Mieux protéger sa vie privée sur le net
CryptoParty Chiroux, 25/04

Table des matières

- Contexte
  - Prism ? Xkeyscore ?
  - Situation en Belgique
- Premiers réflexes
- Solutions logicielles
- Solutions internet
- Liens et contacts

Le contexte

Pourquoi se protéger ?

- L'actualité récente a démontré qu'il devient impératif de protéger ses données et outils informatiques, car notre vie privée est constamment mise à mal sur internet.

- Nous n'avons peut être rien à cacher, mais la vie privée est un droit inaliénable concédé par la charte des droits de l'homme.

Comment le scandale est arrivé

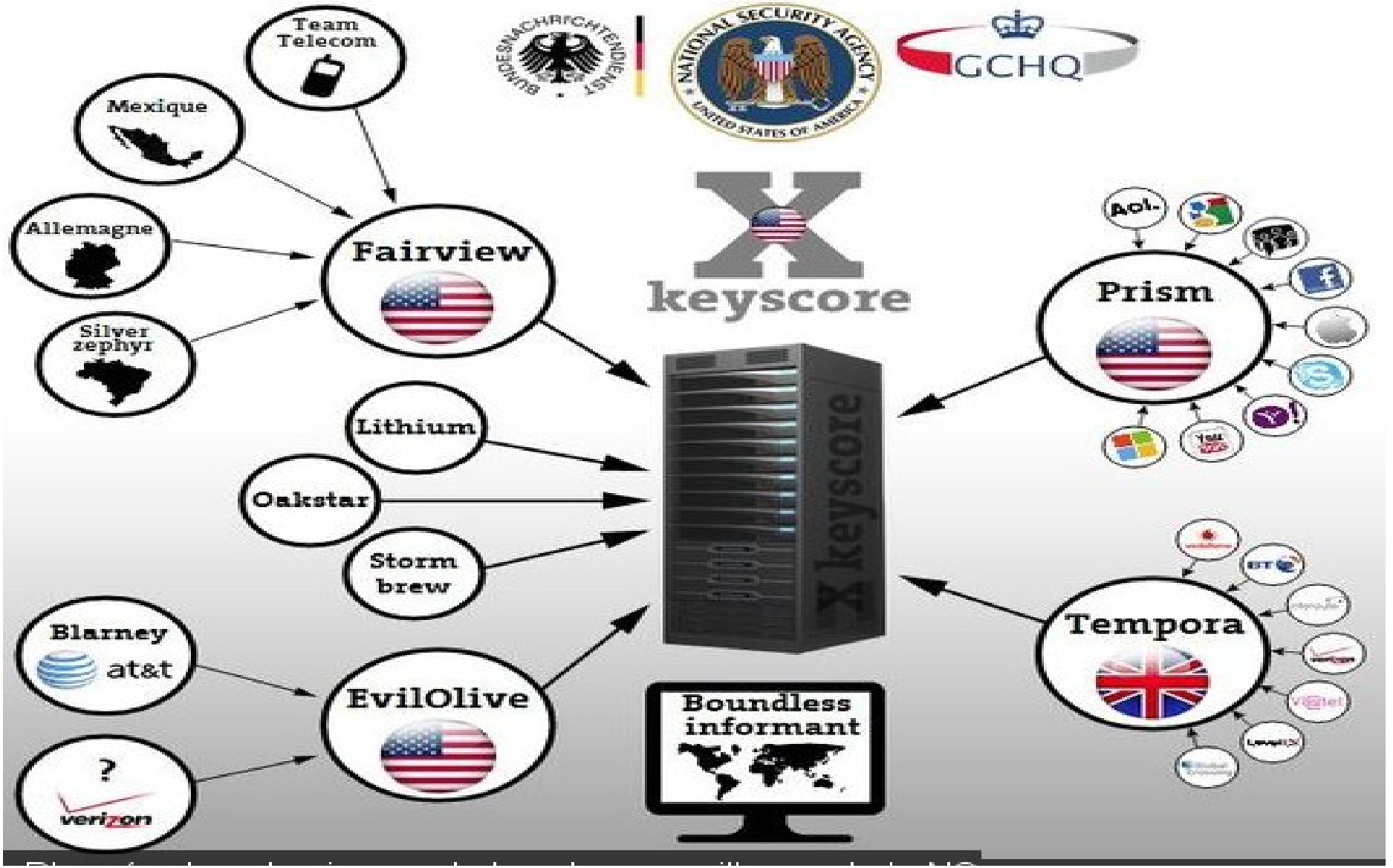
En juin 2013, un ancien consultant de la NSA, Edward Snowden, prit contact avec un journaliste du Guardian, avec en sa possession des milliers de documents sur les pratiques d'espionnage de l'agence, avec, entre autre les programmes PRISM et XKEYSCORE.

De semaines en semaines, les nouvelles révélations d'Edward démontrèrent que le monde entier était espionné par la NSA et GCHQ.

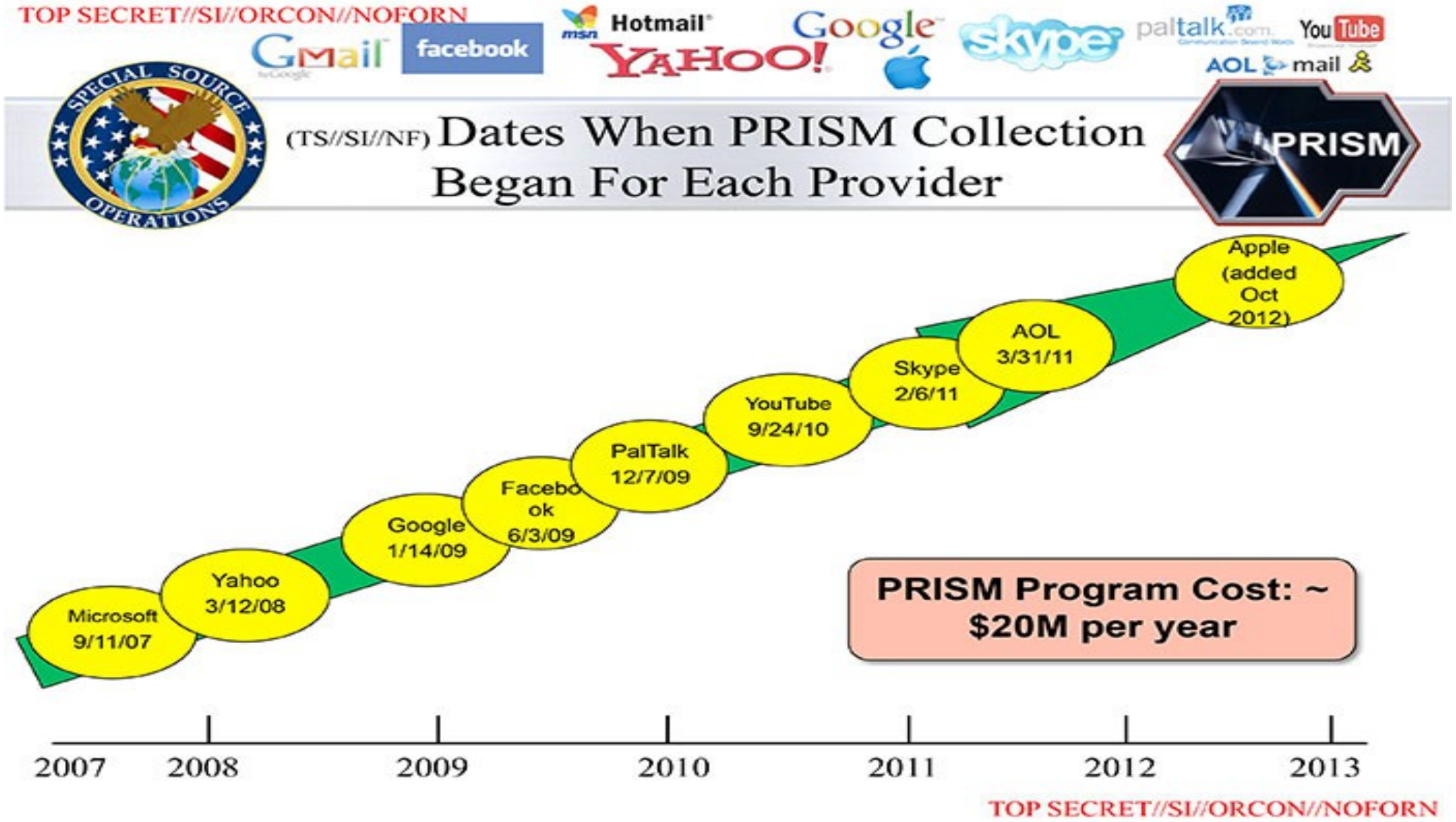
PRISM ? XKEYSCORE ?

