INTRODUCTION À LA SÉCURITÉ INFORMATIQUE
SÉANCE 2 FUITES DE DONNÉES ET PVP

Marc-Olivier Killijian
UQAM, CNRS
INF4471 A21

FIN DE L'INTRODUCTION

UN PEU DE TERMINOLOGIE -> GLOSSAIRE

- **Propriétés** de sécurité : C.+I.+A.+Traçabilité
- **Participants** : entités légitimes qui sont impliquées dans l'exécution d'un protocole (A-lice et B-ob)
- **Adversaire** : entité malveillante (pas malicieuse) qui essaye de porter atteinte à une des propriétés (E-ve)
- **Algorithme** : procédure effectuée localement par un participant
- **Protocole** : procédure effectuée conjointement par les participants, dont les rôles respectifs sont clairement identifiés

TYPOLOGIE DES ATTAQUES

- **Espionnage** : capture d'infos
- **Modification** : altération d'information
- **Rejeu** d'un message capturé
- **Réflection** : rejeu d'un défi qui nous était destiné
- **Déni de service** : empêcher les participants de compléter le protocole
- **Typage** : remplacer un champs par une autre valeur
- **Cryptanalyse** : profiter d'une faiblesse cryptographique pour déchiffrer (sans clé)
- **Manipulation de certificat** : choix ou altération d'un certificat dédié à l'authentification
- **Interactions de protocole** : exploitation d'une même clé utilisée dans différents protocoles

VULNÉRABILITÉ, MENACE, ATTAQUE

- **Menace** : n'importe quel évènement négatif (d'origine malveillante ou non) qui *peut* arriver à un actif ; violation d'une ou plusieurs propriétés de sécurité

- **Vulnérabilité** : une faiblesse, ou une faille, qui rend une menace possible si elle est *exploitée*

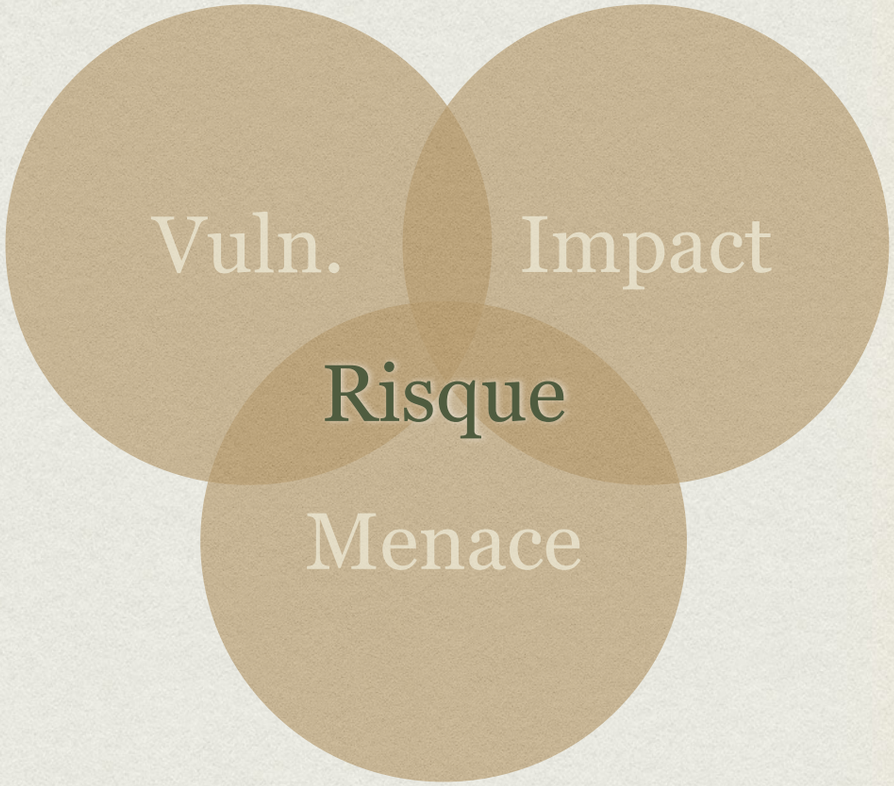
- **Attaque** : action *intentionnelle* qui exploite une *vulnérabilité* ou met en oeuvre une *menace*

- **Intrusion** : violation effective de la politique de sécurité, fait suite à une ou plusieurs *attaques* réussies

GOUVERNANCE

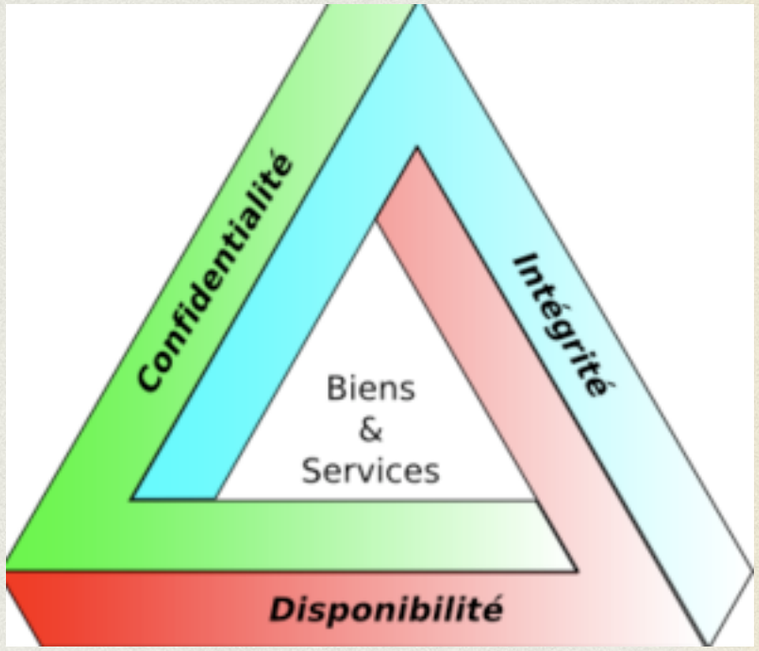
- **Gestion du risque**
  Identifier les biens
  Identifier les sources de menaces
  Evaluer la vulnérabilité face aux menaces
  Evaluer le risque (valeur/dangerosité)
  Identifier des solutions et les prioritiser
  Auditer et recommencer

- **Identifier des solutions ?**
  Politiques de sécurité
  Organisation (responsables, protocoles, etc.)
  Plans de recouvrement
  Gestion des incidents
  Aspects humains (formation)



PROPRIÉTÉS DE SÉCURITÉ

- **Confidentialité**: ne pas être accessible aux personnes non-autorisées
- **Intégrité**: ne pas être modifiable par des personnes non-autorisées
- **Disponibilité**: être accessible aux personnes autorisées
- C.I.A. (Dispo=Availability)



PROPRIÉTÉS DE SÉCURITÉ

- **Confiden** ccessible aux personne s

Craquer un mot de passe

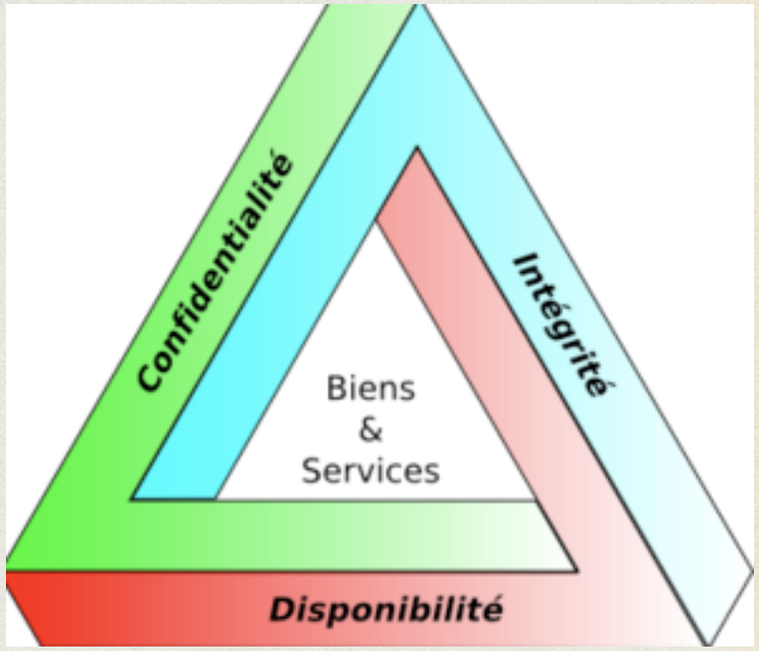
- **Intégrité**: n ifiable par des person

« Défacer » un site web

- **Disponibil** le aux personnes

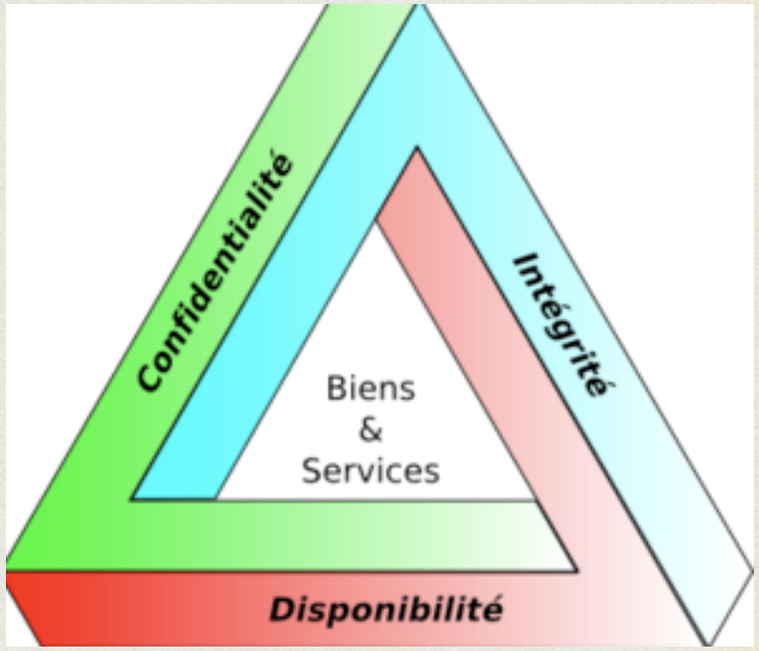
Déni de service

- C.I.A. (Dispo=Availability)



MÉCANISMES DE SÉCURITÉ

- **Authentification**: vérifier une identité
- **Autorisation**: appliquer une politique d'accès à des ressources
- **Traçabilité**: mise en place de logs permettant de savoir ce qui a été consommé ou fait
- **Auditabilité**: généralement post-mortem (analyse forensique), bénéficie grandement de la traçabilité
- A.A.A.(A) : Authentication, Autorisation, Accounting (and Auditing)



MENACES

- **Objectifs classiques**
  - Ecoute (simple ou élaborée)
  - Contournement de moyens d'authentification/ autorisation
  - Déni de service (attaque physique, réseau, vers)
- **Types d'attaquants**
  - **Internes** (un ou plusieurs utilisateurs) ou **externes**
  - *Principalement* ***internes*** **: 80%** d'après Jim Carr « Thwarting Insider Attacks »
  - «

POURQUOI EST-IL IMPORTANT DE MODÉLISER L'ADVERSAIRE

- **Rappel**: *On est « sécure » de ou contre quelque-chose (hackers, criminels, attaquant, etc.)*
  (Schneier on security 2010)

- Savoir **contre qui**/quoi on veut se protéger

  - Mécanismes mis en place pour **protéger une propriété contre un type d'attaque**

  - La sécurité absolue est utopique ou « **le risque 0 n'existe pas** »

  - en fonction des couts/bénéfices on se **protège contre certains attaquants**

- Mais attention, un adversaire plus puissant, des hypothèses mal calibrées et la **sécurité mise en place ne tiendra plus**

- **La sécurité inviolable n'existe pas, on cherche a rendre la vie difficile à l'adversaire**

CHOIX DES ÉQUIPES ET SUJETS

1. les (grandes) fuites de données
2. le paiement sans contact
3. le passeport vaccinal (CoVid)
4. les outils de visioconférence (Zoom, etc.)
5. les bug bounty
6. red-team vs. blue-team
7. le tatouage de vidéo et autres DRMs
8. la cryptographie quantique et/ou la cryptographie post-quantique
9. le chiffrement homomorphe
10. la e-démocratie
11. Le vote électronique et les machines à voter;
12. l'authentification biométrique
13. La sécurité offensive
14. l'évaluation des risques de sécurité
15. ...

FUITES DE DONNÉES ET MÉTADONNÉES

FUITE DE DONNÉES ?

- des données qui sont « essaimées » de façon incontrôlée
  - attaque réussie d’une base de données
  - un employé de la Sécurité sociale oublie une clé USB dans le train
  - un employé de Desjardins « exfiltre » la base de données des clients
  - j’envoie une photo qui contient des métadonnées de localisation
- etc.

QU'EST-CE QUI PEUT FUITER ?

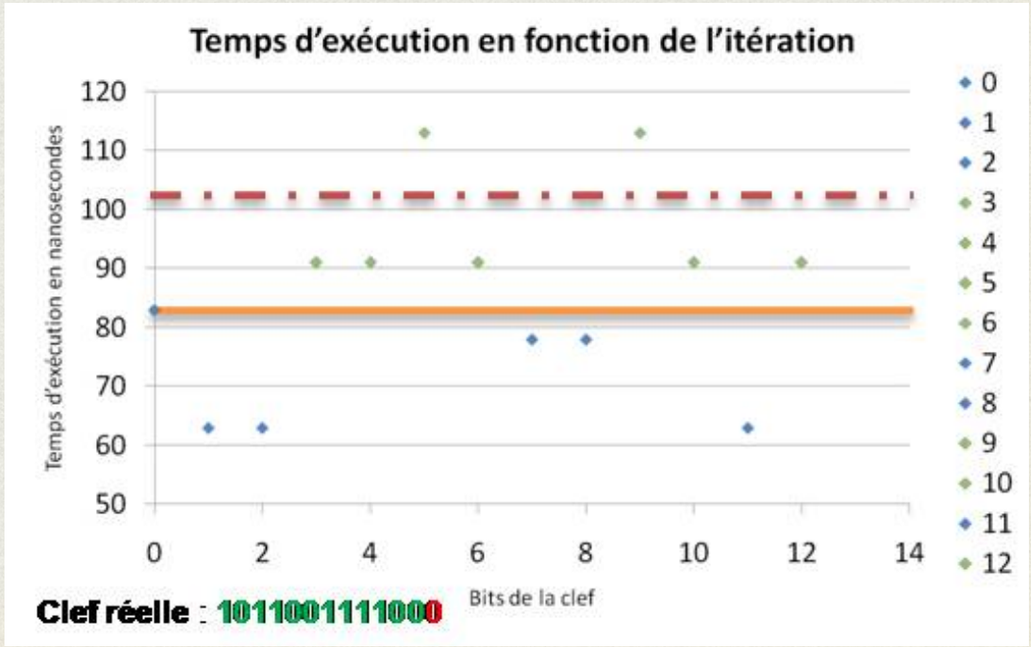
<parano mode>

Ca fuite de partout : matériel, système, applications, réseau, bases de données, web !

