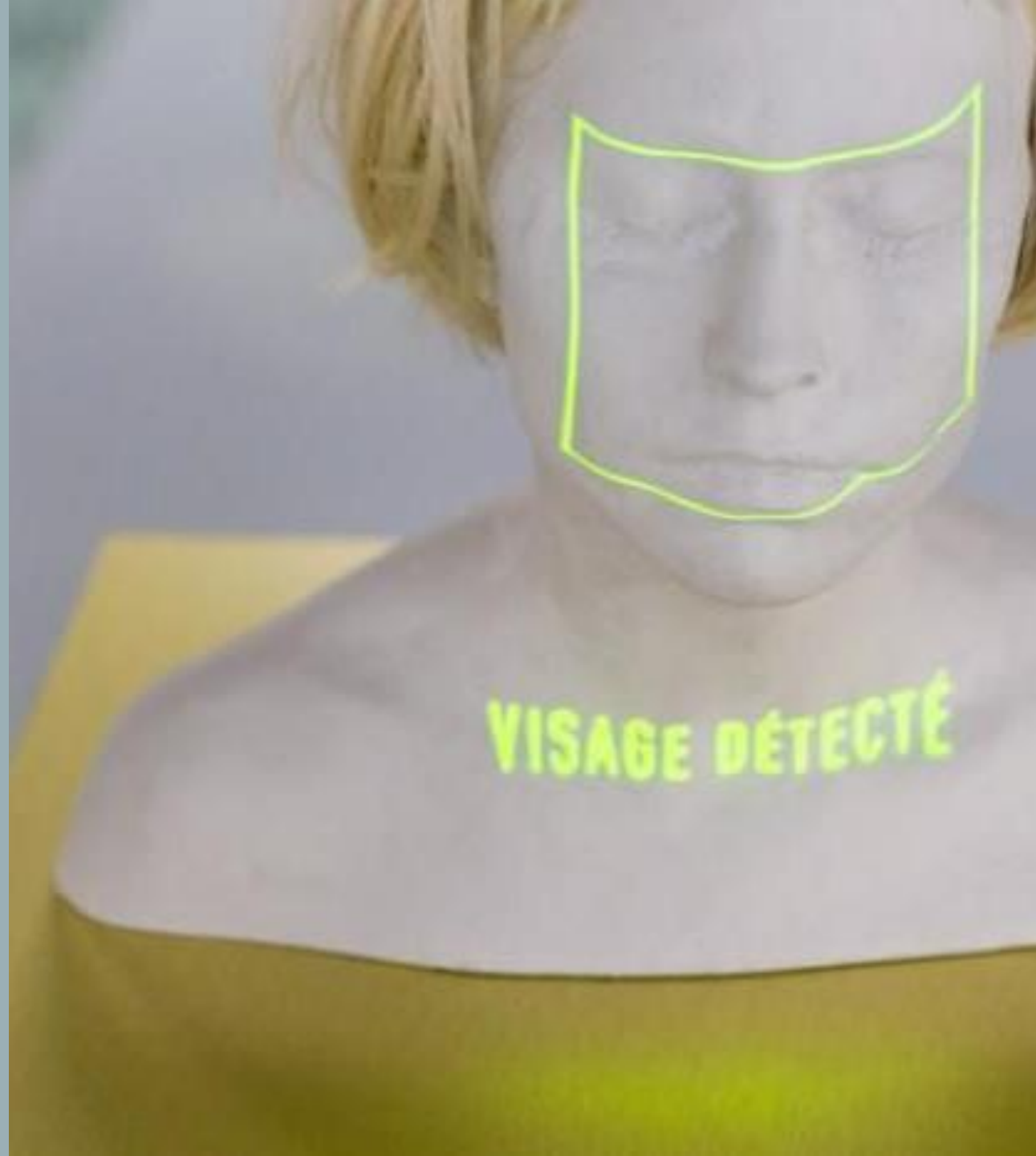
REPRENEZ LE POUVOIR, DEVENEZ INVISIBLE!