- XKEYSCORE est une sorte de Méga moteur de recherche, une sorte de Google pour trouver des informations sur des individus et leurs activités.
- PRISM est une partie du programme XKEYSCORE qui donne un accès direct aux serveurs des acteurs majeurs du monde informatique.
- Nous pouvons apercevoir que Google, Microsoft, Apple, Yahoo, Facebook,... sont impliqués dans ce programme.

XKEYSCORE


Team Telecom
Mexique
Allemagne
Silver zephyr
Fairview
Lithium
Oakstar
Storm brew
Blarney
at&t
?
verizon
EvilOlive
keyscore
X keyscore
Boundless informant
Prism
Tempora
GCHQ
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

PRISM


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider
PRISM
Microsoft 9/11/07
Yahoo 3/12/08
Google 1/14/09
Facebook 6/3/09
PalTalk 12/7/09
YouTube 9/24/10
Skype 2/6/11
AOL 3/31/11
Apple (added Oct 2012)
PRISM Program Cost: ~ $20M per year
2007
2008
2009
2010
2011
2012
2013
TOP SECRET//SI//ORCON//NOFORN

Situation en belgique

- Depuis septembre dernier les FAI belges doivent enregistrer toute l'activité de leurs clients (suivant les directives européennes 2006/24/CE et 2002/58/CE)
- Ils doivent conserver toutes ces données pendant une année
- Présence d'un Firewall qui filtre le contenu d'internet en Belgique
- La N-VA, via le CPAS d'Anvers, fait espionner tous les allocataires sociaux anversois sur internet

Premiers réflexes

Les mots de passe

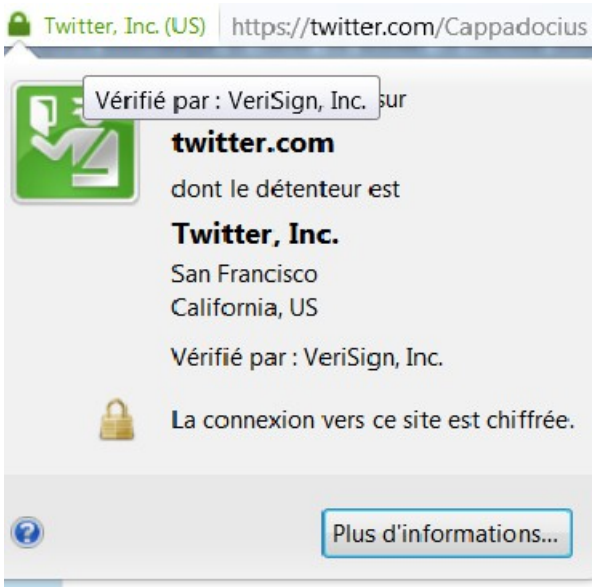
- Faire un bon mot de passe est le premier réflexe élémentaire à avoir, et pourtant c'est l'un des points forts négligé par la majorité des internautes.
- Toujours éviter noms, dates et éléments personnels.
- Toujours faire un mot de passe complexe, et si possible long, avec des lettres minuscules et majuscules, chiffres et caractères spéciaux :

J3-m@Ng3_Un3!P01r3

Https

Https est la version sécurisée du protocole http (hyper text transfert protocol), qui est utilisé pour surfer sur internet. Il permet de :

- Vérifier chez qui on est (petit cadenas vert).
- Sécuriser la visite d'un site internet, en utilisant une connexion chiffrée.