<\parano mode>

FUITES MATÉRIELLES

- Claviers/souris : écoutés à distance ; ou par un *key logger*
- Ecrans : à distance ou malware
- Processeurs : énergie consommée ou temps de calcul permet de retrouver la clé cryptographique
- Poubelles : disques durs, clés USB ou téléphones non-effacés



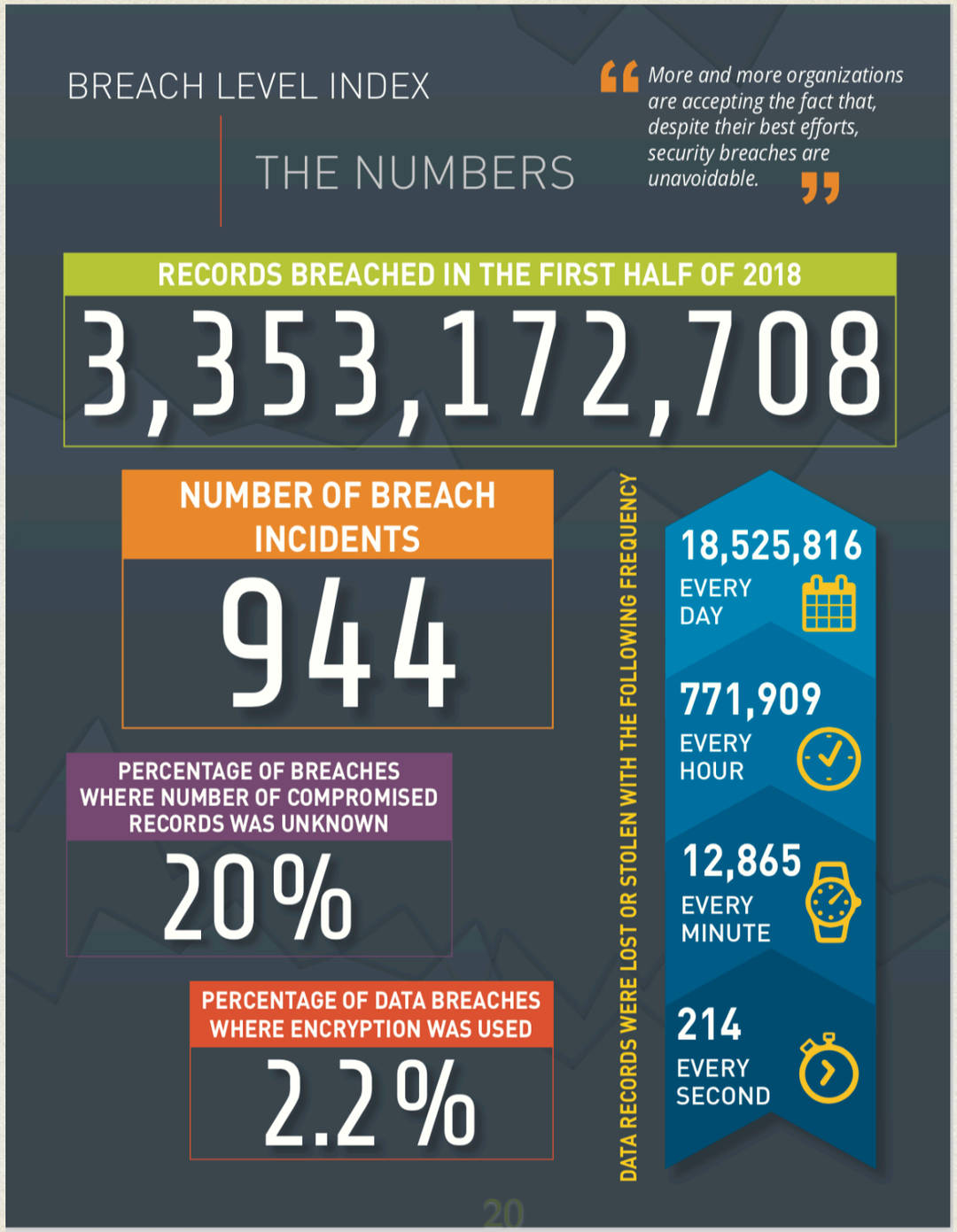
FUITES LOGICIELLES

- Téléphones intelligents qui envoient des données « à la maison » la nuit
- Applications qui oublient des métadonnées dans les documents (pdf, MSOffice, etc.) (lab)
- Photographies *géotaggées (lab)*

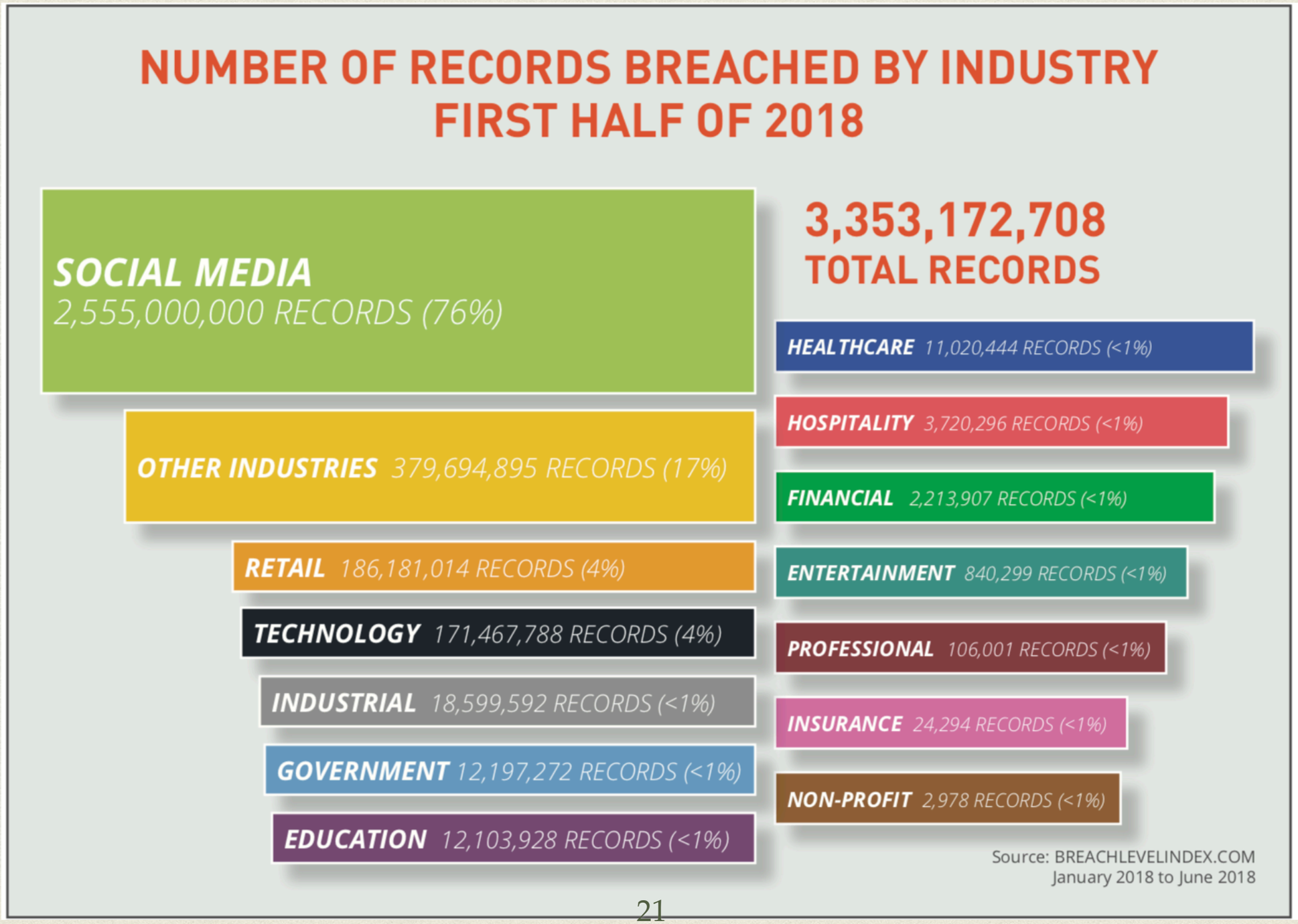
FUITES RÉSEAU

- Cookies du butineur web qui stockent à votre insu une quantité phénoménale d'information (dont des IDs) (lab)
- @IP qui sert d'ID et permet localisation (lab)
- Protocoles réseaux qui fuient

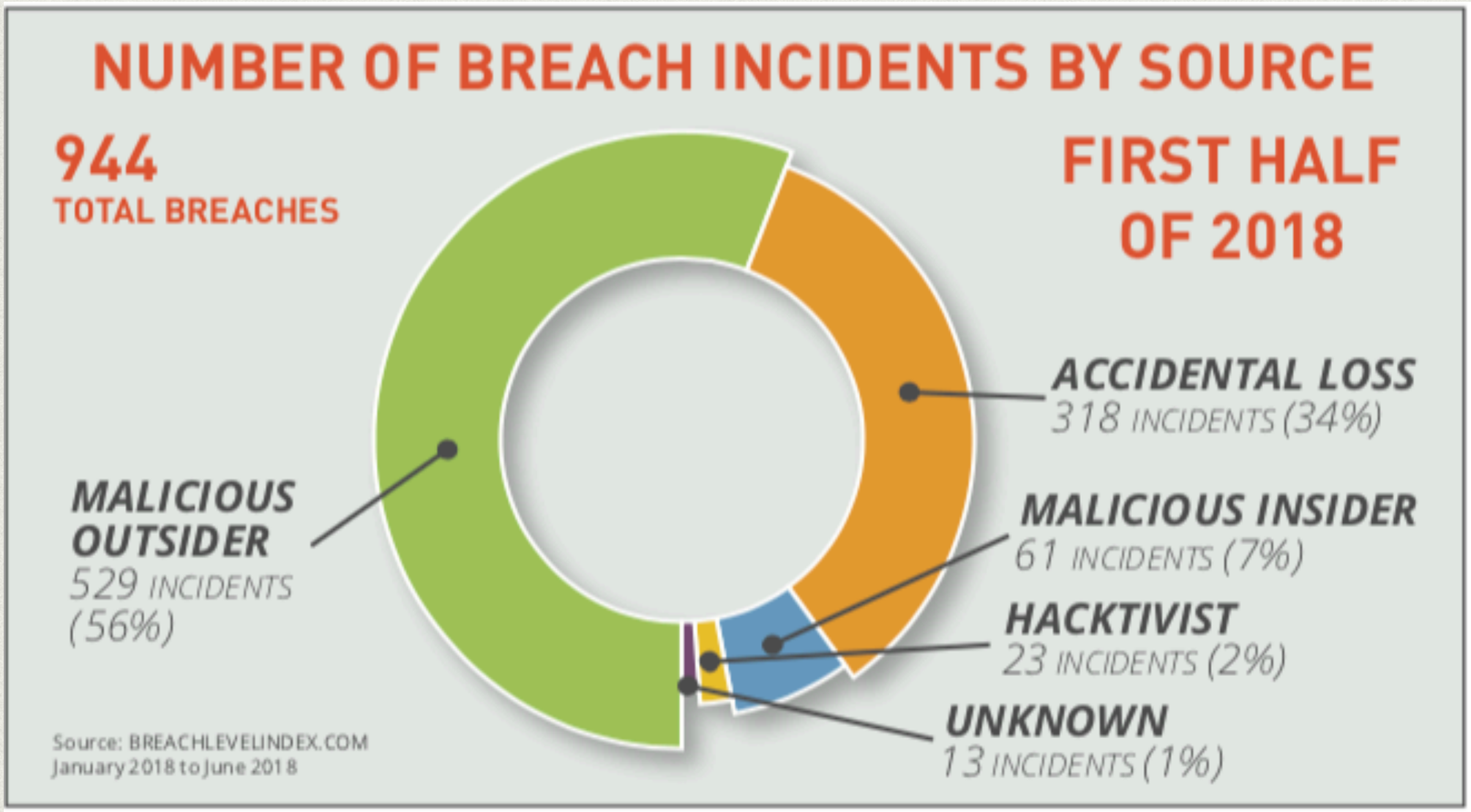
FUITES DE BASES DEDONNÉES



FUITES DE DONNÉES



FUITES DE DONNÉES



FUITES DE DONNÉES

Facebook

RECORDS BREACHED
2,200,000,000
TYPE OF BREACH
Identity Theft
SOURCE OF BREACH
Malicious Outsider
LOCATION
United States
INDUSTRY
Social Media
RISK SCORE
10.0

Facebook revealed that malicious actors could have abused its search and account recovery capabilities to scrape public profile information from most of its more than 2 billion users. The social networking platform discovered that bad actors had the option of submitting phone numbers and email addresses to locate users' public profiles and obtain personal information off them. As Facebook's CTO Mike Schroepfer explained at the time, "Given the scale and sophistication of the activity we've seen, we believe most people on Facebook [over 2 billion users] could have had their public profile scraped in this way." The tech giant responded by disabling the feature and changing its account recovery process to reduce the risk of scraping.

Exactis

RECORDS BREACHED
340,000,000
TYPE OF BREACH
Identity Theft
SOURCE OF BREACH
Accidental Loss
LOCATION
United States
INDUSTRY
Other
RISK SCORE
9.1

Florida-based marketing and data aggregation firm Exactis left a database containing 340 million individual records unprotected on the web. **Security researcher Vinny Troia** discovered in June 2018 that Exactis had left the database exposed on a publicly accessible server. The database contained two terabytes of information that included the personal details of hundreds of millions of Americans and businesses including consumers' email addresses, physical addresses, phone numbers and other extremely sensitive information like the names and genders of their children. It's unknown how many U.S. individuals the breach exposed, but 340 million individual records were stored within the database at the time of discovery.

Under Armour

RECORDS BREACHED
150,000,000
TYPE OF BREACH
Account Access
SOURCE OF BREACH
Malicious Outsider
LOCATION
United States
INDUSTRY
Retail
RISK SCORE
9.1

An attacker gained unauthorized access to software owned by Under Armour and in so doing compromised as many as 150 million people's account information. On March 25th, the American apparel manufacturer learned that someone had gained unauthorized access to **MyFitnessPal**, its platform which tracks users' diet and exercise. According to **CNBC**, those responsible accessed individuals' usernames, email addresses and hashed passwords. They did not expose users' payment information, as Under Armour processes this data separately. Nor did the unauthorized individual(s) compromise users' Social Security Numbers or driver's license numbers, as Under Armour clarified that it doesn't collect those or any other government identifiers.