CV DAZZLE

« Stealth War »

Adam Harvey & Vinciane Verguethen

https://www.nouvelobs.com/rue89/rue89-rue89-culture/20160410.RUE2622/big-data-surveillance-reprenez-le-pouvoir-et-devenez-invisible.html



VII. AUX MAINS DU POUVOIR

PARANOÏA? Exemples de déviances…

BANKSY, *STREET ART*, BRISTOL (UK)

Début 2018 il y a plus de smartphones actifs dans le monde (7,7 milliards) que d'habitants sur Terre (7,4 milliards)

[Réf: ttps://www.planetoscope.com/electronique/728-ventes-mondiales-de-smartphones.html]

CONTRÔLE

« Les téléphones portables vous fliquent en permanence. Je refuse de les utiliser. Ils ont des portes dérobées, des failles vouées à les transformer en dispositifs de surveillance. C'est la vérité nue. Pour moi, le téléphone portable, c'est le rêve de Staline devenu réalité. C'est pire encore que sur un ordinateur : les données de conversation sont conservées. Et ici, en France, il n'y a plus de protection des utilisateurs. Avant, la France avait un système admirable de protection des données, mais c'est fini : tout a été saccagé avec l'état d'urgence. On est dans même situation qu'aux Etats-Unis après le 11 septembre 2001. Après des attentats, l'attaque suivante porte systématiquement contre nos libertés individuelles, et moi j'essaie d'appeler les gens à résister. Mais je n'ai pas beaucoup réussi jusqu'à présent, je dois le concéder. »

R. Stallman, 64 ans, 2017 adoubé « Pape du logiciel libre », auréolé d'un cd-rom

- Réf https://usbeketrica.com/article/le-telephone-portable-c-est-le-reve-de-staline-devenu-realite

LA MORT DE L'AUTEUR

Pensionnaire de Harvard et du prestigieux MIT dans les années 1970, il initie dans les eighties le mouvement du logiciel libre avec sa licence GNU, puis en créant la méthode « copyleft », qui s'oppose à la notion de « copyright ».

SMARTPHONES

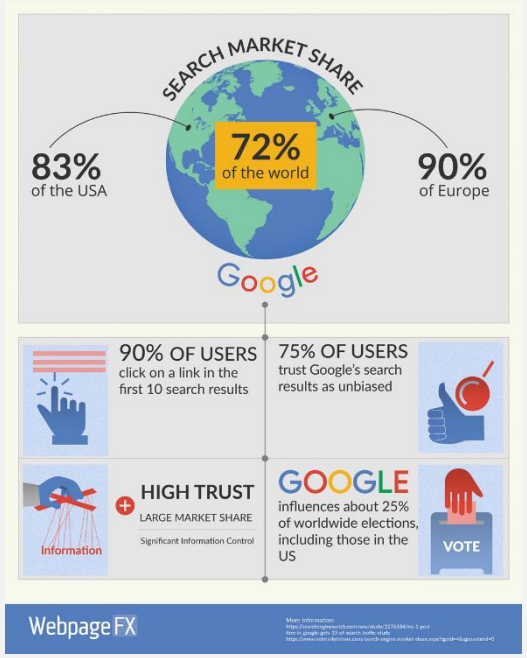
L'injustice de la surveillance commence avec ces logiciels privateurs et l'introduction, souvent volontaire, de failles dans les appareils. Ces logiciels sont conçus pour limiter l'utilisateur, ils permettent d'imposer la censure, comme le font Apple et Microsoft avec leurs applications. Parce que ces appareils sont sous le contrôle total d'une entreprise, au lieu d'être contrôlés par les utilisateurs. Le processeur de communication des téléphones est complètement secret : nous ne savons même pas dans quel langage sont écrites ses instructions, donc il est impossible de concevoir un programme libre pour ce genre de processeurs, comme nous avons pu le faire avec GNU/Linux.