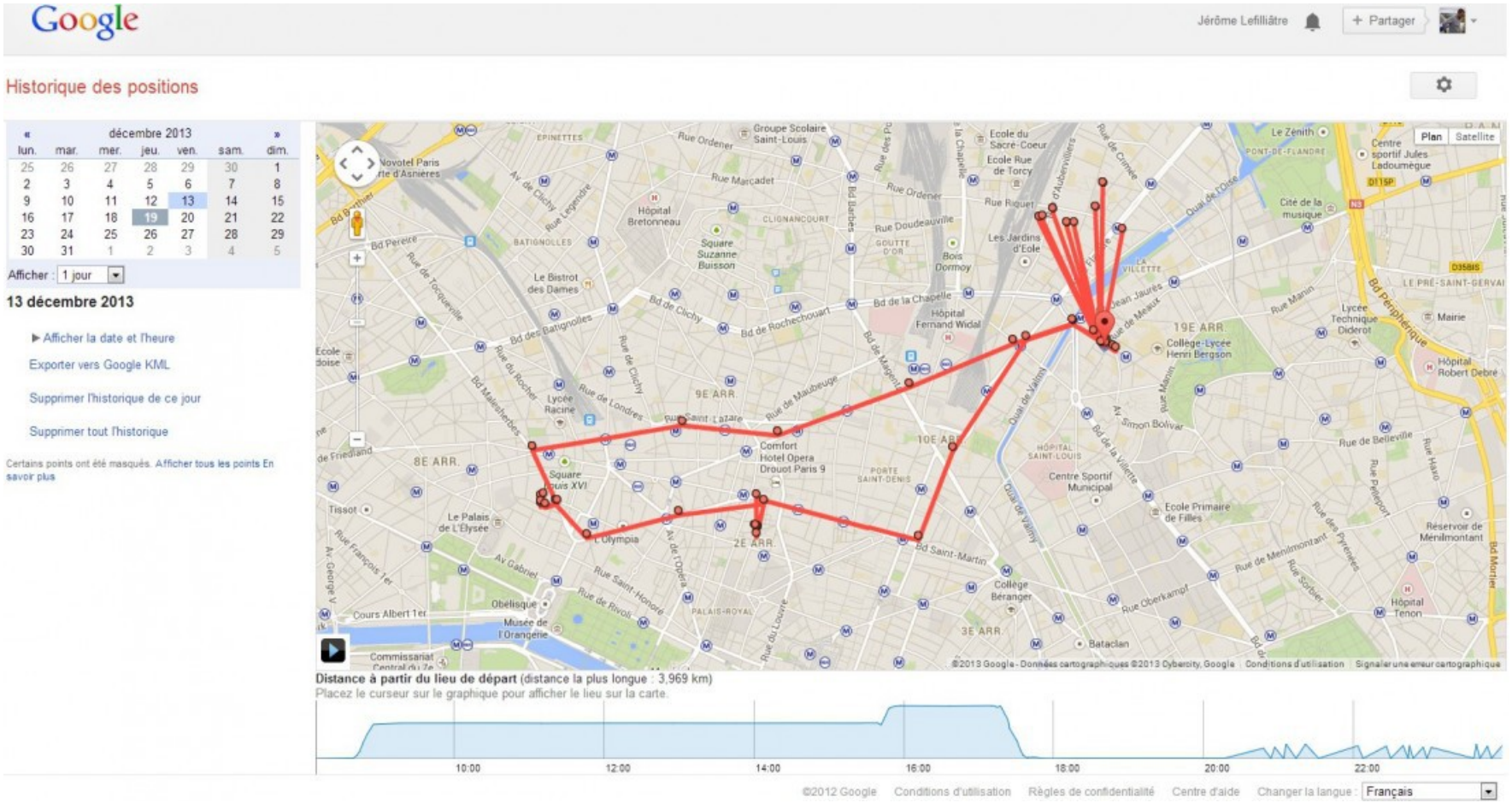


La Géolocalisation

- Tous vos déplacements sont enregistrés sur Android (versions 4 et ultérieures).
- Facebook projette de vous annoncer qui de vos contacts qui se trouvent à proximité.
- Désactiver les services de géolocalisation sur Android, ne les activer qu'en cas de besoin (GPS,...).

Le traçage par Google

- https://maps.google.be/locationhistory/b/0



Autres petits gestes

- Eviter les sites Flash (code non ouvert, backdoors potentiels,...).
- Déconnecter les sessions des réseaux sociaux lorsqu'on ne les utilise pas.
- Désactiver Wi-Fi, bluetooth s'ils ne sont pas utilisés.
- Utiliser moteurs de recherche alternatifs (duckduckgo).

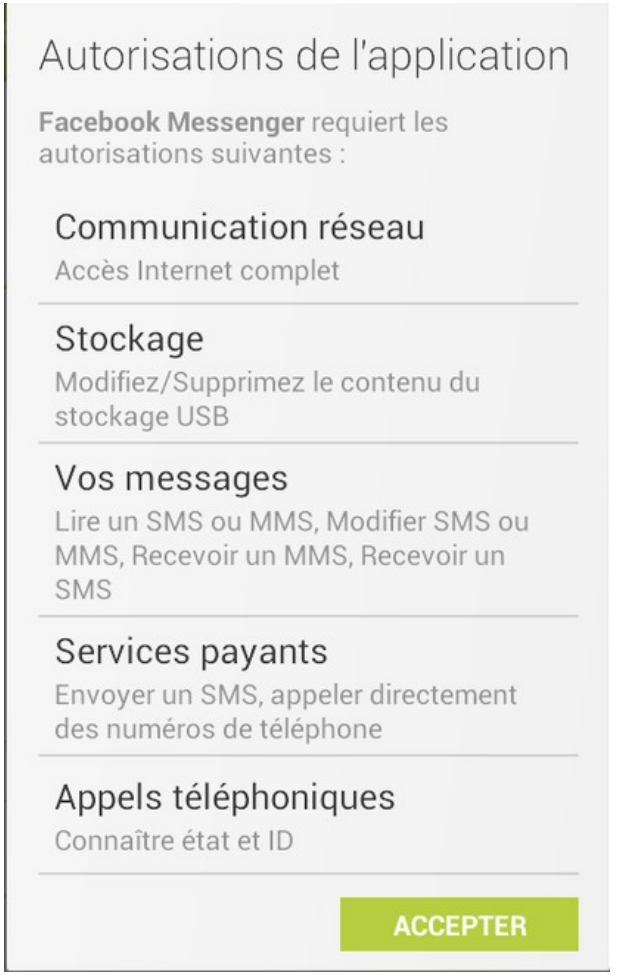
Les réseaux sociaux

Réseaux sociaux : Règles essentielles

- Toute donnée sur un réseau social « propriétaire » doit être considérée comme publique.
- Vous êtes le produit que le réseau social vend à ses annonceurs (publicités, habitudes de consommation,... tout est enregistré).
- Les données mises sur ces réseaux ne sont plus sous votre contrôle.
- Un compte mal sécurisé et le monde entier est au courant de votre vie privée.

Le cas Facebook

- Facebook en sait plus sur vous que vous-même !
  - Contrôle toute vos communications, sms et mms avec Facebook Messenger (et rachat il y a quelques jours des messageries What's App).
  - L'anonymat n'est plus possible, chaque nouvel inscrit doit valider son compte avec téléphone ou envoi de copie de pièce d'identité.(voir slide suivant).
  - Comme beaucoup de réseaux, écoute votre activité sur internet (par exemple avec les boutons like ou la connexion sur site via Facebook,...).
  - Toute donnée effacée par l'utilisateur sont conservées.
  - Suggère la publicité selon vos goûts, habitudes,... et si vous n'aimez pas telle publicité vous demande quelle type d'annonce afficher :