Twitter

RECORDS BREACHED
336,000,000
TYPE OF BREACH
Financial Access
SOURCE OF BREACH
Accidental Loss
LOCATION
United States
INDUSTRY
Social Media
RISK SCORE
9.0

Twitter urged all its more than 330 million users to change their passwords after a software glitch exposed their credentials in plaintext. The glitch involved the failure of Twitter's hashing process to scramble users' passwords prior to writing them to an internal computer log, causing them to be recorded in readable text. According to **Reuters'** reporting on May 3, the social networking service launched an internal investigation after discussing the issue, an exposure which one source said had persisted for "several months" prior to discovery. This analysis revealed that no passwords had been stolen or abused, but out of an abundance of caution, Twitter still cautioned all 336 million users to change their passwords.

SOLUTION ?

- Contrôle de ses données
- Minimisation des données disséminées
- Protection de la vie privée

LA PROTECTION DE LA VIE PRIVÉE

MOTIVATION

- Société de l'information: grande utilisation de dispositifs électroniques connectés (+ CoVid19)
  - Fuites de t**races numériques** multiples, liées à notre **identité**
  - **Danger**: **collectées** par une entité **non-autorisée** à des fins **malveillantes**
- Ex: consultation de page web (même avec **SSL/HTTPS**)
  - **Méta-informations** : adresse du site web + adresse IP
  - Données **inférées** : sujet de la page ET **localisation**
- **Bris de vie privée**

DES TRACES ?

Blizzard

Capture d'écran de Wrath of the Lich King, une extension de World of Warcraft.

Un fugitif trahi par sa passion pour les jeux vidéo en ligne

LEMONDE.FR avec AFP | 06.01.10 | 15h42

La police américaine, qui recherchait un jeune homme en fuite soupçonné de trafic de drogue, est parvenue à le retrouver grâce à sa passion pour un jeu vidéo en ligne. C'est le site spécialisé *Massively* qui a révélé l'affaire, à la fin de l'année 2009. Les autorités de Kokomo, dans l'Indiana, étaient à la recherche d'Alfred Hightower pour trafic présumé de marijuana lorsqu'elle a appris au cours de l'enquête qu'il s'était enfui au Canada.

Les enquêteurs ont interrogé ses relations et ont appris que le jeune homme était un passionné du jeu de rôle massivement multijoueur "World of Warcraft". *"J'ai continué l'enquête et un jour j'ai eu l'information que ce type était un adepte régulier d'un populaire jeu de guerre en ligne"*, raconte à l'Agence France Presse le shérif adjoint, Matt Roberson.

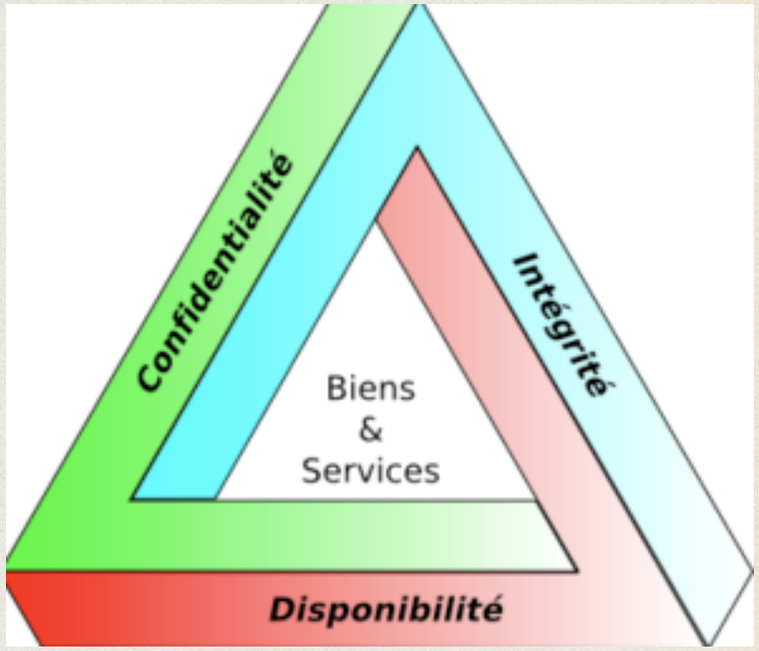
La police a obtenu une procuration pour que la compagnie éditrice du jeu, Blizzard Entertainment, lui soumette les données d'accès du fugitif au jeu en ligne, y compris son adresse IP, nécessaire à tout ordinateur pour se connecter sur Internet. *"Grâce à l'adresse IP, j'ai pu le localiser à Ottawa au Canada"*, souligne M. Roberson.

PROTECTION DE LA VIE PRIVÉE

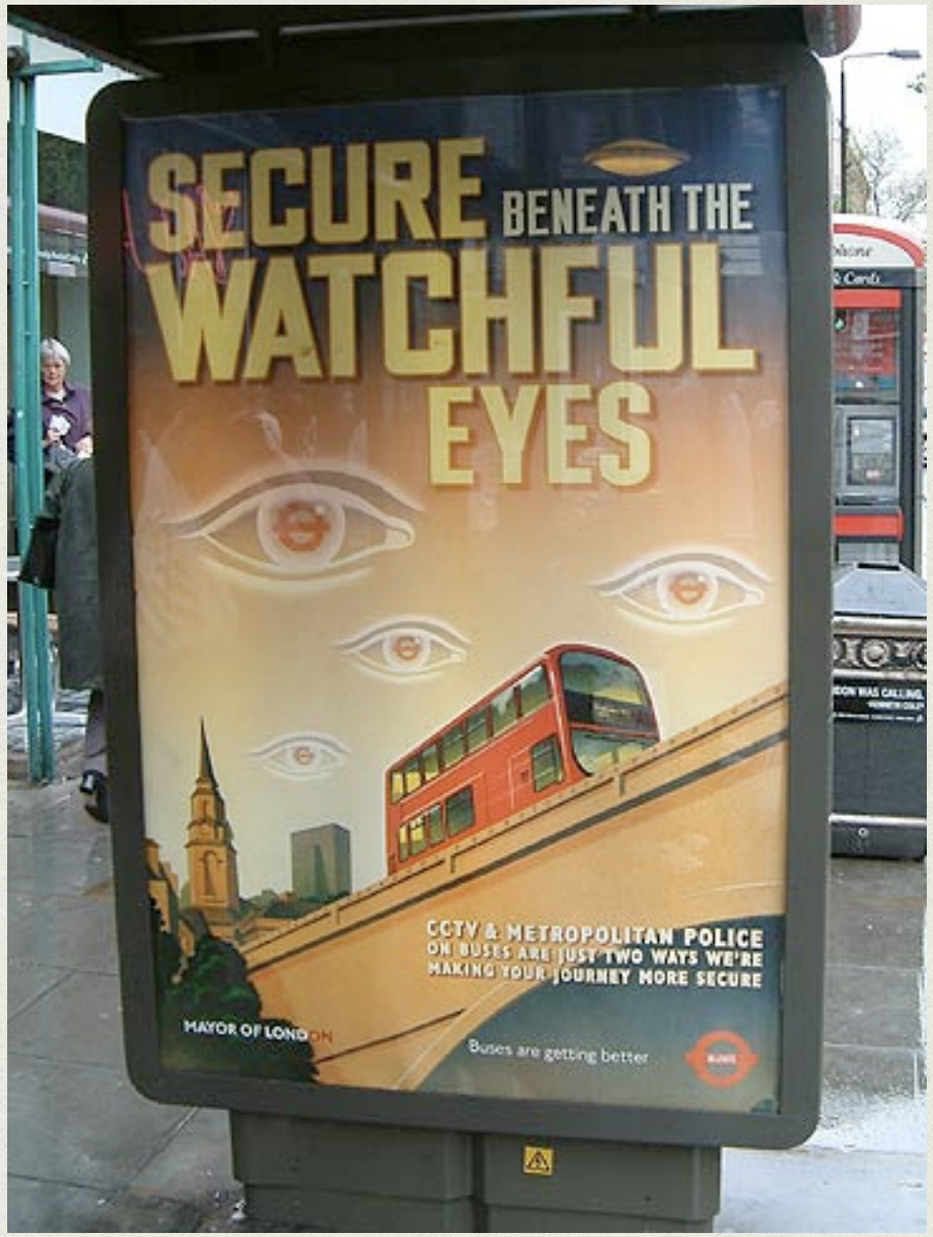
- Droit au respect de la vie privée : **droit individuel fondamental**
  - **Minimiser** les traces numériques semées
  - Grand défi de la *Société de l'Information*, difficile en mode tout connecté ou l'on sème en permanence
    - @IP=localisation, ID, contenu
    - Historique des requêtes (ou cache)=centres d'intérêt
    - Réseau social=opinions politiques ou religieuse, hobbies, etc.
    - Consommation électrique=présence et activités au domicile
    - **Danger**: information utilisée à des fins frauduleuses
      - Spam ciblé, usurpation d'ID, profilage, etc.

PROPRIÉTÉS DE SÉCURITÉ

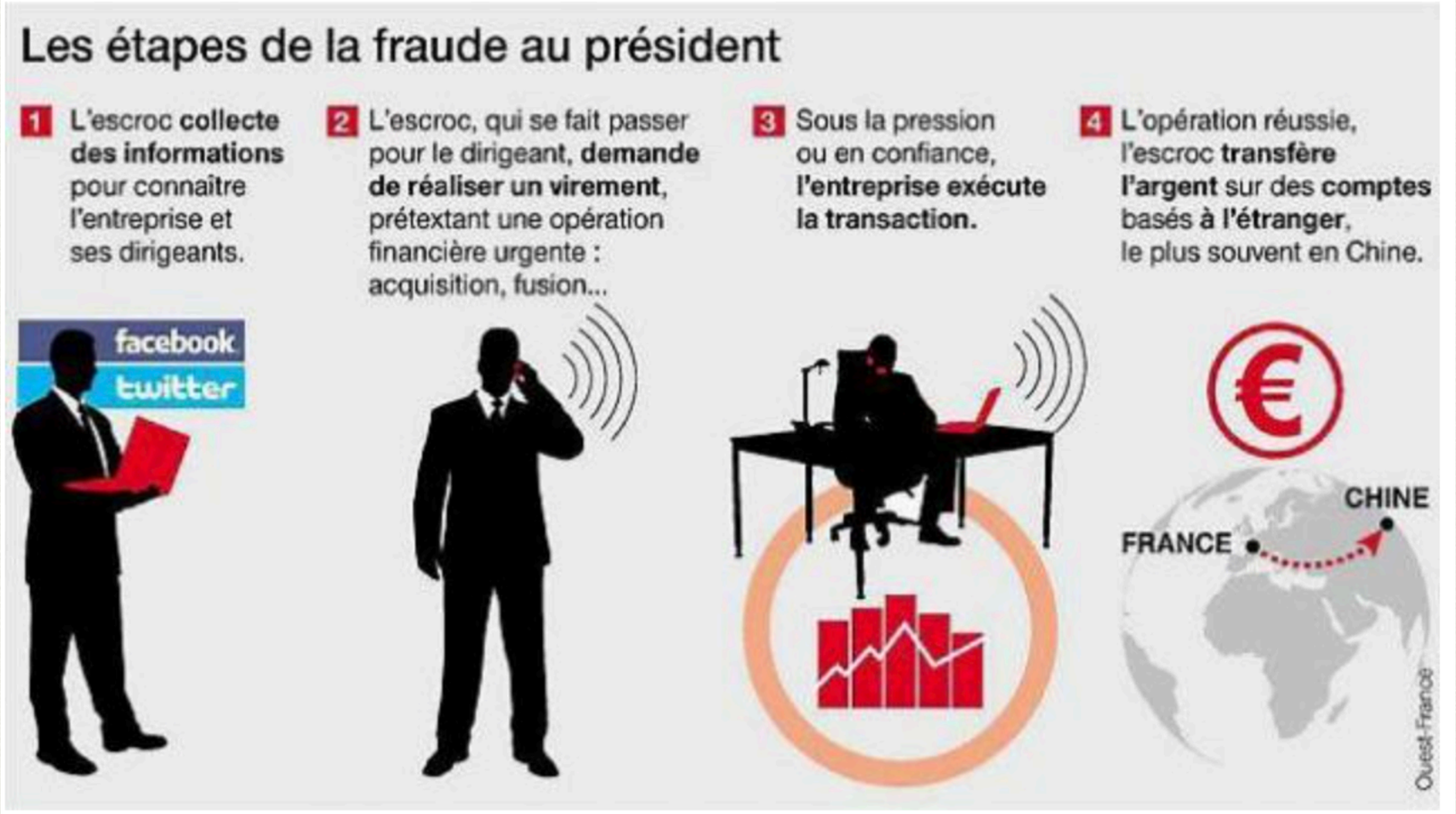
- Protection de la vie privée ~= sécurité des données personnelles
  - **Confidentialité**: contenu des messages (et des métadonnées)
  - Intégrité/**Authentification**: origine et intégrité des messages
  - **Disponibilité**: accès à l'information



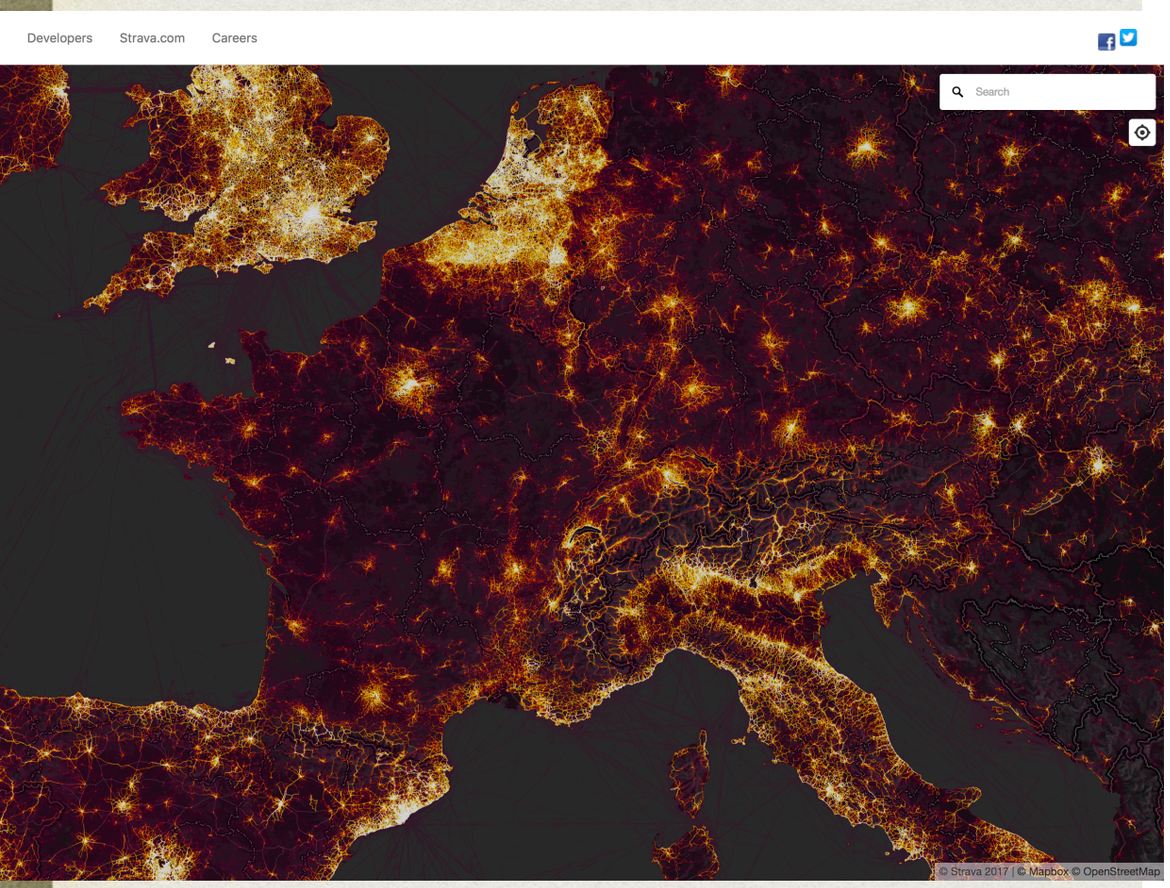
SÉCURITÉ VS. VIE PRIVÉE?