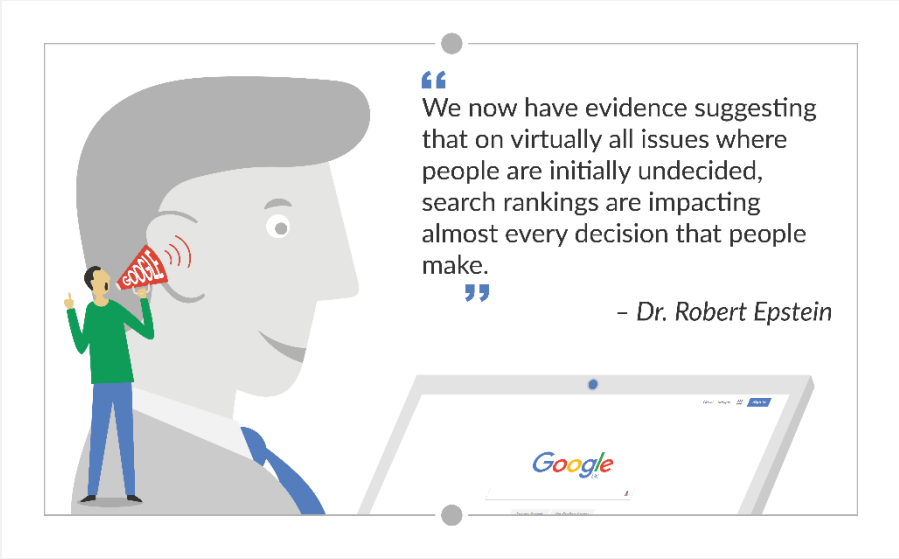
GAFAM – NATU - BATX

« Il y a 15 ans, on pouvait imaginer que la menace provenait d'Hollywood, et de la manière dont l'industrie du cinéma pouvait contrôler l'environnement culturel. Aujourd'hui, Facebook et Google accumulent tellement de données sur nous et peuvent effectuer tellement d'expériences sur les individus que le débat autour du marketing comportemental et de la la vie privée me semble immensément plus urgent [que la protection des droits auteur à l'ère du numérique] »

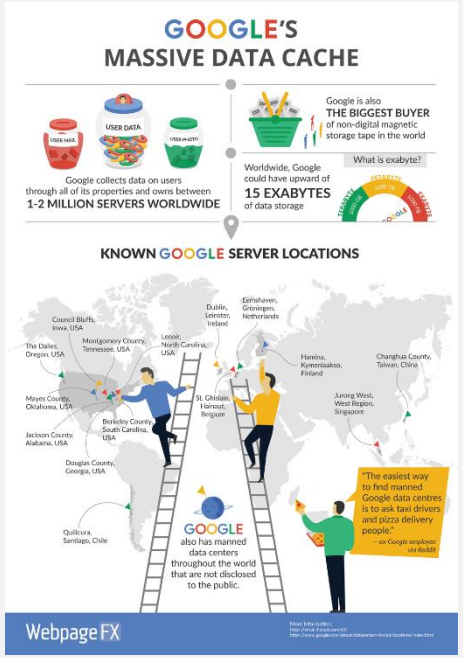
R. Stallman, 64 ans, 2017 adoubé « Pape du logiciel libre », auréolé d'un cd-rom

GAFAM


SEARCH MARKET SHARE
83%
of the USA
72%
of the world
90%
of Europe
Google
90% OF USERS
click on a link in the first 10 search results
75% OF USERS
trust Google's search results as unbiased
HIGH TRUST
LARGE MARKET SHARE
Significant Information Control
GOOGLE
influences about 25% of worldwide elections, including those in the US
Information
VOTE
Webpage FX


We now have evidence suggesting that on virtually all issues where people are initially undecided, search rankings are impacting almost every decision that people make.
– Dr. Robert Epstein
Google