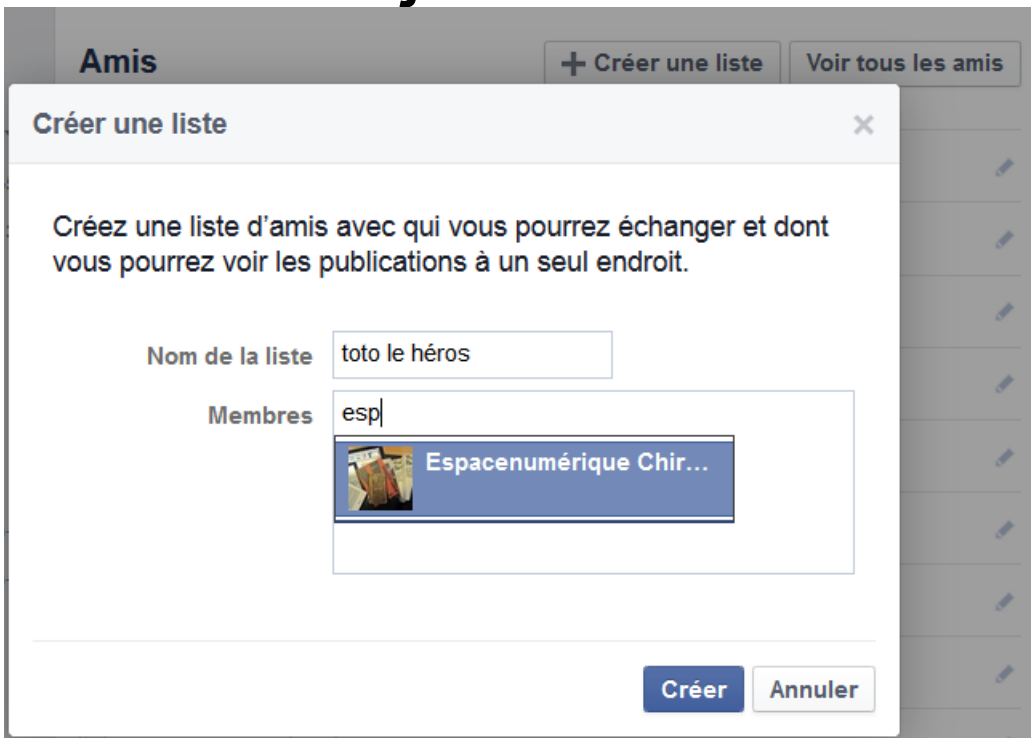


Pas d'anonymat

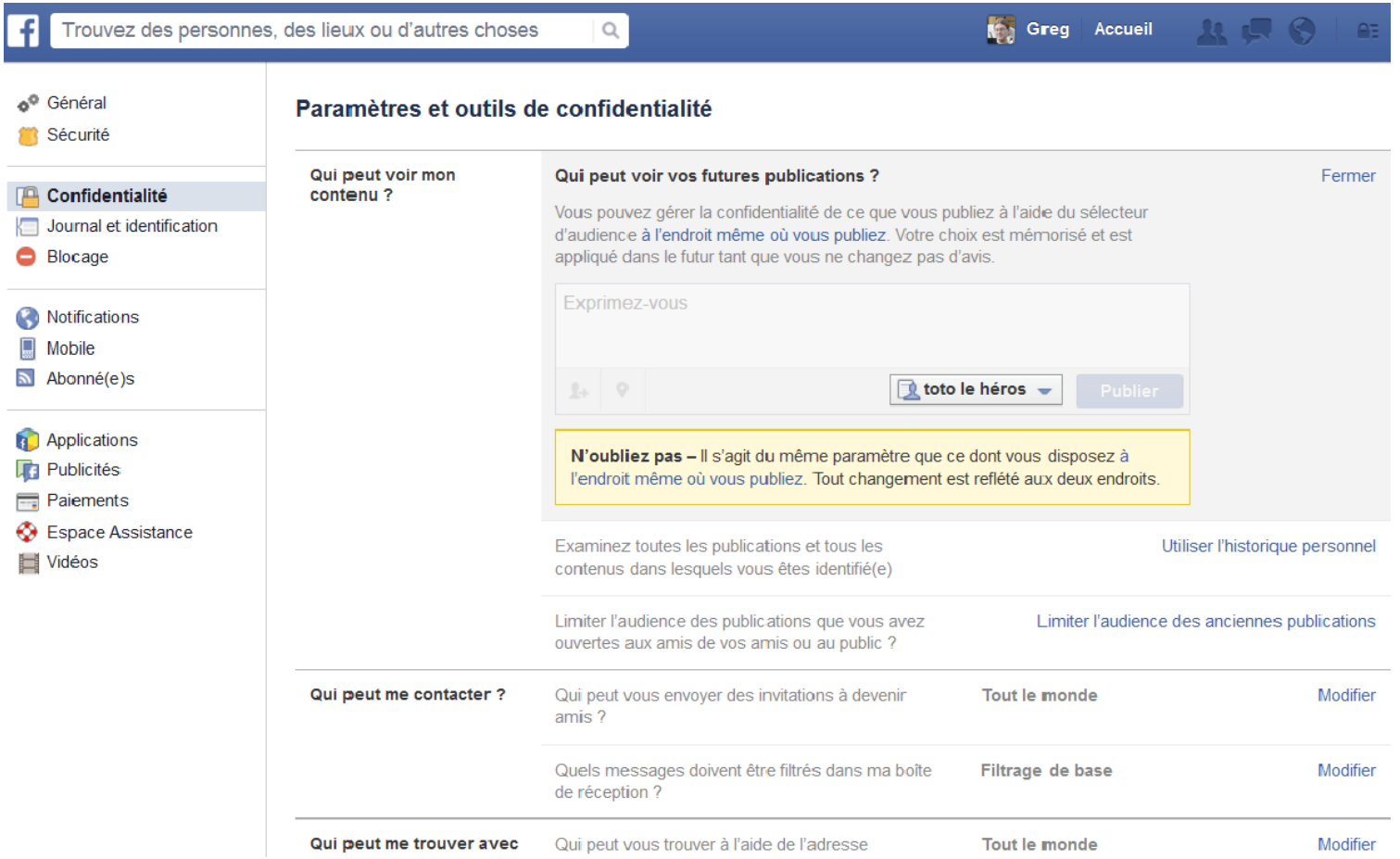
Cloisonnement des publications

- Créer des listes pour cloisonner vos publications, photos, mentions j'aime...