SÉCURITÉ VS. VIE PRIVÉE?



SÉCURITÉ VS. VIE PRIVÉE?



Une application de jogging menace la sécurité des bases militaires

La carte mondiale du jogging, publiée en septembre, fait apparaître des bases militaires, dont certaines sensibles.

LE MONDE | 29.01.2018 à 20h04 • Mis à jour le 30.01.2018 à 12h11 |

Par Nicolas Six

Réagir Ajouter Partager Tweeter

Des milliers de militaires utilisent Strava pour analyser leurs séances de jogging. Problème : certains laissent fuiter sur Internet le détail de leur parcours, relevé

CADRE LÉGAL

- Déclaration universelle des **droits de l'homme** des nations unies (art. 12), 1948 :
  Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

- Directives européennes, **GDPR** : Portabilité des données, consentement éclairé, transparence, sanctions renforcées, droit à l'oubli, etc.
  - GDPR : impact international - si une donnée est générée sur le sol Européen
  - **Fédéral** : PIPEDA
  - **Québec**: Loi sur la protection des renseignements personnels dans le secteur privé
    + nombreuses demandes pour dépoussiérer cette législation, en particulier **post-CoVid19**
- **USA, Californie** : *California SB1386 bill* de 2003 à initié l'obligation de déclaration des fuites de données aux USA ; *California Consumer Privacy Act of 2018* - relecture rapide du GDPR
  1/1/2020: California Consumer Privacy Act (CCPA) seuls les entreprises de Californie, max 7500$

DONNÉES À CARACTÈRE PERSONNEL

- Ensemble d'**informations concernant un individu**
  - nom, prénom, NAS, numéro de sécurité sociale, date et lieu de naissance, adresse postale, courriel, numéro de téléphone, de carte de crédit, données biométriques (empreintes digitales, ADN), ...
- Permettant de l'**identifier de manière unique** et de **croiser des fichiers**
- Limites: **quasi-identificateurs** (anodins mais uniques si combinés); @IP ou *Code Postal + âge*

COMMISSAIRES À LA PROTECTION DE LA VIE PRIVÉE

- Entité chargée de faire respecter la législation en matière de protection de la vie privée auprès des entreprises et institutions
- En France (1978) : la Commission Nationale Informatique et Libertés (CNIL)
- En Europe : regroupés dans le G29 puis dans le *Comité Européen de la Protection des Données* depuis le GDPR
- Fédéral : Commissariat à la Protection de la Vie Privée (CPVP)
- Québec : Commission d'Accès à l'Information (CAI)

PRÉ GDPR

France slaps Google with fine, remedial measure

Google gets hit with the largest fine ever levied by French privacy regulatory group CNIL, which tacked on a bit of humiliation for the company in the process.

by Seth Rosenblatt | January 8, 2014 11:52 AM PST

Follow

40 140 13 g+1 18 More + Comments 51

France's privacy regulatory organization served up a fine and a dose of embarrassment to Google on Wednesday.

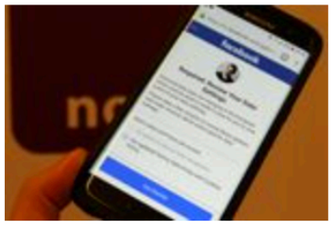
As expected, the national committee on information and liberty (CNIL) served up a 150,000 euros fine (approximately $200,000). The amount won't mean much to Google financially. But in addition to the fine, the group demanded that Google post a warning on its French home page, Google.fr.

The warning must state that the company's unified privacy policy from March 1, 2012 does not comply with French law.

POST GDPR

RGPD : Facebook et Google déjà visés par d'onéreuses plaintes

Le lundi 28 Mai 2018 à 09:30 par Jérôme G. | 15 commentaire(s)



Au premier jour de l'entrée en vigueur en Europe du Règlement général sur la protection des données (RGPD), quatre plaintes sont apparues à l'encontre de Facebook et Google. Le cas échéant, elles représentent des amendes au montant total de 7,6 milliards d'euros.

Me Marie-Eve Tourigny, Avocate - Avocat dpj protection jeunesse
Avocate contre DPJ, contactez-nous rapidement. Aide juridique acceptée metourignyavocate.com

Cela n'a pas traîné. À peine le Règlement général sur la protection des données entré en vigueur au sein de l'Union européenne, la nouvelle association noyb.eu de défense contre les violations de données sur le long terme dépose quatre plaintes pour consentement dit forcé.

Ces plaintes visent Google (Android), Instagram, WhatsApp et Facebook, en rappelant que Instagram et WhatsApp sont tous deux dans le giron de Facebook. Noyb (none of your business) demande aux régulateurs en France, Belgique, Allemagne et Autriche, des sanctions à hauteur de 4 % du chiffre d'affaires des groupes pointés du doigt.

L'amende potentielle monte à 3,7 milliards d'euros pour Google et 1,3 milliard d'euros chacun pour Instagram, WhatsApp et Facebook.

ADVERSAIRE

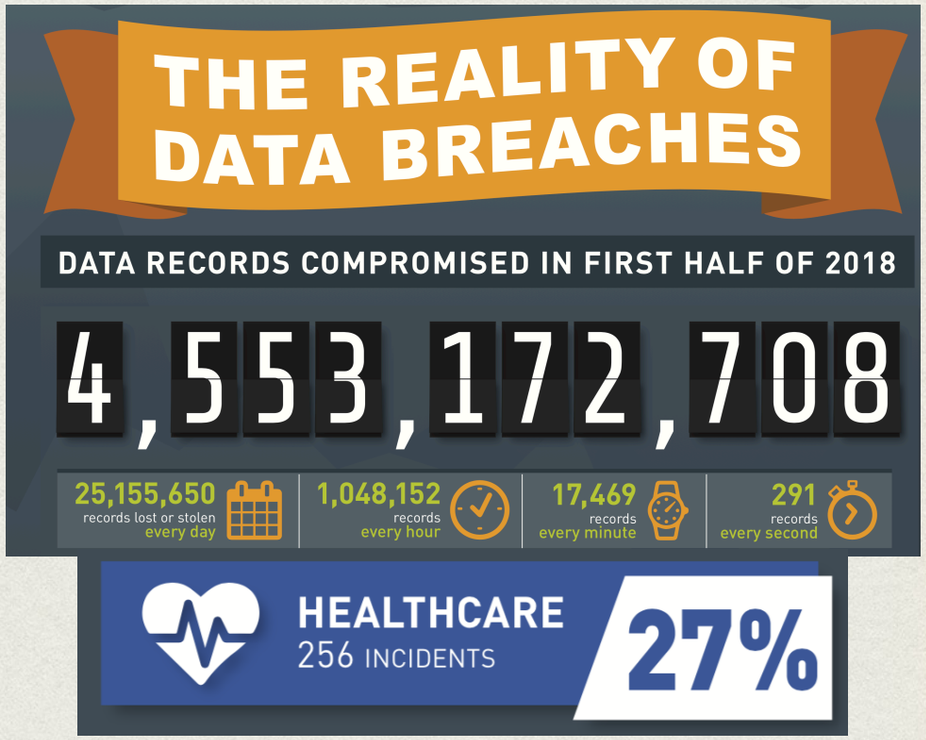
- Entité (individu, organisation ou entreprise) **collectant les traces numériques** d'un individu afin de **commettre un bris de vie privée**

- **Sources de données**: publiques (blogs, réseaux sociaux, aggrégateurs de données), récupération passive (capture sur le réseau), vulnérabilité système (*hameçonnage*, hack)

ADVERSAIRE

- Entité (individu, organisation ou entreprise) collectant les traces numériques d'un individu afin de commettre un bris de vie privée

- Sources de données: publiques (blogs, réseaux sociaux, agrégateurs de données), récupération passive (capture sur le réseau), vulnérabilité système (*phishing*, hack)



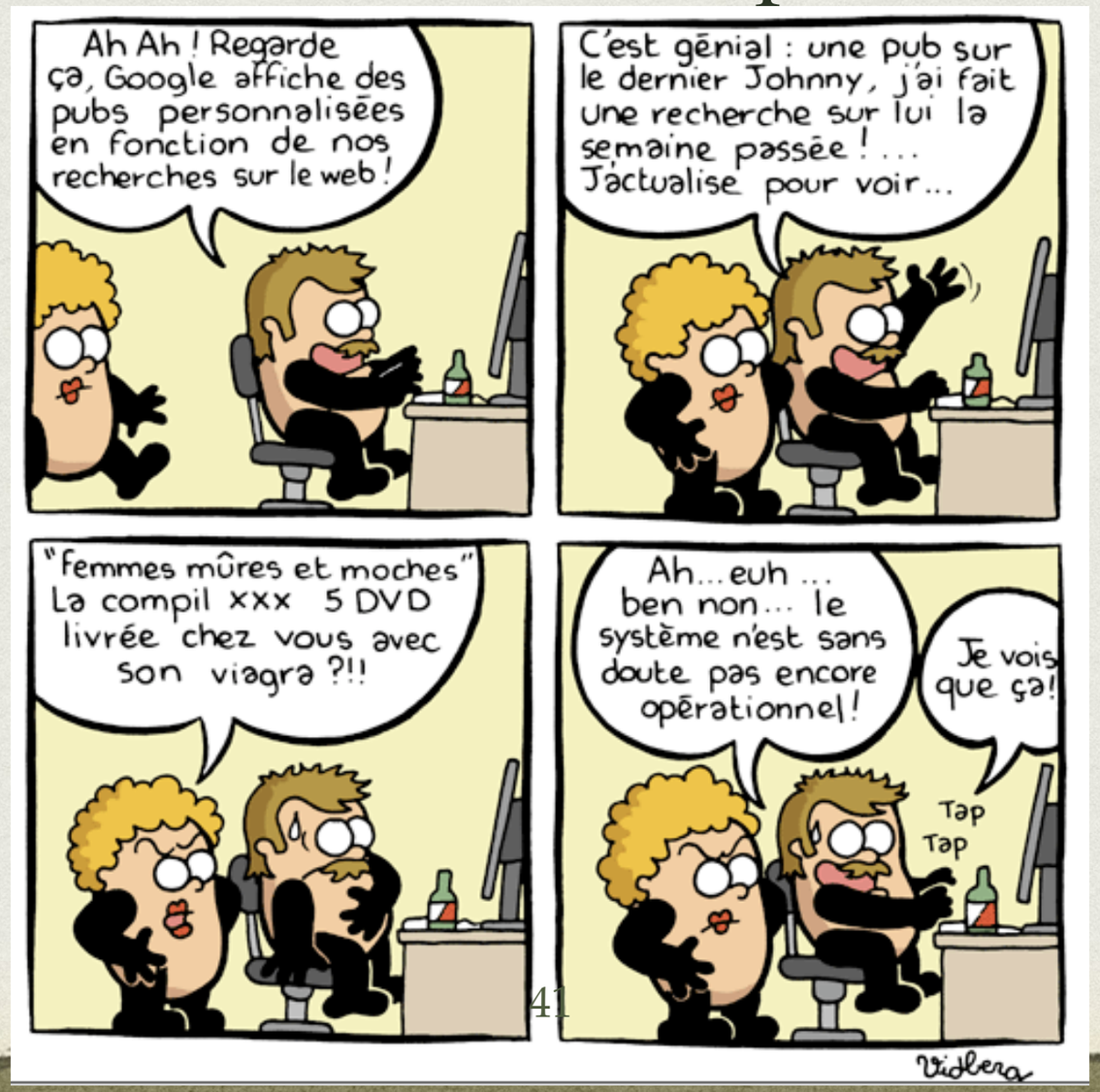
source: breachlevelindex.com 2018H1 report

RISQUES

- Pourriel ciblé
- Mauvaise réputation et crédibilité
- Cyberprédation
- Chantage
- Usurpation d’identité