GAFAM


GOOGLE'S
MASSIVE DATA CACHE
USER MAIL
USER DATA
USER H-DTO
Google collects data on users through all of its properties and owns between 1-2 MILLION SERVERS WORLDWIDE
Google is also THE BIGGEST BUYER of non-digital magnetic storage tape in the world
What is exabyte?
Worldwide, Google could have upward of 15 EXABYTES of data storage
KNOWN GOOGLE SERVER LOCATIONS
Council Bluffs, Iowa, USA
Montgomery County, Tennessee, USA
The Dalles, Oregon, USA
Lenoir, North Carolina, USA
Mayes County, Oklahoma, USA
Berkeley County, South Carolina, USA
Jackson County, Alabama, USA
Douglas County, Georgia, USA
Quilicura, Santiago, Chile
Dublin, Leinster, Ireland
Eemshaven, Groningen, Netherlands
St. Ghislain, Hainaut, Belgium
Hamina, Kymenlaakso, Finland
Changhua County, Taiwan, China
Jurong West, West Region, Singapore
GOOGLE also has manned data centers throughout the world that are not disclosed to the public.
"The easiest way to find manned Google data centres is to ask taxi drivers and pizza delivery people."
— ex Google employee via Reddit
Webpage FX


THE PROBLEMS WITH
GOOGLE'S POSITION
Anticompetitive changes to the search algorithm can be framed as "attempted improvements"
Google itself does not have opinions or an agenda — but the individuals who run it do
Google
Google regularly collects data on its users
GOOGLE'S POSITION as a search giant has 7 MAJOR PROBLEMS FOR CONSUMERS
Currently, there are no laws about search results
There's no paper trail if Google gets rid of evidence
Google has full control over any incriminating evidence against them
Google regularly cooperates with government agencies and shares user data
Webpage FX
More Information:
https://aeon.co/essays/how-the-internet-flips-elections-and-alters-our-thoughts

EXEMPLES DE CONTRÔLE

MARKETING COMPORTEMENTAL

- *Cambridge Analytica*

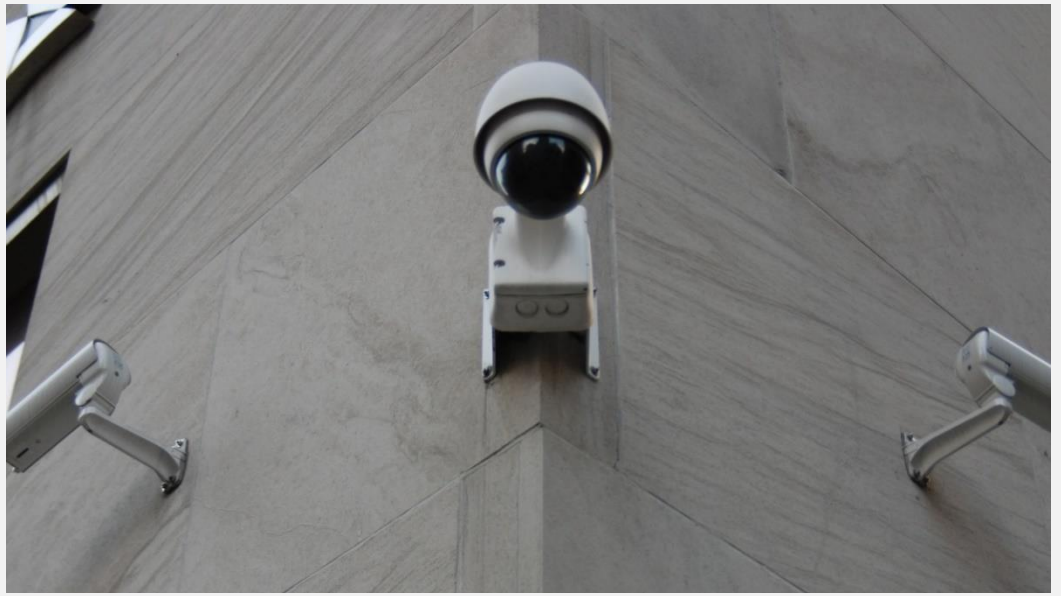
VIE PRIVÉE

- *Déviances assureurs*
- *Points de citoyenneté du système chinois*

MARKETING COMPORTEMENTAL

- *Cambridge Analytica* (2016: collecte et exploite à leur insu les données personnelles de 87 millions d'utilisateurs FB pour établir des profils « psychographiques » à des fins de ciblage pro-Trump et pro-Brexit)
  - Faillite MAIS reprise par la société Ermadata.