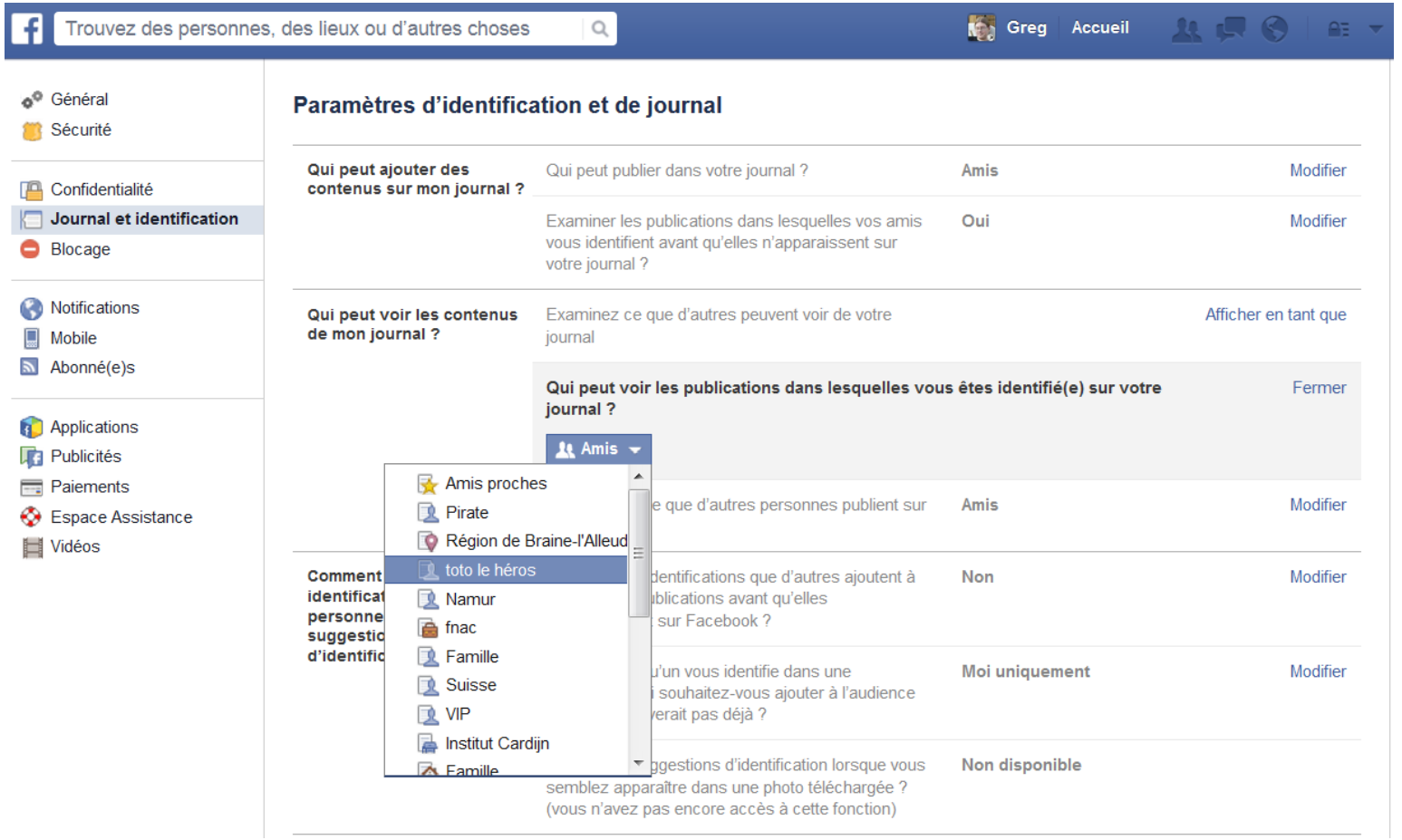
Il est possible de paramétrer presque toute son activité sur Facebook avec les listes, ce qui permet de mieux contrôler nos données sur le réseau, nous verrons comment les utiliser dans les slides suivants.



Gérer la confidentialité

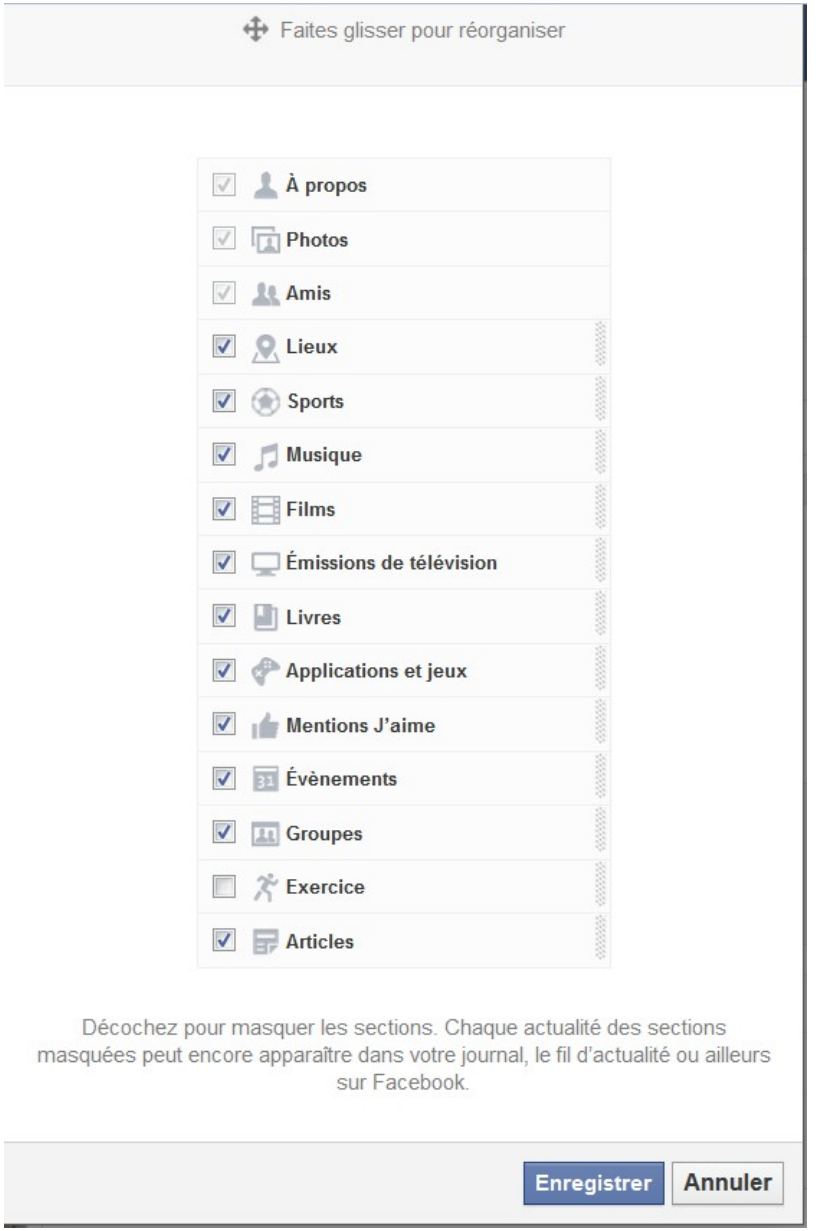


Gérer les identifications et le journal



Gérer qui voit quoi

En cliquant sur le petit crayon sur les panneaux latéraux de gauche, nous pouvons paramétrer ce qui est visible sur le profil. Chaque petit panneau dispose de ses propres panneaux, nous nous arrêterons sur les like, en cliquant sur modifier la confidentialité.