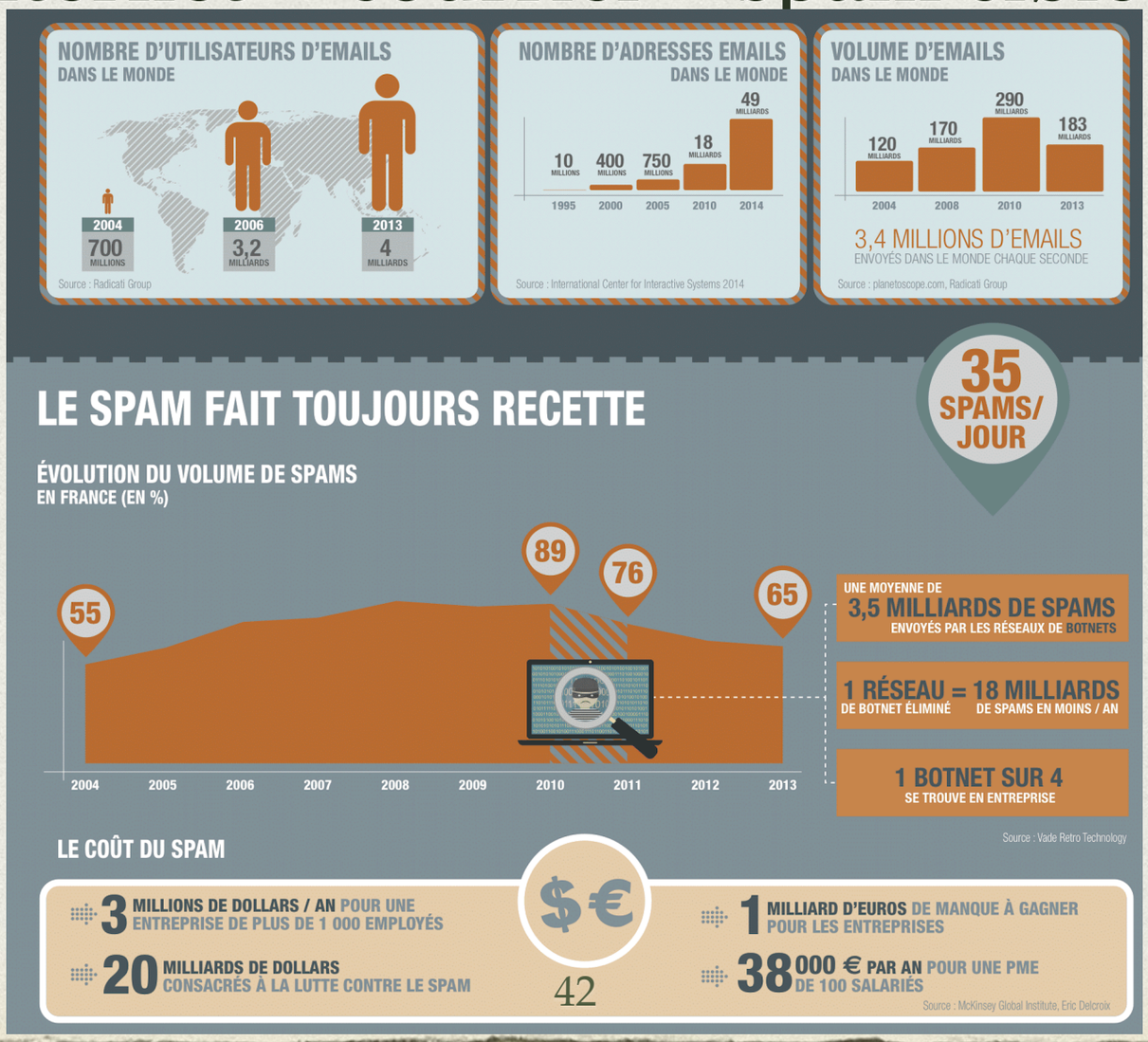
RISQUE : PUBLICITÉ CIBLÉE ET PROFILAGE

- Traces numériques pour établir un profil individuel : requêtes internet + courriel = spam ciblé



RISQUE : PUBLICITÉ CIBLÉE ET PROFILAGE

- Traces numériques pour établir un profil individuel : requêtes internet + courriel = spam ciblé = **$$$$$**



RISQUE : RÉPUTATION ET CRÉDIBILITÉ

- Selon une étude américaine, 86% des employeurs consultent les réseaux sociaux des candidats : une photo mise en ligne durant un *party* peut poser difficulté ....

RISQUE : RÉPUTATION ET CRÉDIBILITÉ

- Une fois embauché aussi ....

Des allocations supprimées pour un sourire

Par Louise Cuneo

La compagnie d'assurance Manulife s'est notamment appuyée sur les photos éditées sur Facebook par sa cliente pour lui supprimer ses allocations de congé maladie © ANDREW HARRER/LANDOV/MAXPPP

VOS OUTILS

Imprimez Réagissez Classez

Buzzer !
sur Yahoo!

Nathalie Blanchard rit jaune. Les photos de la Québecoise de 29 ans diffusées sur Facebook n'ont pas plu à son assureur. Motif : la jeune femme s'affichait sourire aux lèvres à un spectacle de Chippendales. Seulement, voilà : officiellement, Nathalie Blanchard était en congé maladie pour dépression depuis plus d'un an, date à laquelle elle s'était retirée de son poste chez IBM, à Bromont. Et elle avait l'air, sur ces clichés, un peu trop heureuse pour continuer à toucher ses allocations. Celles-ci ne lui ont ainsi plus été versées depuis cet automne.

RISQUE : CYBERPRÉDATION

- Vérifier l'identité de ses contacts sur les réseaux ?

- Ex. Fortnite (voir l'article, sordide)

RISQUE : CYBERCHANTAGE

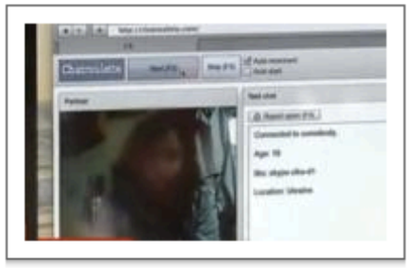
- Impossible d'effacer l'information postée !

Cyberchantage: un lycéen brestois de 18 ans se suicide

Un lycéen de 18 ans s'est donné la mort, sous la terrible menace d'un chantage à la webcam sur Internet, orchestré depuis l'étranger.

Frédéric Bergé | 01net. | le 29/10/12 à 09h26 | 1 réaction

Recommander 14 Tweeter 22 +1 1



agrandir la photo

Un lycéen de 18 ans a été pris au piège d'une arnaque à la webcam sur Internet et a été acculé au suicide sous la menace d'un chantage, a révélé ce week-end le quotidien breton, *Le Télégramme de Brest*. Ces faits tragiques ont été rendus publics par les parents du jeune homme.

La semaine dernière, le lycéen s'était connecté depuis son domicile sur un site de discussions (*chat*) et après s'être livré à des jeux érotiques devant la webcam de son ordinateur aurait été victime d'un terrible chantage : son interlocutrice le sommant en anglais de lui donner 200 euros en le menaçant de diffuser les images compromettantes du jeune homme qu'elle venait d'enregister à son insu. Il a choisi de mettre fin à ses jours quelques heures après, sous la terrible menace.

Une plainte contre X aurait été déposée. L'analyse de l'ordinateur du lycéen a révélé que son interlocutrice se serait connectée depuis la Côte d'Ivoire. Ce tragique épisode confirme

RISQUE : USURPATION D'IDENTITÉ

- Traces numériques pour établir un profil individuel : usurpation d'identité

Près de 213.000 cas d'usurpation d'identité en France chaque année, selon le CREDOC

AP | 06.10.2009 | 19:12

Près de 213.000 cas d'usurpation d'identité avérés sont enregistrés chaque année en France, d'après une étude publiée mardi par le CREDOC. Comptes débités, emprunts indûment contractés, prestations sociales détournées: les escroqueries liées au vol de données personnelles coûteraient en moyenne près de 2.229 euros à chaque victime, soit un total de 474 millions d'euros.

L'enquête a été réalisée par le Centre de recherche pour l'étude et l'observation des conditions de vie (CREDOC) pour Fellowes, une entreprise qui produit notamment des machines de destruction de documents.

Selon les calculs du CREDOC, 212.762 personnes sont victimes d'usurpation d'identité en France chaque année, phénomène qui serait ainsi plus fréquent que les cambriolages au domicile principal (153.000 environ). Sur 2.007 personnes interrogées, 4,2% ont déclaré avoir été victimes d'une usurpation d'identité au cours des dix dernières années.

Dans plus de la moitié des cas, les usurpateurs débitent le compte bancaire (51,9% sur 300 personnes victimes d'une usurpation). Autre escroquerie fréquente, ils contractent un ou plusieurs emprunts au nom de leur victime (21,7%) ou bénéficient de prestations sociales à leur place (11,1%). Mais ils peuvent aussi causer des infractions au code de la route (16,9%), prendre un emploi (1,7%) ou même réaliser un mariage (1,7%) en se faisant passer pour leur victime.

La grande majorité des personnes visées découvrent qu'on leur a volé leur identité en vérifiant leur relevé bancaire (41,4%), en recevant des factures ou procès-verbaux indus (18,7%).

Le coût d'une usurpation atteint en moyenne 2.228,7 euros, entre le montant des détournements (1.520,4 euros), les démarches administratives et judiciaires (564,5 euros) et les coûts supplémentaires comme les frais médicaux ou postaux (142,8 euros). Sur ce total, le montant des remboursements atteint 661,8 euros en moyenne, 1.566,9 euros restant à la charge de la victime.

M Société

SOCIÉTÉ | Police et justice | Éducation | Enquête | Santé | Logement | Famille - vie privée | Immigration

L'usurpation d'identité a doublé en France

Le Monde.fr avec AFP | 10.10.2012 à 10h48 • Mis à jour le 10.10.2012 à 11h18

Abonnez-vous à partir de 1 € | Réagir | Classer | Imprimer | Envoyer | Partager

Recommander | Envoyer | 146 personnes le recommandent.

Quatre cent mille personnes, soit 8 % des Français, déclarent avoir été victimes d'une usurpation d'identité au cours des dix dernières années alors qu'elles n'étaient que 4 % en 2009, selon un sondage CSA publié mercredi 10 octobre. Parmi les personnes interrogées, 34 % estiment que ce risque est *"peu élevé ou totalement nul"*, 45 % qu'il est *"assez élevé"* et 18 % qu'il est *"très élevé"*.

L'usurpation d'identité est le fait de prendre délibérément l'identité d'une autre personne vivante pour réaliser des actions frauduleuses commerciales, civiles ou pénales, accéder aux finances de la personne usurpée ou commettre en son nom un délit, ou accéder à des droits (indemnités sociales) de façon indue. Le criminologue Christophe Naudin, spécialiste de la criminalité identitaire, relève que cette forme de délinquance est en passe de devenir la deuxième infraction en France devant les cambriolages (333 338 en 2011) et derrière le vol de véhicule (552 125 en 2011).

RISQUE : USURPATION D'IDENTITÉ

- Traces numériques pour établir un profil individuel : usurpation d'identité = **$$$$$**

ID theft scams target Canada's health-care system

Criminals are exploiting lax security in government databases to assume false identities and take advantage of Canada's health-care system, warns a leading expert in identity fraud.

BY THE OTTAWA CITIZEN NOVEMBER 3, 2008 BE THE FIRST TO POST A COMMENT

For a time, "the competition for dead children was so fierce that we had situations where two and three different crime groups were accessing the same dead child's identity," said Mr. Pendleton.

BUSINESS

- 2018: 150000 fraudes et vols d'identité au Canada
  - +12% / 2017
  - +58% / 2011
  - ~120 M$
  - « seulement » 17000 au Québec
- Après *Desjardins* : augmentation ?

DESJARDINS 2019

- « Les données volées liées aux 4,2 millions de comptes de particuliers touchés contiennent les noms et prénoms, dates de naissance, numéros d'assurance sociale, adresses, numéros de téléphone, adresses de courriel, habitudes transactionnelles et des détails sur les produits financiers détenus par les clients. «

- Offre de service de protection par Equifax …

EQUIFAX

- 2015: fuite des données fiscales d'entreprises
- 2016: fuite des données fiscales de particuliers
- sept. 2017: Equifax révèle une intrusion datant de mi-mai à fin-juillet
  - **147M** de clients - 44% des américains - (noms, NAS, date de naissance, scores de crédit, adresses, etc.)
- 2019: Equifax accepte une amende de **575M$** (voire 700M$) dans un accord avec la FTC

VALEUR DE LA VIE PRIVÉE ?

VALEUR DES DONNÉES PERSONNELLES

- Marché officiel vs. marché noir :

Federal law (*See* 18 U.S.C. § 2706) requires law enforcement to reimburse providers like Yahoo! for costs incurred responding to subpoena requests, court orders, or search warrants. Yahoo! generally requests reimbursement when responding to legal process, except that Yahoo! maintains an exception to this policy for cases involving the abduction or exploitation of children. Yahoo! may waive reimbursement in specific cases or recognize additional exceptions to this policy in the future.

Yahoo! will seek reimbursement based on the actual time expended by Yahoo!'s compliance staff in complying with the request. The average costs related to compliance matters are listed below for your convenience. These estimates are neither a ceiling nor a floor but represent the average costs of typical searches. Time spent may vary considerably based on the wording of the request and the information available about the user. These time estimates are also based on narrowly tailored requests that do not require extensive searches in multiple databases. These estimates are not price quotes, budgets, or guarantees and should not be used for budgeting purposes. Yahoo! reserves the right to adjust its estimates and reimbursement charges as necessary.

- Basic subscriber records: approx. $20 for the first ID, $10 per ID thereafter
- Basic Group Information (including information about moderators): approx. $20 for a group with a single moderator
- Contents of subscriber accounts, including email: approx. $30-$40 per user
- Contents of Groups: approx. $40 - $80 per group

VALEUR DES DONNÉES PERSONNELLES

- Marché officiel vs. marché noir :
  - carte de credit (*fullz*) : 13-21$
  - comptes bancaires : 100-1000$
  - données médicales : 100$
  - compte netflix : .50$
  - ...
- Attention à bien effacer vos disques et téléphones avant de les jeter, vendre !
- Plus sur le sujet dans la vidéo d'Alain Rallet dans les activités de la semaine

TECHNOLOGIES DE PROTECTION DE LA VIE PRIVÉE

PROTECTION AU PLUS TÔT !

- Comme pour les **considérations non-fonctionelles**, comme la **sécurité** (security ET safety), il est plus facile (lire **moins cher**) de prendre en compte la protection de la vie privée dès la **conception**

- **Privacy-by-design** (Ann Cavoukian, commissariat PvP ON):
  vie privée *a priori* plutôt que de réagir *a posteriori* après un bris de vie privée

  - Utilisation de PETs ....

La promotion de l'utilisation des technologies d'amélioration de la confidentialité (PET), ainsi que le soulignait déjà la communication de la Commission de 2007 à ce sujet, ainsi que du principe de prise en compte du respect de la vie privée dès la conception («*Privacy by Design*») pourrait jouer un rôle important à cet égard, y compris pour garantir la sécurité des données[30].

La Commission examinera les mesures suivantes destinées à responsabiliser davantage les responsables du traitement:

---

29 Voir, notamment, l'avis n° 3/2010 du groupe de travail «Article 29» adopté le 13 juillet 2010.

30 S'agissant des PET, voir: communication de la Commission au Parlement européen et au Conseil sur la promotion de la protection des données à l'aide de technologies d'amélioration de la confidentialité ou PET (*Privacy Enhancing Technologies*) [COM(2007) 228 final]. Le principe de «*Privacy by Design*» signifie que la protection de la vie privée et des données à caractère personnel est prise en compte tout au long du cycle de vie des technologies, depuis le stade de leur conception jusqu'à leur déploiement, utilisation et élimination finale. Ce principe figure notamment dans la communication de la Commission intitulée «Une stratégie numérique pour l'Europe» [COM(2010) 245].

