FICHE : LISTE DE RESSOURCES SUR LA PROTECTION DE LA VIE PRIVÉE

> **« Abandonner sa vie privée parce qu'on n'a rien à cacher c'est comme abandonner sa liberté d'expression parce qu'on n'a rien à dire. » Edward Snowden**

Introduction

Nos données personnelles sont collectées et partagées de façon massive. Nos ordinateurs et autres objets connectés génèrent des mégadonnées (big data) qui vendues et analysées par des algorithmes. Les analyses servent à nous cibler individuellement pour nous proposer des produits et des services, mais aussi à nous influencer. La vidéo ci-dessous présente le cas de Cambridge Analytica qui n'est qu'une compagnie parmi des milliers qui font parler nos données personnelles.

Nos données sont transmises de trois façons :

- Transmission active : partage sur les réseaux sociaux, formulaires, commentaires, articles, etc.
- Transmission passive : navigation web, app, Internet des objets, etc.
- Transmission non désirée : hacking, bug, **doxxing**, **sexting**, etc.

Transmission active

La transmission active concerne les données que vous choisissez de partager sur une base volontaire en ligne, en téléchargeant des documents, en remplissant un formulaire, en ajoutant des commentaires, en partageant sur les réseaux sociaux, etc.

Transmission passive

La transmission passive se produit à votre insu mais avec votre accord parce que vous acceptez les termes et conditions ainsi que les politiques de confidentialité. C'est l'objet principal de cette page.

Traquer notre localisation

La plupart de nos appareils collectent et partagent nos données de géolocalisation.

Exemples

- **Digital Billboards Are Tracking You. And They Really, Really Want You to See Their Ads**, Consumer Report, 20 novembre 2019.
- **Your Apps Know Where you Were Last Night, and They're Not Keeping It Secret**, *New York Times*, 10 décembre 2018.

Comment s'en protéger?

- Choisissez bien vos fournisseurs de produits et services, certains respectent davantage votre vie privée.
- Configurez vos appareils pour limiter le traçage. Ex : **How to Stop Apps Tracking Your Location**, *New York Times*, 10 décembre 2018.

- Acheter des **cages de faraday** pour vos clés de voiture, votre passeport, votre ordinateur, votre téléphone, vos cartes bancaires. Ex : **Silent Pocket**

Test

Sur votre iPhone suivez le chemin suivant pour voir quels sont les lieux importants qu'Apple a enregistrés sur vous : *Réglages->Confidentialité->Service de localisation->Services Système->Lieux importants*

Sur vos téléphones Android allez voir : **https://myactivity.google.com/**

Traquer le contenu de nos courriels

Nombreuses sont les compagnies qui lisent nos courriels pour ensuite nous recommander des produits ou des services.

Exemples

- **Google Says It Continues to Allow Apps to Scan Data From Gmail Accounts**, *The Wall Street Journal*, 20 septembre 2018.

Extrait (traduction libre) : « Google Inc. a déclaré aux législateurs qu'elle continue de permettre à d'autres entreprises de scanner et de partager les données des comptes Gmail, en répondant aux questions soulevées au Capitole sur la confidentialité et l'utilisation abusive potentielle des informations contenues dans les courriels des utilisateurs. »

Comment s'en protéger?

- Utilisez un service courriel qui respecte votre vie privée - Ex : **Pronton Mail**

Traquer ce que vous visionnez sur votre téléviseur et les appareils connectés dans votre habitation

Les compagnies identifient ce que vous regardez et quels sont les appareils connectés à votre domicile pour vous envoyer des publicités ciblées.

Exemples

- **How Smart TVs in Millions of U.S. Homes Track More Than What's On Tonight**, *New York Times*, 5 juillet 2018.

Extrait (traduction libre) : « Ces dernières années, les sociétés de données ont exploité les nouvelles technologies pour identifier immédiatement ce que les gens regardent sur les téléviseurs connectés à Internet, puis utiliser cette information pour envoyer des publicités ciblées à d'autres appareils dans leurs foyers. **...** Une fois activée, Samba TV peut suivre presque tout ce qui apparaît sur le téléviseur sur une base seconde par seconde, essentiellement la lecture des pixels pour identifier les émissions réseau et les publicités, ainsi que les programmes sur Netflix et HBO et même les jeux vidéo joués sur la télévision. »

Comment s'en protéger?

- Déconnectez votre téléviseur de l'Internet si vous n'utilisez pas le streaming.
- N'acceptez pas de partager vos données lors de la configuration de votre téléviseur (ex: ne pas activer Samba TV). Pour allez plus loin lisez : **How to Stop Your Smart TV From Tracking What You Watch**.
- Choisissez un produit qui respecte votre vie privée.