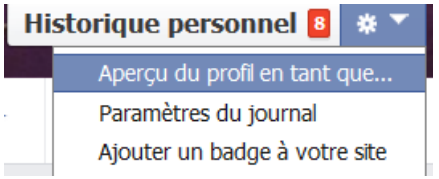


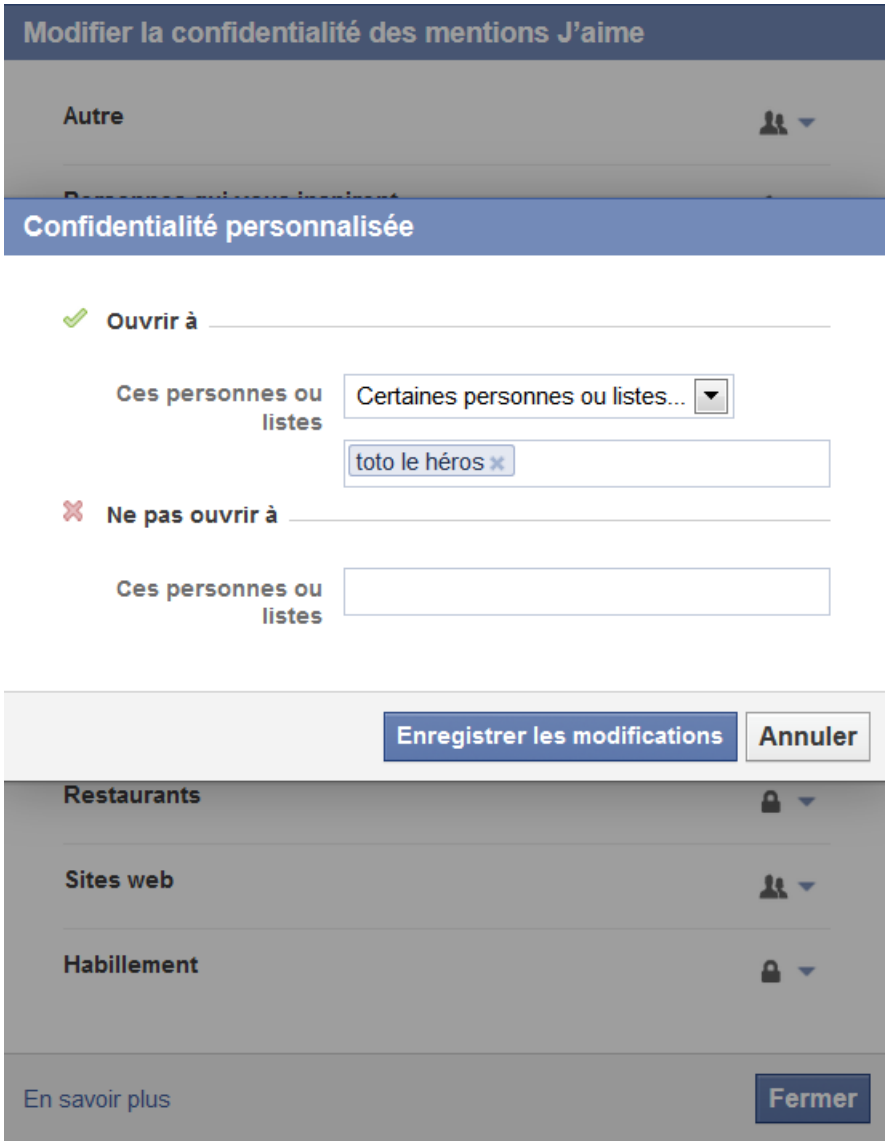
Personnaliser la confidentialité

Chaque catégorie des mentions j'aime est personnalisable. Pour cela, il faut choisir certaines personnes ou listes, et paramétrer comme bon vous semble.

Vous pouvez bien sûr vérifier ce qu'une personne voit (qu'elle soit dans vos contacts ou un simple visiteur).

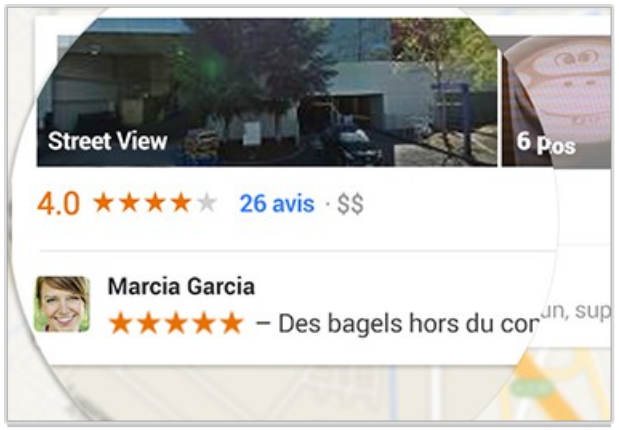
Pour ce faire, cliquez sur le petit verrou près de votre photo de couverture et cliquez sur « Afficher le profil en tant que... »

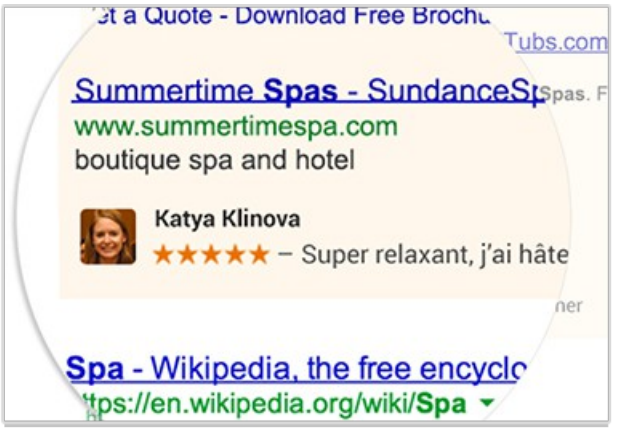




Google Plus

- Toute la confidentialité des listes de Facebook se font via les cercles et son utilisation beaucoup plus simple.
- Néanmoins, Google se réserve le droit d'afficher certaines de vos publications sur son moteur de recherche :





- Se désactive via une case à cocher en bas de page.