PETS

- Privacy-Enhancing-Technologies (PETs) - Technologies d'Amélioration de la Confidentialité (TACs)

- Techniques qui permettent de **protéger** ses informations personnelles et de **contrôler** ses traces numériques : **Minimisation et Souveraineté**

- par exemple **anonymisateur** : service permettant de naviguer « anonymement » qui masque les infos personnelles (@IP, système, etc.) - anti « *fingerprinting* » amiunique.org (laboratoire)

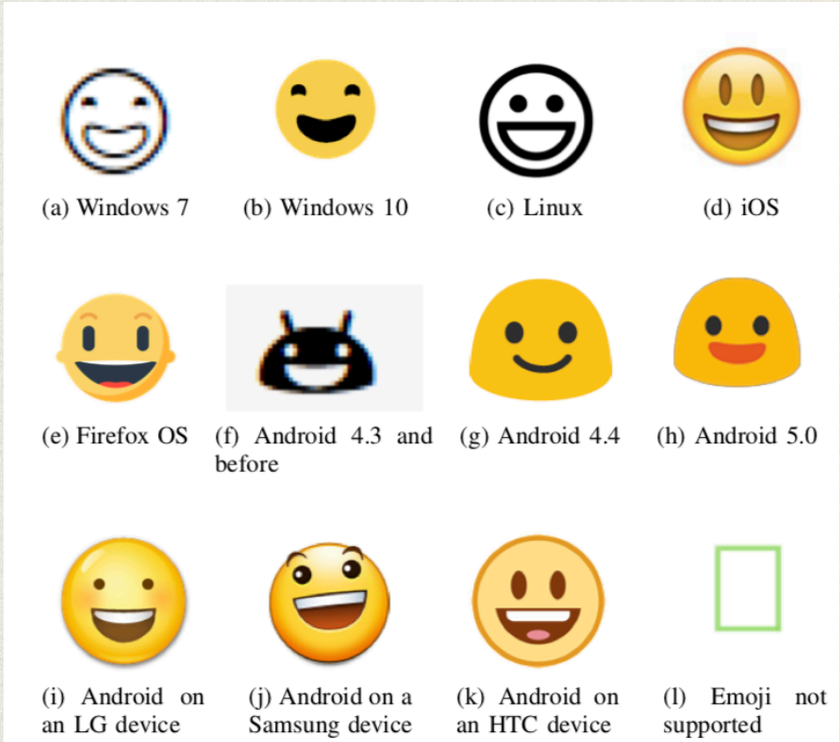


Fig. 2. Comparison of the "Smiling face with open mouth" emoji on different devices and operating systems

PRINCIPES FONDAMENTAUX

- **Minimisation**: seule l'information **nécessaire** devrait être collectée
  - Droit: critère de légitimité
  - Nombreux TACs : anonymisateur, PIR, PSI, etc.
- **Souveraineté**: les données liées à un individu lui **appartiennent** et il devrait pouvoir **contrôler** leur dissémination et leur usage
  - Extension de la législation sur les données médicales
  - Difficile dans un monde ultra-connecté (fuites de données in-controlées)
  - **Droit**: consentement, transparence, droit à l'oubli, portabilité, imputabilité, etc.
  - Peu de TACs car **techniquement difficile à assurer** (salage des données, tracer les traitres)

DIFFÉRENTS NIVEAUX DE PROTECTION

- **Pseudonymat** : utiliser un pseudonyme au lieu de son identité
  - *ElCuistoLoco* sur Ricardo, *MadMovix* sur IMDB, etc.
- **Anonymat**: pouvoir réaliser une action sans qu'elle puisse être reliée à une identité particulière
  - Emprunter le réseau de transport de façon anonyme
- **Non-chaînabilité** : être incapable de relier deux actions anonymes menées par le même individu
  - Visionné *50 shades of grey* et La ligne verte ....
- **Non-observabilité** : ne pas pouvoir détecter si une action particulière a eut lieu
  - Système téléphonique anti-lobbying au parlement Européen

CLASSIFICATION DES MÉTHODES DE PROTECTION

- **Moment** :
  en-ligne (durant la connexion, à la génération de l'information)
  hors-ligne (accès aux données stockées dans un BDD)

- **Objectif** :
  protection individuelle (local) ou de groupe (global)

- **Technique** :
  perturbation de l'information
  cryptographie ou calcul multiparité sécuritaire
  accès restreint ou limité à l'information (e.g. niveau requêtes)

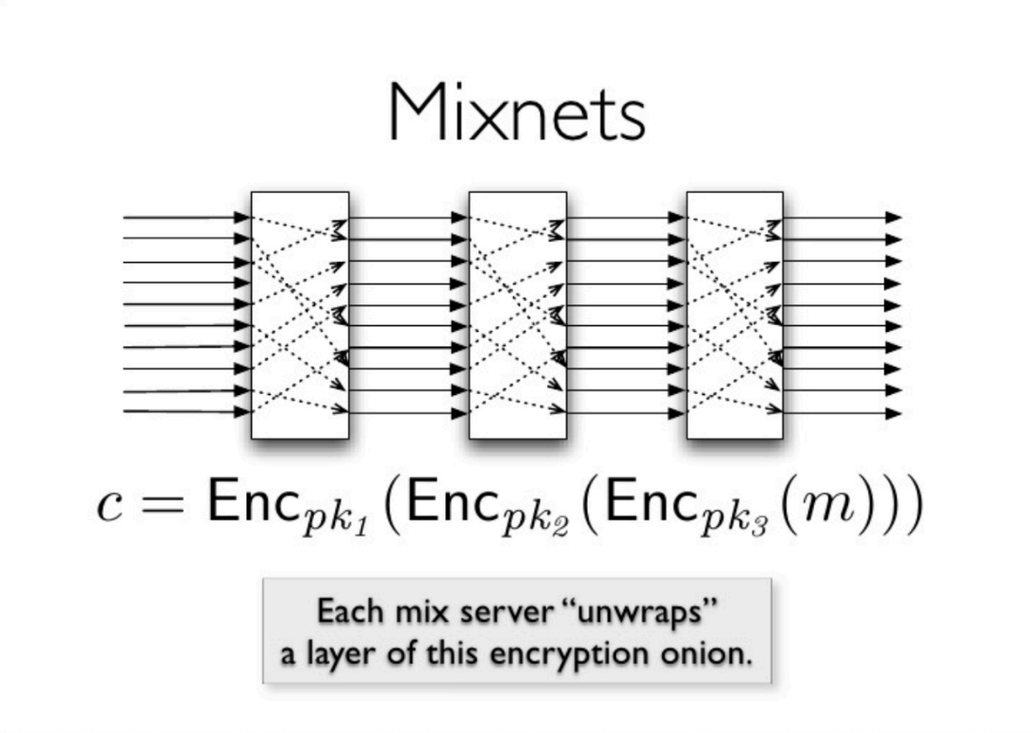
- **Autres dimensions**: localité, interactivité, adaptabilité, paramètrisation, etc.

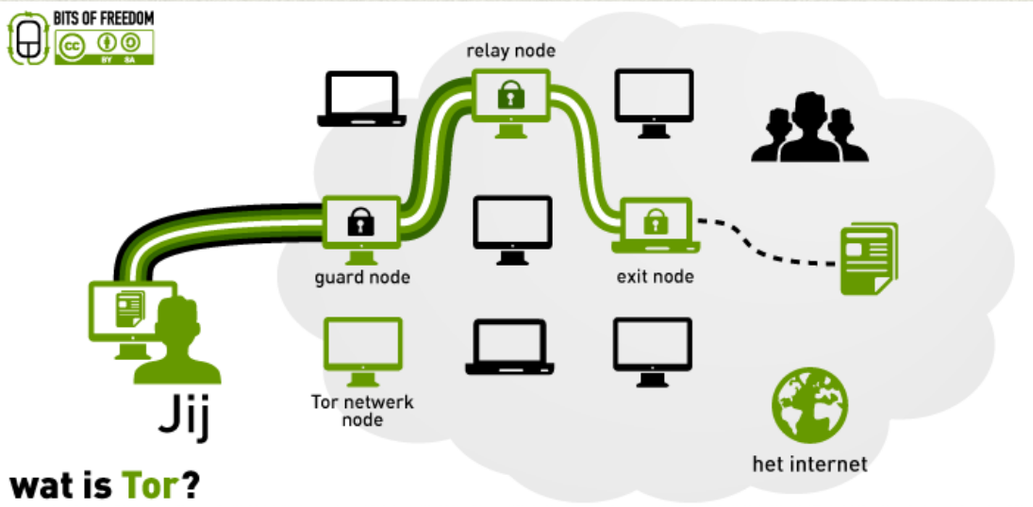
QUELS TACS

- Communications *anonymes*
- Accréditations *anonymes*
- Authentification biométrique
- Retrait d'information *privé*
- Intersection d'ensemble *privée*
- … pour l'instant un petit **aperçu** en termes **d'usage**

COMMUNICATIONS ANONYMES

- communiquer de façon anonyme dans un réseau
  - protéger ID émetteur et/ou récepteur
  - ex: MixNets, routage en oignon (TOR), Crowds.
- Brique de base pour d'autres TACs pour cacher l'identité d'une entité derrière une action, envoi de messages
  - ex.: surf anonyme sur internet, mail anonyme, téléphonie non-observable





ACCRÉDITATIONS ANONYMES

- Version **anonyme** des **accréditations**
  - Prouver une propriété ou un droit lié au possesseur de l'accréditation, **mais sans révéler son identité**
  - Souvent sous la forme d'un **jeton cryptographique** montré pour prouver une propriété liée à son possesseur
    - **créé** et **certifié** par une autorité de confiance qui garantit son authenticité
    - **vérifiable** par d'autres entités
- Ex: signatures de groupe, signatures aveugles, preuve de connaissance à divulgation nulle

RETRAIT D'INFORMATION PRIVÉ

- **PIR** pour *Private Information Retrieval*
- **Définition informelle**: protocole qui permet à un utilisateur de récupérer un élément dans une base de données sans révéler son choix
- ~~Retrait d' {Information Privée}~~ : non **l'information** est a priori **publique**
- {Retrait privé} d'information : c'est la **sélection** qui est **privée**
- Ex: Netflix, Stock Exchange, License et brevets, etc.

BREF ....

- TACs font de la protection en-ligne, sur les services
- Techniquement possible de concevoir des systèmes qui protègent la vie privée
- Certes, c'est plus couteux (temps de calcul, $)
- Mais moins cher de le faire a priori que de traiter une fuite de donnée a posteriori (procès, image, etc.)

ASSAINISSEMENT DE DONNÉES ET ATTAQUES

IL SUFFIT DE PSEUDONYMISER

- Replacer l'ID par un pseudonyme ne suffit pas !

A Face Is Exposed for AOL Searcher No. 4417749

The New York Times — August 8, 2006

What Revealing Search Data Reveals

AOL posted, but later removed, a list of the Web search inquiries of 658,000 unnamed users on a new Web site for academic researchers. An interview with one of those unnamed users, Thelma Arnold, combined with her data reveal what she was searching for, why and on which Web sites.

A sample of Thelma Arnold's search data released by AOL

4417749	swing sets	2006-04-24	15:39:30	4	http://www.byoswingset.com
4417749	swing sets	2006-04-24	15:39:30	9	http://www.buychoice.com
4417749	swing sets	2006-04-24	15:39:30	10	http://www.creativeplaythings.com
4417749	swing sets	2006-04-24	15:39:30	5	http://www.childlife.com
4417749	swing sets	2006-04-24	15:39:30	6	http://www.planitplay.com
4417749	that do not shed	2006-04-28	9:05:54	2	http://www.gopetsamerica.com
4417749	dog who urinate on everything	2006-04-28	13:24:07	6	http://www.dogdaysusa.com
4417749	walmart	2006-04-28	14:07:32	1	http://www.walmart.com
4417749	womens underwear	2006-04-28	14:12:28	10	http://www.bizrate.com
4417749	jcpenny	2006-04-28	14:16:05		
4417749	jcpenny	2006-04-28	14:16:49	1	http://www.jcpenney.com
4417749	tortus and turtles	2006-04-29	13:12:47		
4417749	manchester terrier	2006-05-02	9:05:31	1	http://www.manchesterterrier.com
4417749	delta	2006-05-02	11:49:26		
4417749	fingers going numb	2006-05-02	17:35:47		
4417749	dances by laura	2006-05-02	17:59:32		
4417749	dances by lori	2006-05-02	17:59:57		
4417749	single dances	2006-05-02	18:00:18	1	http://solosingles.com
4417749	single dances in atlanta	2006-05-02	18:01:13		
4417749	single dances in atlanta	2006-05-02	18:01:50		
4417749	dry mouth	2006-05-06	16:49:14	2	http://www.mayoclinic.com
4417749	dry mouth	2006-05-06	16:49:14	8	http://www.wrongdiagnosis.com
4417749	tyroid	2006-05-06	16:55:34		
4417749	thyroid	2006-05-06	16:55:44		
4417749	competitive market analysis of homes in lilburn	2006-05-14	12:14:52		
4417749	competitive market analysis of homes in lilburn	2006-05-14	12:16:17		
4417749	competitive market analysis of homes in lilburn	2006-05-14	12:16:43		

Why the search

"I was thinking about my grandchildren"

"I was looking for some."

"A woman was in the [public] bathroom crying. She was going though a divorce. I thought there was a place called 'Dances by Lori,' for singles."

"I wanted to find out what my house was worth."

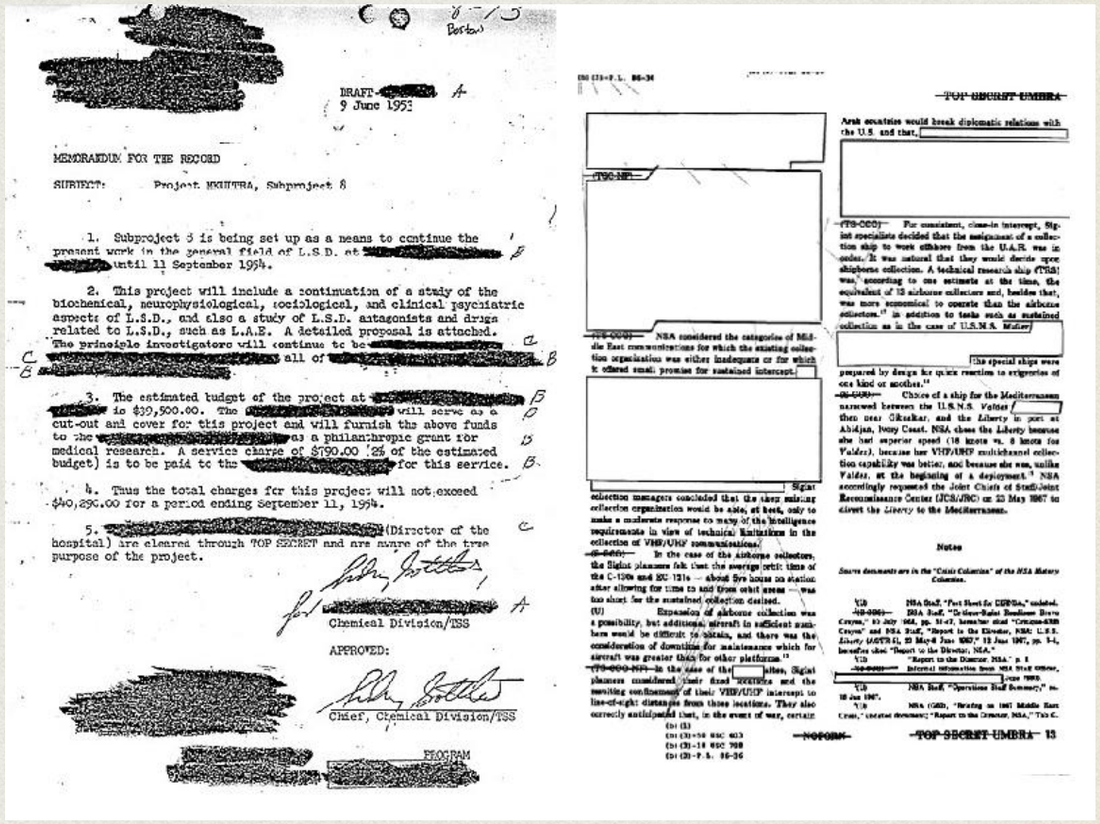
Erik S. Lesser for The New York Times

Thelma Arnold's identity was betrayed by AOL records of her Web searches, like ones for her dog, Dudley, who clearly has a problem.