Traquer les données de jeu de vos enfants

Des chercheurs ont montré que plus de la moitié des applications Android gratuites partagent des données avec des sociétés tierces à l'encontre de la loi.

Exemples

- **How Game Apps That Captivate Kids Have Been Collecting Their Data**, *New York Times*, 12 septembre 2018.
- **FBI Warns Parents of Privacy Risks With Internet-Connected Toys**, *NBC News*, 18 juillet 2017.

Comment s'en protéger?

- Choisissez bien les jeux de vos enfants. Si possible lisez les termes et conditions.
- Méfiez-vous des jeux gratuits, souvent le modèle d'affaires consiste à vendre les données.

Traquer vos applications

Nombreuses sont les compagnies qui traquent la façon dont nous utilisons nos applications et appareils. Le but avoué est d'améliorer la sécurité ce qui peut être le cas, mais souvent ces données peuvent avoir d'autres fins.

Exemples

- **No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data**Privacy International, 9 septembre 2019.
- **Banks and Retailers Are Tracking How You Type, Swipe and Tap**, *New York Times*, 13 avril 2018.

Extrait (traduction libre) : « La façon dont vous appuyez, faites défiler et tapez sur l'écran ou le clavier d'un téléphone peut être aussi unique que vos empreintes digitales ou les caractéristiques de votre visage. Pour lutter contre la fraude, un nombre croissant de banques et de commerçants suivent les mouvements physiques des visiteurs lorsqu'ils utilisent les sites Web et les applications. **...** Les traits comportementaux peuvent être capturés en arrière-plan, sans que les clients ne fassent quoi que ce soit pour s'inscrire. »

Comment s'en protéger?

- Lisez les termes et conditions.
- Limitez les applications que vous téléchargez. Il est très difficile de se protéger totalement de ce type de traçage.

Traquer votre visage

Les gouvernements et les compagnies traquent nos visages et nos déplacements. Pour ce faire, les flux collectés par les caméras de surveillance sont analysés par des algorithmes de reconnaissance faciale et de reconnaissance d'affects. On cherche avec les affects à trouver ce que signifie la forme de votre nez, votre façon de sourire ou tout autres traits. Ces pratiques ne sont pas sans rappeler la **phrénologie** à la mode au 19e siècle.

Exemples

- **BArtificial Intelligence Experts Issue Urgent Warning Against Facial Scanning With A "Dangerous History"**, *The Intercept*, 6 décembre 2018.
- **AI Now 2018** (Rapport .PDF)
- **IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color**, *The Intercept*, 6 septembre 2018.
- **New facial recognition tool tracks targets across different social networks**, *The Verge*, 8 août 2018.
- **Facial recognition technology: The need for public regulation and corporate responsibility**, Blog Microsoft, 13 juillet 2018

Comment s'en protéger?

Il est très difficile de se protéger de ce type de traçage. Quelques possibilités émergent ci-dessous. Toutefois il serait préférable de limiter l'usage de ce type de technologies et de les règlementer.

- **Camouflage from face detection.**

Traquer votre ADN

Des compagnies privées offrent des tests de séquençage génétique liées à différents services. Ces tests sont de moins en moins chers mais impliquent souvent la vente de vos données à des tiers. Des gouvernements accumulent aussi de plus en plus de données génétiques à des fins discutables.

Exemples

- **China Uses DNA to Map Faces, With Help From the West**, *The New York Times*, 3 décembre 2019.

Comment s'en protéger?

Ne faites pas de test génétique sans des garanties de confidentialité et si le test est absolument nécessaire.

Traquer vos habitudes par ultrasons

Des compagnies développent des applications qui communiquent entre elles par ultrasons à votre insu (mais vous avez accepté les termes et conditions). Votre téléviseur peut ainsi parler à d'autres appareils dans votre maison.

Exemples

- **Twenty Thousand Hertz - Ultrasonic Tracking** (podcast)

Comment s'en protéger?

- Configurez vos applications afin qu'elles ne puissent pas utiliser les micros de vos appareils.
- Lisez les termes et conditions.

Traquer votre navigation Web

De nombreux sites web et compagnies traquent les pages web que vous visitez à l'aide de cookies, de cookies tiers, de pixels, de technologies d'empreinte (fingerprinting), etc.

