Vie privée et Neutralité du Net

Schleithal – 21 septembre 2016

Qu'est ce que la vie privée ?

Tout ce qui n'est pas publié (rendu public)

Des éléments de vie privée

Coordonnées d'une personne
(nom, prénom, adresse…)

Données personnelles
(age, sexe, n° sécu…)

Convictions politiques et croyances religieuses

Faits et geste d'une personne
(discours, localisation…)

Métadonnées générées par les usages
(quel contact, quand, combien de temps, combien de fois, horodatage…)

Contenu des communications

Qu’appel t-on la Neutralité du Net (netneut) ?

« La neutralité du Net ou la neutralité du réseau est un principe devant garantir l'égalité de traitement de tous les flux de données sur Internet. Ce principe exclut par exemple toute discrimination à l'égard de la source, de la destination ou du contenu de l'information transmise sur le réseau. »

Wikipedia

En quoi la Netneut et la vie privée sont-elles menacées ?

Boites noires

Inspection de paquets par les FAI (DPI)

Offres «illimités»

Lois liberticides

Surveillance de masse

GAFAM

Logiciels espions

Scripts espions

Web neutre → applications

Internet tel que...

ses fondateurs l'ont voulu

- Décentralisé
- Neutre et Libre
- Outils d'émancipation et de savoir
- Le politique n'a aucun pouvoir

qu'il existe

- Centralisé
- Au mains des GAFAM
- Outil de contrôle des masses
- Contrôlé de plus en plus par les États

Comment défendre la netneut ?

Difficile à faire car ça dépend beaucoup de l'opérateur

Parler de la netneut autour de soi
Soutenir les règlements européens pour la netneut
Ne pas utiliser les services «illimités»
Souscrire à un FAI qui ne pratique pas le DPI

Atteinte à la vie privée

Délit réprimant celui qui, sans le consentement d'une personne, capte, enregistre ou transmet les paroles qu'elle a prononcées à titre privé ou confidentiel ou fixe, enregistre ou transmet son image alors qu'elle était dans un lieu privé. (Constituent également une atteinte à la vie privée la falsification, l'importation, la détention, l'exposition, l'offre, la location ou la vente sans autorisation d'appareils permettant la détection à distance de conversations ou l'interception de télécommunications.)

Larousse

Rien à cacher ?

Donneriez vous vos identifiants et mot de passe de compte à un inconnu ?

Mettriez vous une camera dans votre chambre ? Un microphone ?

Les lois et les personnes au pouvoir peuvent changer

Un pirate peut se servir des failles

Rien à cacher ? - http://jenairienacacher.fr/

Je n'ai rien à cacher. En fait si, et vous également !

👉 Puis-je vous demander une copie de tous vos emails, de vos messages et photos sur Facebook, et de tous les fichiers sur votre ordinateur ? J'aimerais tout savoir sur votre vie privée.

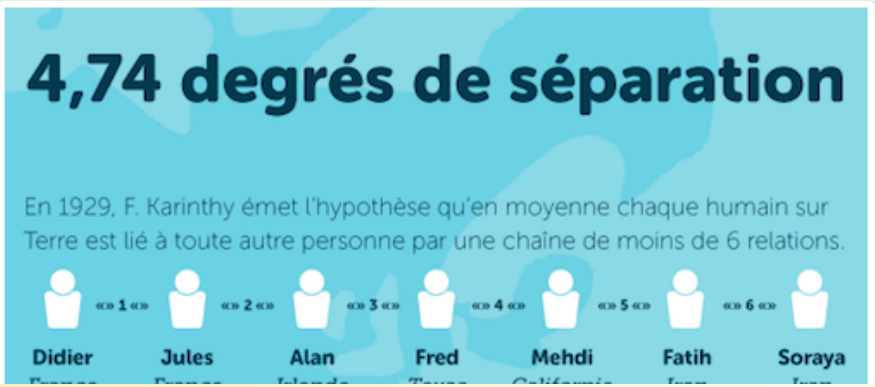
Comment oseriez-vous répondre *non* ? Lorsque vous n'avez rien à cacher, vous ne pouvez pas faire de **distinction** entre ce que vous admettez rendre public et ce qui vous dérange un peu plus. Dès lors que vous imposez une **barrière**, vous avez quelque chose à cacher (et c'est bien normal !).

Nous autres, êtres humains, nous distinguons les uns des autres parce que nous avons tous une **vie privée**, une **intimité** que nous ne dévoilons pas à tout bout de champ.

👉 Si vous ne le faites pas pour vous, faites-le pour moi !

surveillance Depuis des années, les agences gouvernementales et autres services secrets s'affairent à créer des **graphes sociaux**, représentants les **liens entre individus**. En effet, une personne peut devenir *intéressante* du jour au lendemain, que ce soit parce qu'elle devient célèbre, nuisible ou simplement parce que ses opinions (politiques, religieuses) ne sont plus en phase avec le gouvernement en place.