AOL posted, but later removed, a list of the Web search inquiries of 658,000 unnamed users on a new Web site for academic researchers. An interview with one of those unnamed users, Thelma Arnold, combined with her data reveal what she was searching for, why and on which Web sites.

ASSAINISSEMENT DE DONNÉES ?

- (**Sanitization** en anglais)
- Accroitre **l'incertitude** dans les données
- **Compromis** entre le **niveau de protection** désiré et la qualité des données assainies (**utilité**)



DRAFT [redacted] 9 June 1955

MEMORANDUM FOR THE RECORD

SUBJECT: Project MKULTRA, Subproject 8

1. Subproject 8 is being set up as a means to continue the present work in the general field of L.S.D. at [redacted] until 11 September 1954.

2. This project will include a continuation of a study of the biochemical, neurophysiological, sociological, and clinical psychiatric aspects of L.S.D., and also a study of L.S.D. antagonists and drugs related to L.S.D., such as L.A.E. A detailed proposal is attached. The principle investigators will continue to be [redacted] all of [redacted]

3. The estimated budget of the project at [redacted] is $39,500.00. The [redacted] will serve as a cut-out and cover for this project and will furnish the above funds to the [redacted] as a philanthropic grant for medical research. A service charge of $790.00 (2% of the estimated budget) is to be paid to the [redacted] for this service.

4. Thus the total charges for this project will not exceed $40,290.00 for a period ending September 11, 1954.

5. [redacted] (Director of the hospital) are cleared through TOP SECRET and are aware of the true purpose of the project.

Chemical Division/TSS

APPROVED:

Chief, Chemical Division/TSS

PROGRAM

TOP SECRET UMBRA

Arab countries would break diplomatic relations with the U.S. and that, [redacted]

(TS-CCO) For consistent, close-in intercept, Signal specialists decided that the assignment of a collection ship to work offshore from the U.A.R. was in order. It was natural that they would decide upon shipborne collection. A technical research ship (TRS) was, according to one estimate at the time, the equivalent of 12 airborne collectors and, besides that, was more economical to operate than the airborne collectors.[17] In addition to tasks such as sustained collection as in the case of U.S.N.S. Valdez [redacted] the special ships were prepared by design for quick reaction to exigencies of one kind or another.[18]

(S-CCO) Choice of a ship for the Mediterranean narrowed between the U.S.N.S. Valdez [redacted] then near Gibraltar, and the Liberty in port at Abidjan, Ivory Coast. NSA chose the Liberty because she had superior speed (18 knots vs. 8 knots for Valdez), because her VHF/UHF multichannel collection capability was better, and because she was, unlike Valdez, at the beginning of a deployment.[19] NSA accordingly requested the Joint Chiefs of Staff/Joint Reconnaissance Center (JCS/JRC) on 23 May 1967 to divert the Liberty to the Mediterranean.

Notes

Source documents are in the "Crisis Collection" of the NSA History Collection.

[17] NSA Staff, "Fact Sheet for COPRA," undated.

(S-CCO) [18] NSA Staff, "Deliver-Relief Resilience Brave Crayon," 13 July 1967, pp. 16-17, hereafter cited "Crayon-RRR Brave Crayon" and NSA Staff, "Report to the Director, NSA; U.S.S. Liberty (AGTR-5), 23 May-8 June 1967," 12 June 1967, pp. 1-4, hereafter cited "Report to the Director, NSA."

[19] "Report to the Director, NSA," p. 2

(TS-CCO-NF) Informal information from NSA STAR Office, [redacted] June 1969.

[20] NSA Staff, "Operations Staff Summary," 16-18 June 1967.

[21] NSA (GSD), "Briefing on 1967 Middle East Crisis," undated document; "Report to the Director, NSA," Tab C.

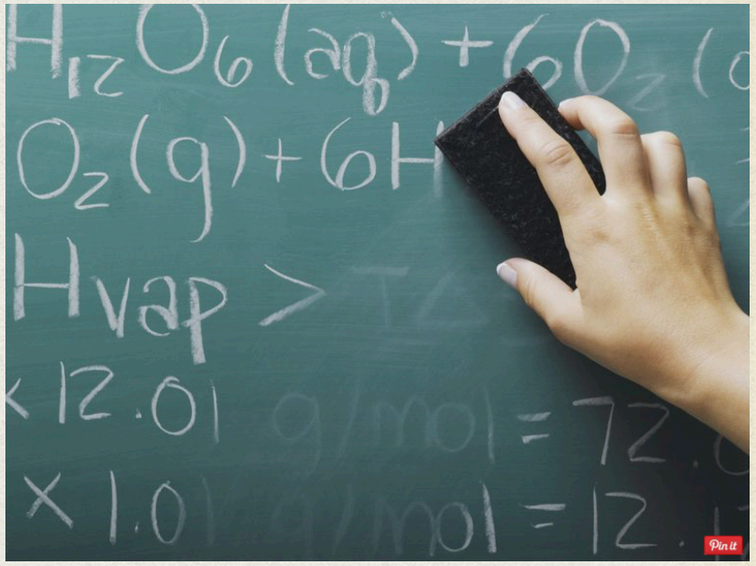
(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

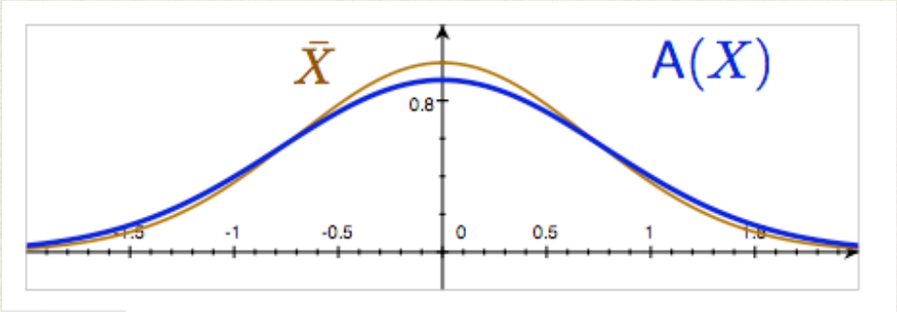
NOFORN

TOP SECRET UMBRA 13

ASSAINISSEMENT DE DONNÉES ?

- **Quantité** de données
  - échantillonnage
  - agrégation (temporelle, spatiale, multi-utilisateur, etc.)
- **Qualité** des données
  - Injection de bruit (Gaussien, Laplacien, uniforme) aux enregistrements
    - cacher les valeurs spécifiques mais conserver la distribution
  - Injection de faux enregistrements (*dummies*)





ASSAINIR JUSQU'À QUAND ?

- Compromis entre **protection** et **utilité**: nécessite d'évaluer chaque propriété
- Utilité : dépend du type des données et de leur utilisation future
- Protection : différents **modèles** de vie privée
  - k-anonymat : chaque individu est **indistinguable** parmi un groupe de *k*
  - Confidentialité différentielle (*Differential-privacy*) *:* il n'est (statistiquement) pas possible de déterminer si **un individu est présent** dans la BDD
  - attaques par inférences

ATTAQUES

- **Inférence**: l'adversaire essaye d'inférer de nouvelles connaissances à partir de
  - ensemble de données assainies
  - **données auxiliaires**
- **Chainage:** l'adversaire essaye de relier les enregistrements de 2 ensembles de données différents ayant des individus en commun
- **Défi**: donner des garanties de protection de la vie privée même contre un adversaire ayant des connaissances auxiliaires (qui peuvent être inconnues au départ)
  - Ex: libérer un jeu de données de mobilité dans la ville de Montréal

ATTAQUE PAR CHAINAGE DE SWEENEY

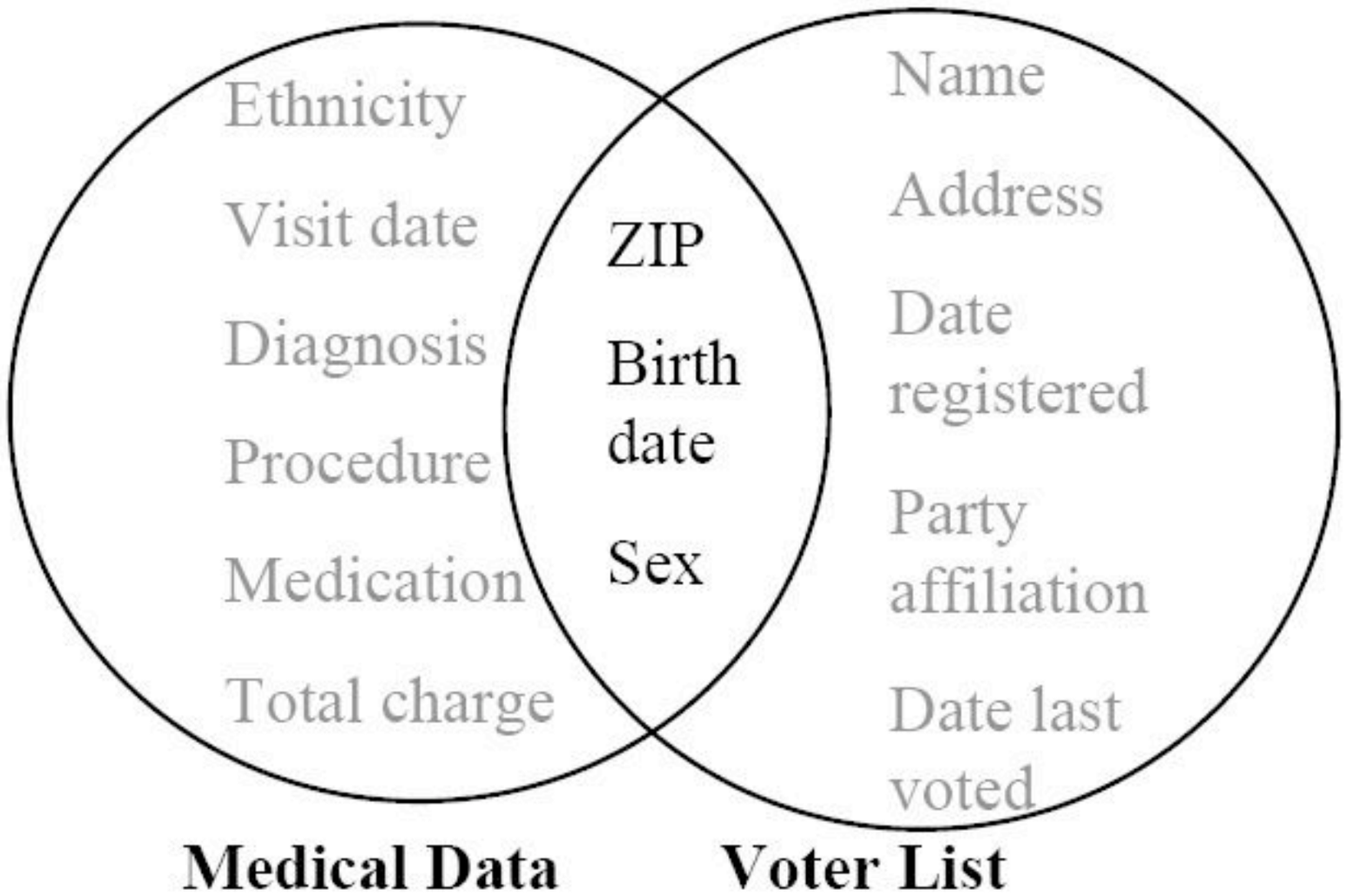


Figure 1 Linking to re-identify data

K-ANONYMAT - SWEENEY

- **Garantir** que dans chaque groupe de l'ensemble assaini, chaque individu est identique à au moins *k-1* autres
  - Généralisation et suppressions
  - Ex: données médicales

	Non-Sensitive			Sensitive
	Zip Code	Age	Nationality	Condition
1	13053	28	Russian	Heart Disease
2	13068	29	American	Heart Disease
3	13068	21	Japanese	Viral Infection
4	13053	23	American	Viral Infection
5	14853	50	Indian	Cancer
6	14853	55	Russian	Heart Disease
7	14850	47	American	Viral Infection
8	14850	49	American	Viral Infection
9	13053	31	American	Cancer
10	13053	37	Indian	Cancer
11	13068	36	Japanese	Cancer
12	13068	35	American	Cancer

Figure 1. Inpatient Microdata

	Non-Sensitive			Sensitive
	Zip Code	Age	Nationality	Condition
1	130**	< 30	*	Heart Disease
2	130**	< 30	*	Heart Disease
3	130**	< 30	*	Viral Infection
4	130**	< 30	*	Viral Infection
5	1485*	≥ 40	*	Cancer
6	1485*	≥ 40	*	Heart Disease
7	1485*	≥ 40	*	Viral Infection
8	1485*	≥ 40	*	Viral Infection
9	130**	3*	*	Cancer
10	130**	3*	*	Cancer
11	130**	3*	*	Cancer
12	130**	3*	*	Cancer

Figure 2. 4-anonymous Inpatient Microdata

ATTAQUE PAR COMPOSITION

- **Question:** le patron d'Alice sait quelle a 28 ans, qu'elle a pour code postal 13012 et qu'elle a visité deux hôpitaux. Que peut-il inférer ?