Exemples

- **Health websites are sharing sensitive medical data with Google, Facebook, and Amazon**, MIT Technology Review, 13 novembre 2019.
- **Facebook and Google Trackers Are Showing Up on Porn Sites**, *New York Times*, 17 juillet 2019.
- **Your Porn Is Watching You**, *Motherboard*, 6 avril 2015.
- **Pornhub Insight 2018 Year in Review**

Comment s'en protéger?

- Utilisez un VPN (attention de ne pas vous faire traquer par votre VPN. Choisissez un bon service payant ex: **Proton VPN**)
- Utilisez un navigateur qui respecte votre vie privée
- Configurez les paramètres de confidentialité de votre navigateur
- Installez des bloqueurs de traqueurs (attention de ne pas vous faire traquer par votre bloqueur...)

Test

Testez le niveau de protection contre le traçage de votre navigateur avec **Panopticlick**

Traquer vos objets connectés

Un nombre croissant d'objets sont aujourd'hui connectés à Internet. C'est objets s'apparentent souvent plus à des ordinateurs qu'à des objets traditionnels. Votre voiture connectée est un ordinateur sur roues, votre téléphone est un ordinateur qui permet de passer des appels téléphoniques, etc.

Exemples

- **The Internet of Dildos is Watching You**, *Motherboard*, 6 avril 2016.
- **Medtronic disables pacemaker programmer updates over hack concern**, *Reuters*, 11 octobre 2018.
- **Strava’s privacy PR nightmare shows why you can’t trust social fitness apps to protect your data**, MIT Technology Review, 29 janvier 2018.

Comment s'en protéger?

- Limitez le nombre d'objets connectés. Des objets connectés défaillants peuvent avoir des conséquences sur votre intégrité physique. Lire : **For safety's sake, we must slow innovation in internet-connected things**, MIT Technology Review, 6 septembre 2018.
- Configurez et mettez à jour vos objets connectés.

Traquer votre départ

Les fournisseurs d'applications ont développé des mécanismes de traçage qui vous suivent même lorsque vous désinstallez une application.

Exemples

- **Now Apps Can Track You Even After You Uninstall Them**, *Bloomberg*, 22 octobre 2018.

Extrait : « Les entreprises qui s'adressent aux fabricants d'applications ont trouvé des moyens de jouer à la fois à iOS et à Android, ce qui leur permet de savoir quels utilisateurs ont désinstallé un logiciel donné récemment - et facilite l'affichage d'annonces visant à les reconquérir. »

Comment s'en protéger?

- Mettez à jour vos systèmes. Ce type de traqueurs violent les termes et conditions de Google et d'Apple, ces derniers devraient agir en conséquence.

Traquer votre absence

Des compagnies comme Facebook vous traquent même si vous n'avez pas de compte chez eux. Ainsi le jour où vous ouvrez un compte ils ont déjà beaucoup de données sur vous. On appelle cela les *shadow profils*.

Exemples

- **Shadow profiles are the biggest flaw in Facebook's privacy defense**, Gizmodo, 11 avril 2018.

Comment s'en protéger?

- Protégez votre navigation (VPN, etc.)
- Encryptez vos données.

Ces compagnies et gouvernements qui traquent votre vie

Lorsque l'on cumule les technologies de traçage, on arrive à des réalités qui dépassent les dystopies les plus pessimistes.

- **What 7 Creepy Patents Reveal About Facebook**, *New York Times*, 21 juin 2018.
- **People You May Know**, *Gizmodo*, collection d'articles.
- **Who needs democracy when you have data?**, *MIT Technology Review*, 20 août 2018.

- **Leave no dark corner**, *ABC News* 17 septembre 2018.

Transmission non désirée

Vente de vos données sur le Dark Web après qu'une base de données ait été hackée.

Exemples

- **Les tendances sur le piratage des données médicales dans le Dark Web**, *Info High Tech*19 juillet 2018.

Extrait : « Les PHI sont généralement vendus en paquets que les cybercriminels appellent «fullz». Les Fullz sont des enregistrements de renseignements personnels structurés qui peuvent ensuite être utilisés pour divers types de fraude et d'extorsion tels que la fraude bancaire et de crédit, la fraude en matière de santé, le vol d'identité et l'extorsion de rançon. »

Comment s'en protéger?

- N'utilisez jamais deux fois le même mot de passe.
- Utilisez un gestionnaire de mots de passe.
- Activez la double authentification.
- Encryptez vos données (communications et disques durs)

Test

Vérifiez si vos courriels ont fait l'objet d'un hack. Si oui, il y a de fortes chances que votre courriel et votre mot de passe soient disponibles sur le Dark Web. Il est donc important de changer votre mot de passe.