VIE PRIVÉE?



VOIR DERRIÈRE LES MURS…

- Camera 1 pixel ou caméra à pixel unique peut voir derrière un mur… à Xi'an Jiaotong University (China). Peut photographier des objets quand ils ne sont pas en vue directe.
  - ✓ Source: MIT Technology review
  - ❖ https://www.technologyreview.com/s/603314/new-camera-can-see-around-corners/

L'« ŒIL CÉLESTE », GUIYANG

Expérience : un journaliste britannique retrouvé en 7 mn dans la ville de Guiyang.

Nombreux filtres de l'information, dont le Grand Firewall, muraille numérique qui encercle l'Internet chinois depuis 1998, et se resserre depuis un an. »

VIE PRIVÉE?

« *On ne sait pas si les interviewés soutiennent réellement le gouvernement ou donnent des réponses prudentes aux étrangers. On ne sait pas pourquoi les Chinois disent aux sondeurs qu'ils ont plus confiance en leurs concitoyens que dans n'importe quel pays du monde. En réalité, la* paranoïa est si endémique *que les personnes âgées ne sont pas aidées dans les rues par peur d'une arnaque, et qu'on laisse mourir les enfants comme la petite Wang Yue, qui avait été renversée par une voiture* (accident filmé de 2011 au scandale planétaire). »

- Vrais chiffres du PIB? Nombre exact d'habitants? Convictions profondes de la population?
  - « Personne ne sait rien sur la Chine » James Palmer, correspondant Asie de *Foreign Policy* (21/03/2018)

VIE PRIVÉE?

- « Citoyenneté numérique », mesure officielle depuis mai 2018 (Alibaba : crédit sésame).
  - 2017: 6,15 millions de chinois se sont vus refusés un vol pour mauvais comportement social placé sur liste noire avec interdiction de voyager (perturbé des vols, déclenché une fausse alerte pour terrorisme, avoir présenté des titres de transport périmés, fumé dans les trains …

« Il est très difficile de savoir aujourd'hui ce qui relève du plan et ce qui relève de son application, À défaut d'une notation qui prenne réellement la forme d'un algorithme, des listes noires existent d'ores et déjà, dans différents domaines, économique, par exemple : avoir fait de la publicité mensongère ou ne pas avoir remboursé ses dettes peut vous faire perdre le droit de monter une entreprise. »

Séverine Arsène, politologue, sinologue* et spécialiste de l'Internet chinois, Hong Kong .

- https://usbeketrica.com/article/videosurveillance-big-data-notation-citoyenne-la-chine-black-mirror
- https://www.reuters.com/article/us-china-credit/china-to-bar-people-with-bad-social-credit-from-planes-trains-idUSKCN1GS10S

RECONNAISSANCE FACIALE & PAPIER TOILETTE, BEIJING

46 000 caméras (couvrant la ville à 100 %), 4600 officiers de police pour regarder.

Enlever les gants et les lunettes: 3 secondes devant une caméra haute définition, de reconnaissance faciale parfois 1 mn.

9 minutes avant de réutiliser la machine et rejet de ceux qui viennent trop souvent.

VIE PRIVÉE?

Définition numérique de la personne:

1. Perte de liberté. Perte de vie privée.
2. Contrôle autoritaire: risques de déviances politiques, économiques, sociales; eugénisme.
3. Comportement normé. « Culture de la sincérité ». Autocensure, autocontrôle… Censure des émotions. Bienséance, censure des opinions tranchées .

« A partir du moment où c'est historicisé, ça peut être ressorti. » (Z)

VIII. RESTER LIBRE ?

RESTER LIBRE?