	Non-Sensitive			Sensitive
	Zip code	Age	Nationality	Condition
1	130**	<30	*	AIDS
2	130**	<30	*	Heart Disease
3	130**	<30	*	Viral Infection
4	130**	<30	*	Viral Infection
5	130**	≥40	*	Cancer
6	130**	≥40	*	Heart Disease
7	130**	≥40	*	Viral Infection
8	130**	≥40	*	Viral Infection
9	130**	3*	*	Cancer
10	130**	3*	*	Cancer
11	130**	3*	*	Cancer
12	130**	3*	*	Cancer

(a)

	Non-Sensitive			Sensitive
	Zip code	Age	Nationality	Condition
1	130**	<35	*	AIDS
2	130**	<35	*	Tuberculosis
3	130**	<35	*	Flu
4	130**	<35	*	Tuberculosis
5	130**	<35	*	Cancer
6	130**	<35	*	Cancer
7	130**	≥35	*	Cancer
8	130**	≥35	*	Cancer
9	130**	≥35	*	Cancer
10	130**	≥35	*	Tuberculosis
11	130**	≥35	*	Viral Infection
12	130**	≥35	*	Viral Infection

(b)

AUTRES MÉTRIQUES DE PROTECTION

- Le k-anonymat n'est pas forcément suffisant
- **l-diversité**: maintient de la diversité dans chaque groupe par rapport aux valeurs possibles des attributs sensibles
  - instantiation possible basée sur la mesure de **l'entropie**
  - protection contre les attaques basées sur l'homogénéité
- **t-proximité**: la distribution des attributs dans chaque groupe doit être proche de celle globale
  - *t* est un seuil à ne pas dépasser qui représente la proximité entre distributions

COMPÉTITION NETFLIX

- Challenge proposé de 2007 à 2009 par Netflix à la communauté d'apprentissage machine pour améliorer la précision de son système de recommandation de films
- Ensemble de données de 500k individus ayant noté 17k films, 100M notes (~20 film/individu) à une certaine date
  - <user,film,date,note>
- Pas d'identifiants (mais des *pseudonymes*)
- Peut sembler fournir un certain anonymat

COMPÉTITION NETFLIX

- Mais c'est sans compter sur les connaissances auxiliaires !
- Désanonymisation possible pour un nombre important d'enregistrements en utilisant .... IMDB !
  - grâce aux dates des notes
  - robuste à une erreur de 14j
- Et Netflix a arrêté cette compétition ...

seaview1

Send an IMDb private message to this author or view their message board profile.

Jump To: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Page 1 of 3: [1] [2] [3]

Expanded | Show all | Show summaries | **Alphabetical** | Chronological | Useful

1. 3:10 to Yuma (2007) 13 September 2007
2. A History of Violence (2005) 12 October 2005
3. An Education (2009) 5 March 2010
4. Angels & Demons (2009) 25 May 2009
5. A Serious Man (2009) 5 March 2010
6. Atonement (2007) 8 February 2008
7. Avatar (2009) 5 March 2010
8. AVP: Alien vs. Predator (2004) 12 August 2004
9. Babel (2006) 3 November 2006
10. Batman Begins (2005) 27 July 2005
11. Be Cool (2005) 3 March 2005
12. Beyond the Sea (2004) 22 December 2004
13. Blade: Trinity (2004) 2 December 2004
14. Bridget Jones: The Edge of Reason (2004) 4 November 2004
15. Broken Flowers (2005) 12 August 2005
16. Capitalism: A Love Story (2009) 14 November 2009
17. Charlie's Angels (2000) 4 November 2000
18. Christmas with the Kranks (2004) 23 November 2004
19. Cinderella Man (2005) 4 July 2005
20. Collateral (2004) 6 August 2004

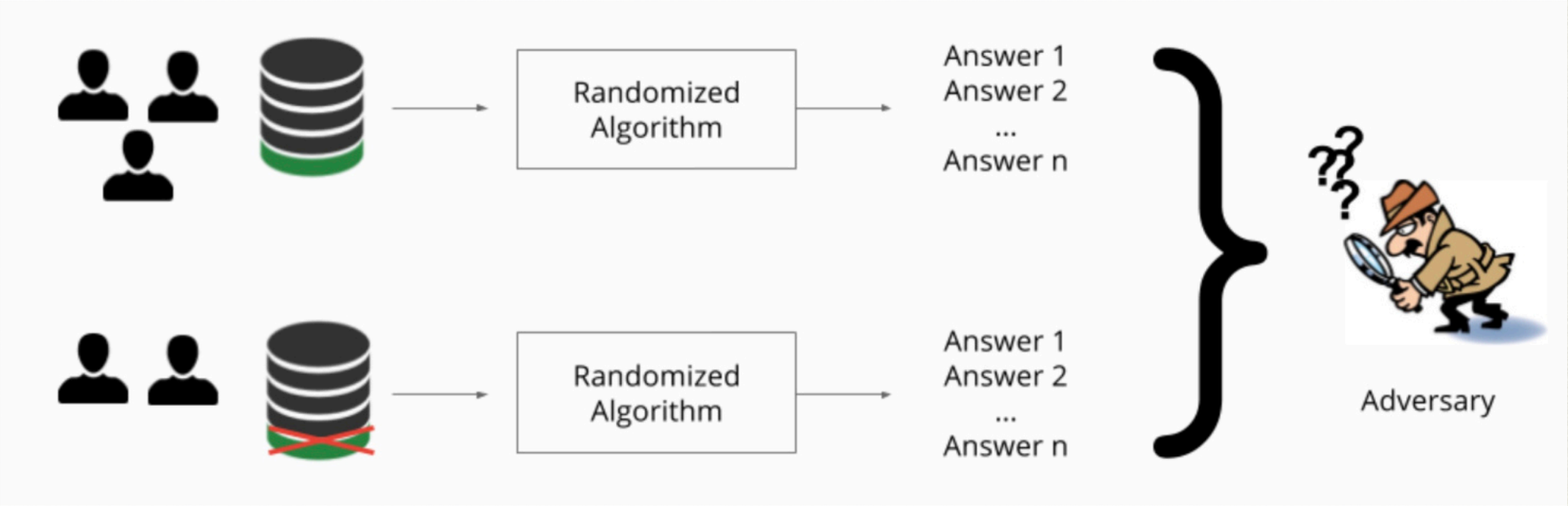
EN CONCLUSION

- Il est nécessaire d’assainir les données collectées
  - Minimisation des données
    = minimisation des risques
- Pseudonymiser n’est pas suffisant
- Compromis protection/utilité
- Attention aux données auxiliaires (et même à celles qui n’existent pas encore!)

CONFIDENTIALITÉ DIFFÉRENTIELLE

CD? DP?

- Confidentialité Différentielle (CD) - *Differential Privacy (DP)* [Cynthia Dwork 2006]
- Déf. informelle: l'**absence ou la présence** d'un individu dans une base de données n'**influence pas le résultat** des requêtes à cette base sauf **faible probabilité**
  - Sinon le résultat permet d'inférer la présence ou l'absence de l'individu
- Fortes garanties de VP. **Robuste aux connaissances auxiliaires**



Source

RÉPONSE RANDOMISÉE

- Techniques issue des sciences sociales pour collecter des statistiques sur des comportements embarrassants ou illégaux
  - Lancer une pièce
  - Si **pile**, répondre la **vérité**
  - Si **face**, lancer une autre pièce et répondre **OUI** pour **face** et **NON** pour **pile**

- **Utilité**: Permet la collecte de statistiques sur les participants ayant la propriété P (probabilité p) :
  OUI : 3/4 des individus qui ont P + 1/4 des individus qui n'ont pas P
  $|OUI| = \frac{1}{4}(1-p) + \frac{3}{4}p = \frac{1}{4} + \frac{p}{2}$
  On peut donc estimer p : $p = 2|OUI| - \frac{1}{2}$

- **PVP**: La randomisation permet le **déni plausible** car une réponse OUI (ou NON) peut provenir d'un lancé de pièce

DÉFINITION ET BUDGET

Définition 2.1. (Differential Privacy) Un mécanisme randomisé $\mathcal{A}$ satisfait la ϵ-differential pivacy (ϵ-DP) si pour toutes bases de données D_1 et D_2 différant seulement d'un individu et pour n'importe quelle sortie $O \in Im(\mathcal{A})$, la propriété suivante est respectée :

$$Pr[\mathcal{A}(D_1) = O] \leq e^{\epsilon} \times Pr[\mathcal{A}(D_2) = O]$$

- ϵ : budget qui quantifie le niveau de protection du mécanisme

  ϵ petit (proche de 0), garantie forte

  ϵ grand, garantie faible (mais distorsion faible)

- **Comment fixer ϵ ?**

Documents de référence : The Algorithmic Foundations of Differential Privacy - Dwork & Roth 2014
Differential Privacy: A Survey of Results - Dwork 2008

SENSIBILITÉ D'UNE FONCTION

Définition 2.2. (Sensibilité Globale) Pour toutes fonctions $f : D \to \mathbb{R}^d$, sa sensibilité notée Δf est définie par :

$$\Delta f : max_{D_1,D_2}||f(D_1) - f(D_2)||$$

pour tout D_1, D_2 deux bases de données différant par un seul individu.

- Δf : la sensibilité de la fonction f
  - paramètre très important qui mesure la contribution maximale d'un individu dans la base de données
  - En général, peut être difficile à calculer, voire à estimer mais cas simples comme les comptes:
    - f=nombre de chauves dans une BDD Δf=1
    - f=nombre de chauves arrondi à un multiple de 5 Δf=5

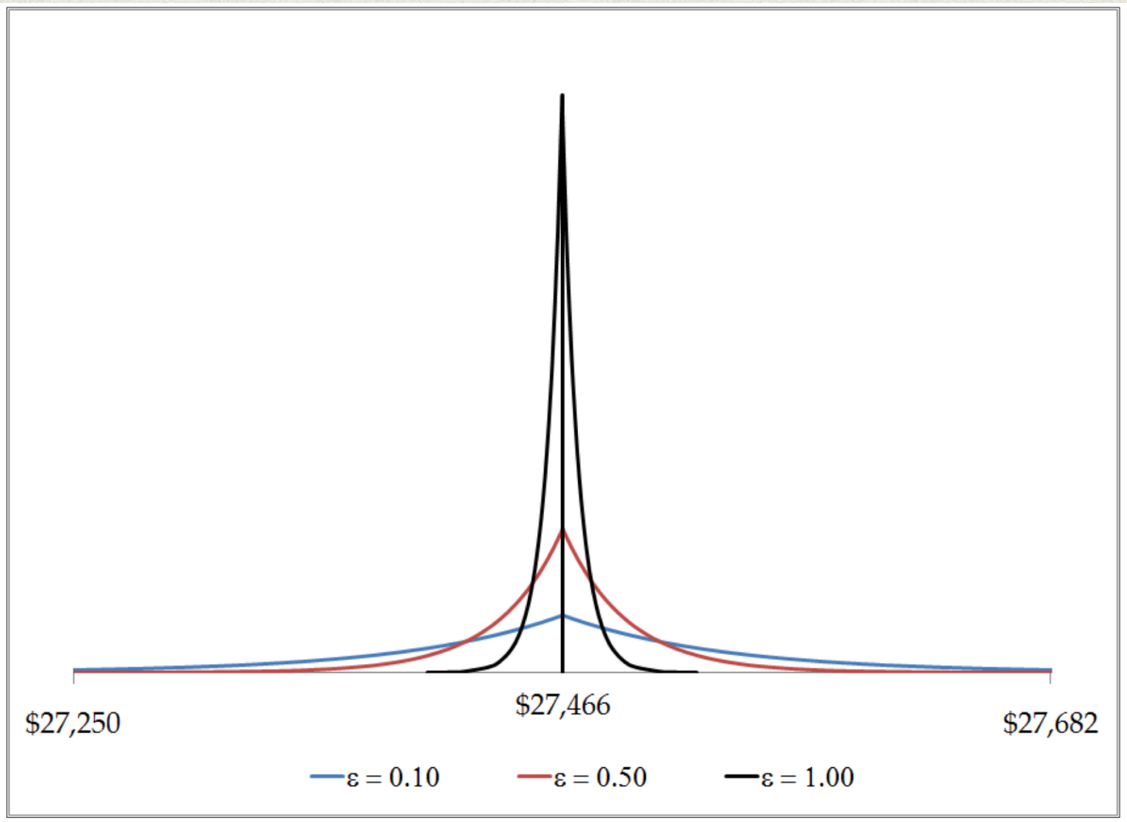
MÉCANISME LAPLACIEN

Définition 2.3. (Mécanisme Laplacien) Pour toutes fonctions $f : D \to \mathbb{R}^d$, le mécanisme $\mathcal{A}$

$$\mathcal{A}(D) = f(D) + (\mathcal{L}_1(\lambda), \ldots, \mathcal{L}_k(\lambda))$$

est ϵ-DP si $\mathcal{L}_i(\lambda)$ sont des variables aléatoires indépendantes tirées de la distribution Laplacienne de paramètre $\lambda = \frac{\Delta f}{\epsilon}$

- Pour une fonction f avec k termes
  - Si k=1 : $\mathscr{A}(D) = f(D) + Lap(\frac{\Delta f}{\epsilon})$
- $\epsilon \to 0 \Rightarrow Lap(\frac{\Delta f}{\epsilon})$ plus « plat »
  - bruit plus large
- Bien adapté aux « comptes »



COMPOSITION

Théorème 2.1. (Fermeture sous post-traitement) Soit $\mathcal{A}$ ϵ-DP et soit $f : \mathcal{R} \to \mathcal{R}$ une fonction arbitraire, indépendante de D. Alors $f \circ \mathcal{A} : D \to \mathcal{R}$ est ϵ-DP.

Théorème 2.2. (Composition séquentielle) Soient $\mathcal{A}_i$ chacun garantissant la ϵ_i-DP. Une séquence de $\mathcal{A}_i(D)$ sur une base de données D est $(\sum_i \epsilon_i)$-DP.

Théorème 2.3. (Composition parallèle) Soient $\mathcal{A}_i$ chacun garantissant la ϵ_i-DP. Une séquence de $\mathcal{A}_i(D_i)$ sur des bases de données disjointes D_i est $(max(\epsilon_i))$-DP.

Documents de référence : The Algorithmic Foundations of Differential Privacy - Dwork & Roth 2014
Differential Privacy: A Survey of Results - Dwork 2008

COMPOSITION 2

- Les propriétés de composition sont ce pourquoi la DP est devenue un standard *de facto*
  - On peut prouver qu'un algorithme est DP
  - Th2.1 : n'importe quelle fonction appliquée à un mécanisme DP est DP; i.e. on peut publier des données DP sans se soucier des futures analyses à l'inverse du k-anonymat (cf. Capsule prec.)
  - Th2.2 : on peut « découper » ϵ à différentes requêtes séquentielles
  - Th2.3 : on peut borner ϵ lors d'appels à des mécanismes disjoints

LA DP DANS LE MONDE RÉEL

- US Census bureau - résultat des recensements 2020
- Google - outil RAPPOR pour Chrome
- Apple - Statistiques d’usage des macs/iPhones
- Facebook - fourniture de sonnées pour les sciences sociales
- Uber/Amazon/Mozilla/Snapchat
- cont.