- Allez sur **Have I Been Pwned** pour vérifier vos adresses courriels corrompus.
- Allez sur **We Leak Info** pour vérifier vos adresses courriels, numéros de téléphone, mots de passe, noms, adresses IP, hashs qui ont été corrompus (Service payant).

Doxxing

Bug

Les bugs sont fréquents dans tous les logiciels et systèmes d'exploitation.

Juice Jacking

Le **juice jacking** consiste à vous soutirer vos données lorsque vous rechargez vos appareils à une borne de rechargement publique. Au lieu d'uniquement faire circuler de l'électricité dans le câble de chargement, vos données sont également aspiré.

Comment s'en protéger?

- Évitez de recharger vos appareils sur des bornes de chargement publiques ou dont vous n'êtes pas certain de la sécurité.
- Utilisez un batterie de rechargement portative.
- Si vous devez absolument utiliser une borne de chargement publique, munissez vous d'un adaptateur USB qui bloquent le transfert de données entre votre appareil et la borne.

Conclusion

Posez vous ces questions de bases pour limiter votre exposition :

- Avez-vous besoin de partager cette information en ligne?
- Avez-vous besoin de cette technologie ? - Limitez vos produits et services au minimum cela réduit l'exposition de vos données et réduit votre surface d'attaque et le partage de vos données.
    - Avez-vous besoin de cet objet connecté (traqueur, montre, cafetière, voiture, téléviseur, brosse à dents...)?
    - Avez-vous besoin de cette application ou ce logiciel?
- Quel est le modèle d'affaires ? - Les solutions gratuites ont en général pour modèle la vente de vos données à des tiers. Faites également attention aux solutions qui prétendent vous protéger et font l'inverse (Ex : **How Free VPNs Sell Your Data**)
- Qui développe le produit ou service ? - Vérifiez la crédibilité de vos fournisseurs.
- Quels sont les termes et conditions ? - Lisez-les au moins en ce qui concerne le partage de données.
- Qu'elles sont les politiques de confidentialité? - Lisez-les au moins en ce qui concerne le partage de données.
    - Où sont stockées les données ?
    - Combien de temps sont stockées les données ?
    - Qui a accès aux données ?
    - Qui va extraire des renseignements de vos données?

Synthèse des bonnes pratiques pour tous :

- Configurez correctement vos appareils.
- Sauvegardez vos données - En cas de vol, de bris, ou autres, vous ne perdrez rien.
- Utilisez des applications qui respectent votre vie privée et sont approuvées par votre organisation - Certaines applications sont conçues pour respecter votre vie privée.
    - Navigateurs mobiles exemples : **Brave** ; **DuckDuckGo** ; **Firefox**.
    - Limitez les publicités ciblées sur vos mobiles en désactivant voir cet **article**.
    - Navigateurs PC/Mac : **Brave** ; **Firefox** ; **Tor**
    - Désinstallez toute application douteuse.
- Utilisez un **gestionnaire de mots de passe** - Un gestionnaire génère des mots de passe longs et compliqués et les retient à votre place.
- Utilisez des alias - Ne donnez pas systématiquement vos "vraies" coordonnées.
- Utilisez des courriels temporaires. Ex : **10 Minute Mail**

- Encryptez vos données (communications et disques durs) - En cas de vol ou de hack, les données sont illisibles. Ex : **File Vault** sur Mac OS.
- Ne cliquez sur aucun lien suspect, si vous n'êtes pas certain au lieu de suivre le lien, allez directement sur le site de l'institution.
- Réfléchissez deux fois avant de publier en ligne.
- Limitez votre usage de Google, Facebook et autres services qui vendent vos données.
- Ne faites pas confiance à vos objets connectés.
- Désactivez le Wi-Fi et le Bluetooth lorsque non utilisés et utilisez un VPN sur des réseaux publics.
- Faites régulièrement les mises à jour de tout vos appareils connectés.

Synthèse des bonnes pratiques pour une protection plus avancée :

- Bloquez les **publicités** et les traqueurs avec des extensions fiables
- Utilisez la **double authentification** pour vos comptes les plus importants.
- Utilisez un VPN fiable exemples : **ProtonVPN**.
- Utilisez le navigateur **Tor** - Tor vous permet de masquer votre adresse IP
- Utilisez des **cages de faraday** pour vos appareils, clés, passeport, cartes de crédit, ordinateurs, etc.
- Faites de l'**OSINT** sur vous même - En cherchant des renseignements de sources ouvertes sur vous même, vous verrez à quel point vos données sont exposées.