« Les programmes libres n'ont pas que des raisons pratiques mais sont une véritable conscience. Si les utilisateurs ont le contrôle des programmes, alors ces programmes respectent les droits de l'humain. Liberté, égalité, fraternité : ce sont les bases du logiciel libre. Liberté, parce qu'un logiciel ne soumet pas au pouvoir de quelqu'un d'autre : l'utilisateur est libre. Égalité, parce qu'avec le logiciel libre, tout le monde jouit des mêmes libertés et personne n'a de pouvoir sur personne. Et enfin, fraternité, car nous encourageons la coopération entre les utilisateurs. Il n'y a rien de plus important que ces droits-là, les droits de l'humain. »

- Pr. Yokai Benkler, Harvard, Etudes juridiques entrepreneuriales, chargé de travailler à la rédaction d'une future « déclaration sur l'information et la démocratie », commission lancée le 11/09/2018 par l'ONG Reportes sans frontières

PR. YOKAI BENKLER, HARVARD

- Thématiques de prédilection : les communs, le rôle du domaine public informationnel et de la collaboration décentralisée dans l'innovation et la place de la liberté dans une économie et une société en réseau.

- « Le **consentement et l'anonymat sont impossibles**. Donc les deux piliers sur lesquels reposait la protection de la vie privée ne sont plus praticables. La priorité doit à présent être donnée à **contenir la manipulation de nos comportements.** On verra si le règlement général sur la protection des données porte ses fruits. »

PR. YOKAI BENKLER, HARVARD

« Nous devons mettre place un nouveau cadre règlementaire qui utiliserait le pouvoir de l'Etat pour contrôler les entreprises. L'idée serait de les contraindre à créer et mettre en œuvre un ensemble de règles visant à un usage raisonnable de nos données personnelles, et en nous laissant l'accès à nos données. Et cela, nous y parviendrons uniquement si les entreprises y sont contraintes. »

JOUER AU ÉCHEC CUBIQUE…

« La question est donc de savoir comment on combine les aspects positifs de l'Etat (imposer des régulations aux entreprises), la compétition saine entre entreprises sur les marchés et la force de légitimation de la production entre pairs pour se rapprocher du meilleur des mondes possibles. Ce n'est pas un processus facile. »

https://usbeketrica.com/article/a-l-ere-post-snowden-on-ne-peut-plus-se-voiler-la-face

CRYPTOGRAPHIE QUANTIQUE

C.Villani & Baudoin
Ballade pour un bébé robot (2018)

« Grosse rupture technologique - dans 10-20 ans ?

C'est un outil qui permettra de casser les clés & les documents chiffrés. Les mythes militaires ultra-sécurisés et forts seront pétables dans 20 ans, si cette rupture a lieu. » (Z)

CONCLUSION: QUI SUIS-JE?

Identification & authentification

« Les doubles fantomatiques »

CRISE D'IDENTITÉ NUMÉRIQUE

Trompé par nos sens, le droit de propriété est difficile à transcrire en numérique. Au cœur de cette surveillance, ciblage et contrôle, on a presque l'impression d'avoir encore ses données. On ne sait pas ce qu'on nous a pris, il nous les reste! si il faut les donner ce qu'on doit donner, si on va nous les rendre… On ne comprend pas qu'on doive les racheter!

1. Donner sur « consentement »
2. Anonymat & ré-identification
3. Prix de protection de la « vie privée »
4. Se faire cracker ses données/ les racheter
5. Déformer ses données

IDENTIFICATION & AUTHENTIFICATION

Sécurité informatique: identification (dire qui on est) & authentification, (le prouver).

Pour le prouver il y a 4 moyens fondamentaux, le reste est une combinaison « dynamique » de ces quatre moyens:

- **tu possèdes (une clé, un badge, un passeport)**
- **tu connais (un secret, un mot de passe, une clé de chiffrement)**
- **tu es (biométrie : empreinte, iris, démarche, signature…)**
- **tu sais faire**

IDENTIFICATION ET AUTHENTIFICATION

- Comment authentifier les gens si tu ne les as jamais vu ?

… Arrive un moment, retour au réel nécessaire !

MERCI!

FIN

(~~HAPPY~~ END

…pour les ~~amoureux~~ ~~pros~~

~~Singes~~ Homo Sapiens

~~américains chinois~~ français ?)