Lorsqu'une personne est placée sous "surveillance", son entourage l'est également, ce qui se traduit par une



Chiffrement et logiciel libre

Logiciels libres = code source disponible et modifiable = confiance

Dès que possible, c'est le logiciel libre qui est privilégié.
Mais MACOS, Windows et Android posent le souci de ne pas être des systèmes libres, donc on ne peut pas leur faire confiance.
Windows et MACOS sont plus que fortement déconseillés dans le contexte de la confiance et de la cryptographie.

Faire de la crypto là-dessus, c'est un peu comme avoir une porte blindée à sa maison, mais avec des murs en carton-pâte.

Genma

Faire de la cryptographie sur des OS privateurs ?

Oui on peut utiliser des outils cryptographiques sur MS Windows et Apple Mac OS. Mais alors on part immédiatement avec un déficit.

Ces systèmes vous espionnent et chiffrer ses données n'y changent rien. Les données privées sont interceptées avant d'être chiffrées.

Modèle de menace

Il est impossible de se protéger contre toutes les menaces

Il faut se concentrer sur les attaques les plus probables contre ses données numériques les plus vitales

Élaborer un ensemble d'attaques possibles contre lesquelles vous envisagez de vous protéger se dénomme modèle de menace.

Définition de l'EFF

Modèle de menace

Le modèle de menaces peut être représenté sous forme de diagramme en trois sections :

- les données que vous voulez protéger
- les menaces extérieurs
- les moyens pour protégez vos données

Exemple de modèle de menace

Citoyen soucieux de défendre sa vie privée

Protéger sa navigation

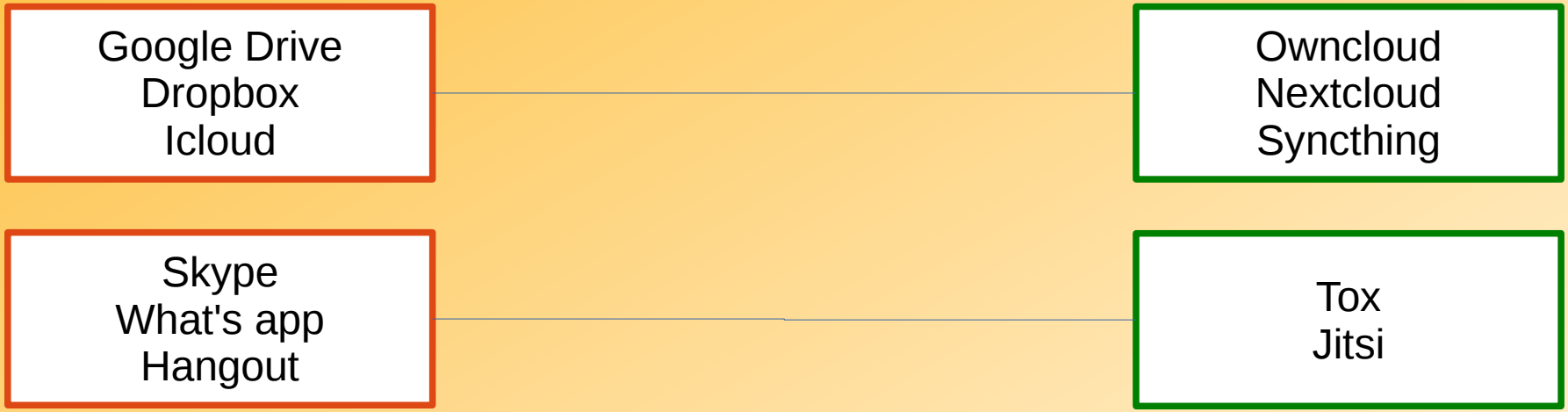
Surfer sur le web avec Mozilla Firefox
(navigateur libre développé par une fondation à but non lucratif)

Avec des extensions protectrices :

- Ublock Origin (bloqueur de pub et de traqueurs)
- Ssleuth (audit de sécurité des sites web)
- httpseverywhere (forcer les communications sécurisées)

Des alternatives aux GAFAM

Tous les services des GAFAM ont une alternative



Pour une liste complète : https://prism-break.org/fr/

Protéger ses fichiers

Utiliser un OS sécurisé
(GNU/Linux)

Chiffrer ses fichiers sensibles ou non
(veracrypt, LUKS)

Sécuriser sa machine
(faire les mises à jours, installer depuis des sources sûres)

Faire le lien entre son usage et son modèle de menaces

Échanger de façon chiffrée

Utiliser des logiciels libres de messagerie

Sur PC : Tox, Jitsi, Ring, Thunderbird+Enigmail…

Sur Android : Antox, Silence...

Comment protéger sa vie privée dans les environnements numériques ?

Avoir un modèle de menaces cohérent

Gérer son identité numérique (cloisonnement)

Se détacher des GAFAM

Utiliser les services et logiciels libres sans «cloud»

Faire ses mise à jour

Utiliser des logiciels libres de chiffrement

Participer à des chiffrofêtes

Faire de la veille numérique pour monter en compétence

Merci de votre attention !