Solutions logicielles

Les solutions logicielles

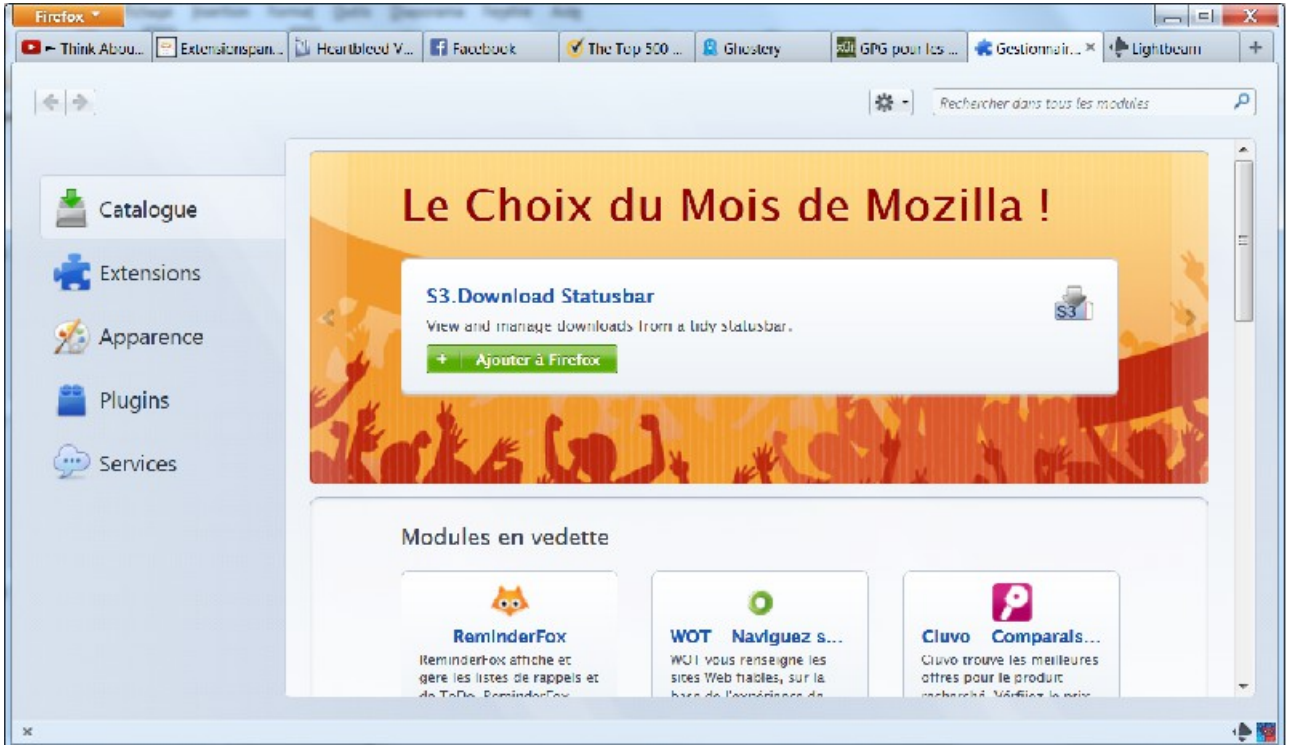
- Le logiciel libre est la meilleure solution
  - Beaucoup de rapports sur des « backdoors » dans les produits Microsoft.
  - L'utilisateur n'a aucun contrôle sur le comportement d'une application propriétaire
  - Le code source d'un logiciel libre est accessible à tous, lisible et donc aisément modifiable en cas de besoin ou problème.
  - Une communauté active qui permet de corriger les bugs/problèmes de sécurité plus rapidement qu'un programme payant.

Changez vos applications !

Application propriétaire	Equivalent libre
Internet Explorer, Safari, Chrome	Mozilla Firefox, Chromium
M$ Office	Open Office, Libre Office
Photoshop	The Gimp
3DS MAX	Blender
Skype	LinPhone, Jabber,Tox...
Mail, Outlook, Incredimail, Livemail,...	Mozilla Thunderbird
Appareils sous Android	Firefox OS ou Cyanogenmod
Windows et Mac OS	GNU/Linux ou FreeBSD (Unix libre)
Nero , cd burner	Géré nativement par les autres systèmes
Win Media Player, WinAmp,...	VLC

Extensions indispensables

- Petits ajouts pour un programme. S'installe en quelques clics.
- Accéder au centre d'applications de Firefox :
  bouton firefox -> Modules complémentaires

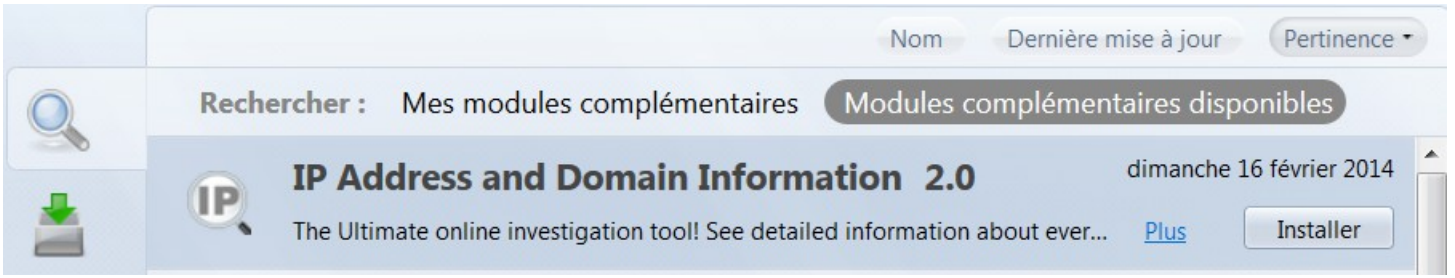


Extensions indispensables

- Adblock : bloqueur d'annonces publicitaires.
- Do Not Track Me / Mask Me : coupe les connexions qui regarde votre activité sur un site internet.
- LightBeam : Permet de visualiser en graphique qui espionne votre activité sur un site internet.
- Cryptocat : « chat » sécurisé et crypté du destinateur au destinataire.
- Foxy Proxy Basic : pratique pour gérer plusieurs proxies.

Installer une extension

- Dans le centre de contrôle des applications, rechercher l'extension désirée et juste cliquer dessus
- Une fois que la barre de progression arrive au bout, l'extension est installée (il se peut qu'un redémarrage du navigateur soit demandé pour que l'application fonctionne.

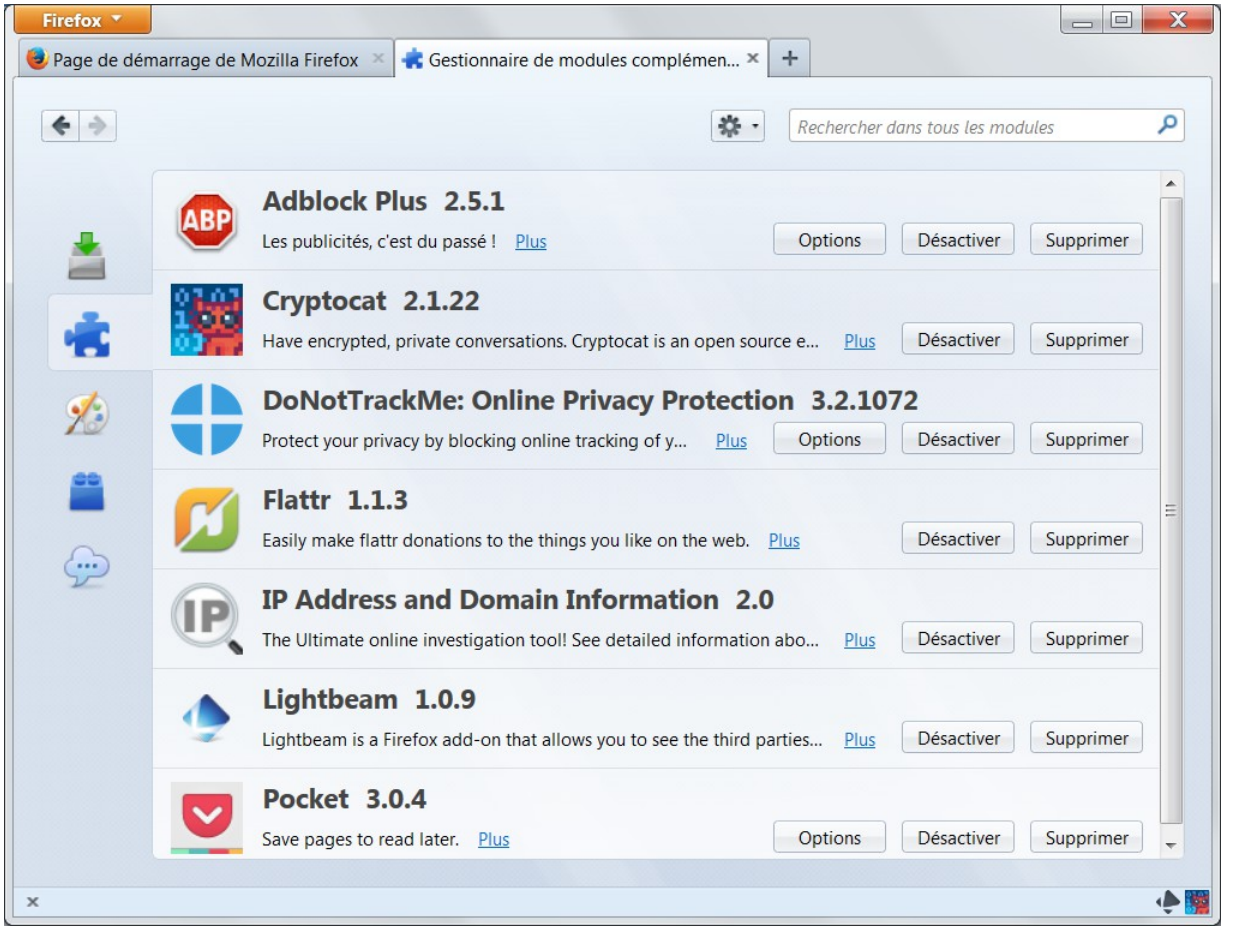


Gestion des extensions

Accès par la petite icône sous forme de pièce de puzzle.

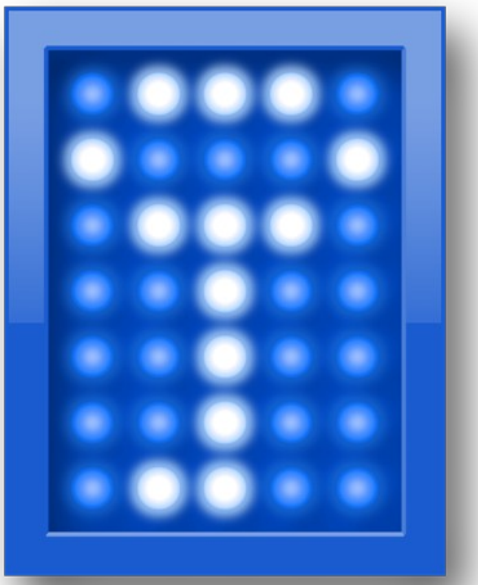
Les options de configuration des extensions s'y trouvent.

Désactivation et suppression des extensions.



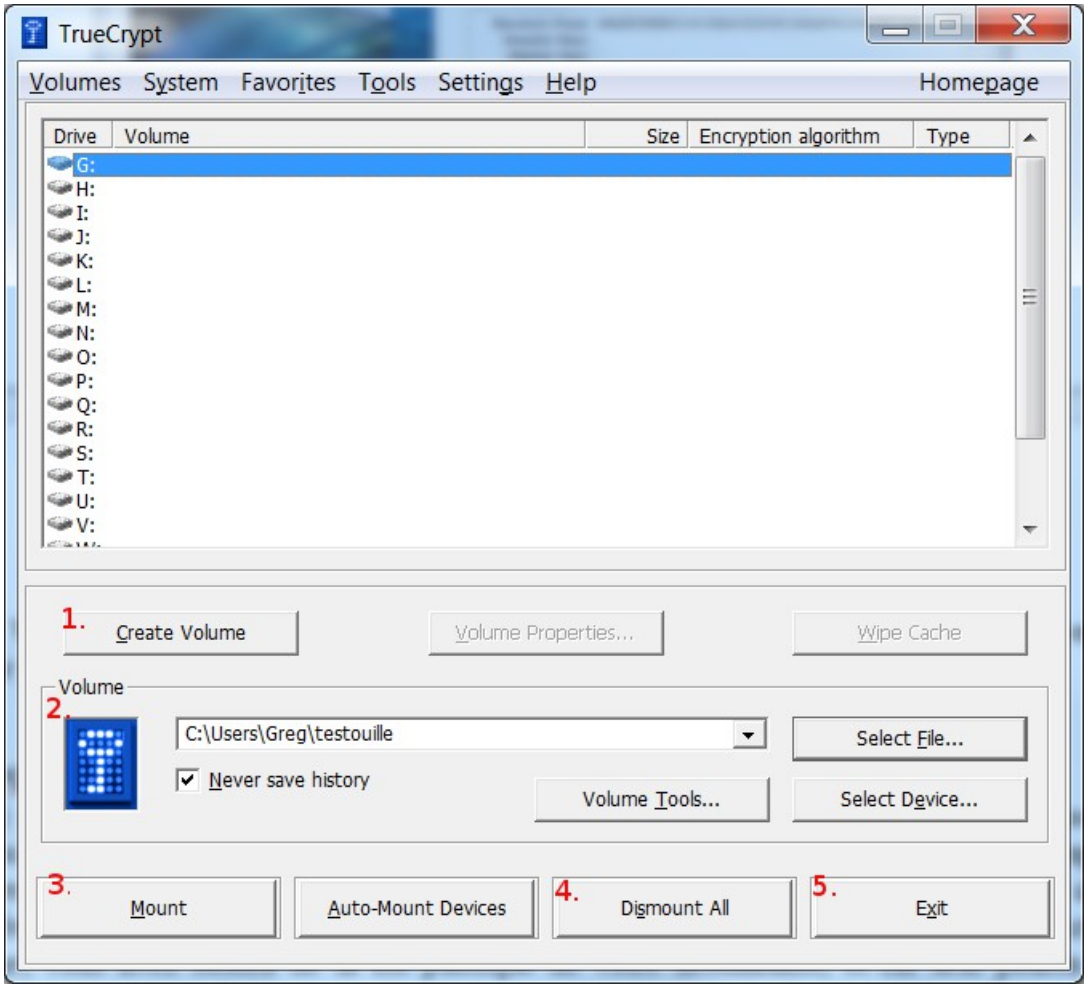
Truecrypt

- Permet de crypter des dossiers, containers, disques durs, clés USB ou systèmes entiers.
- Fonctionne sur tous les systèmes majeurs et rend les données facilement transportables.



Créer un dossier crypté - 1

L'interface d'accueil de Truecrypt sous Windows



1. Options pour créer le dossier crypté.

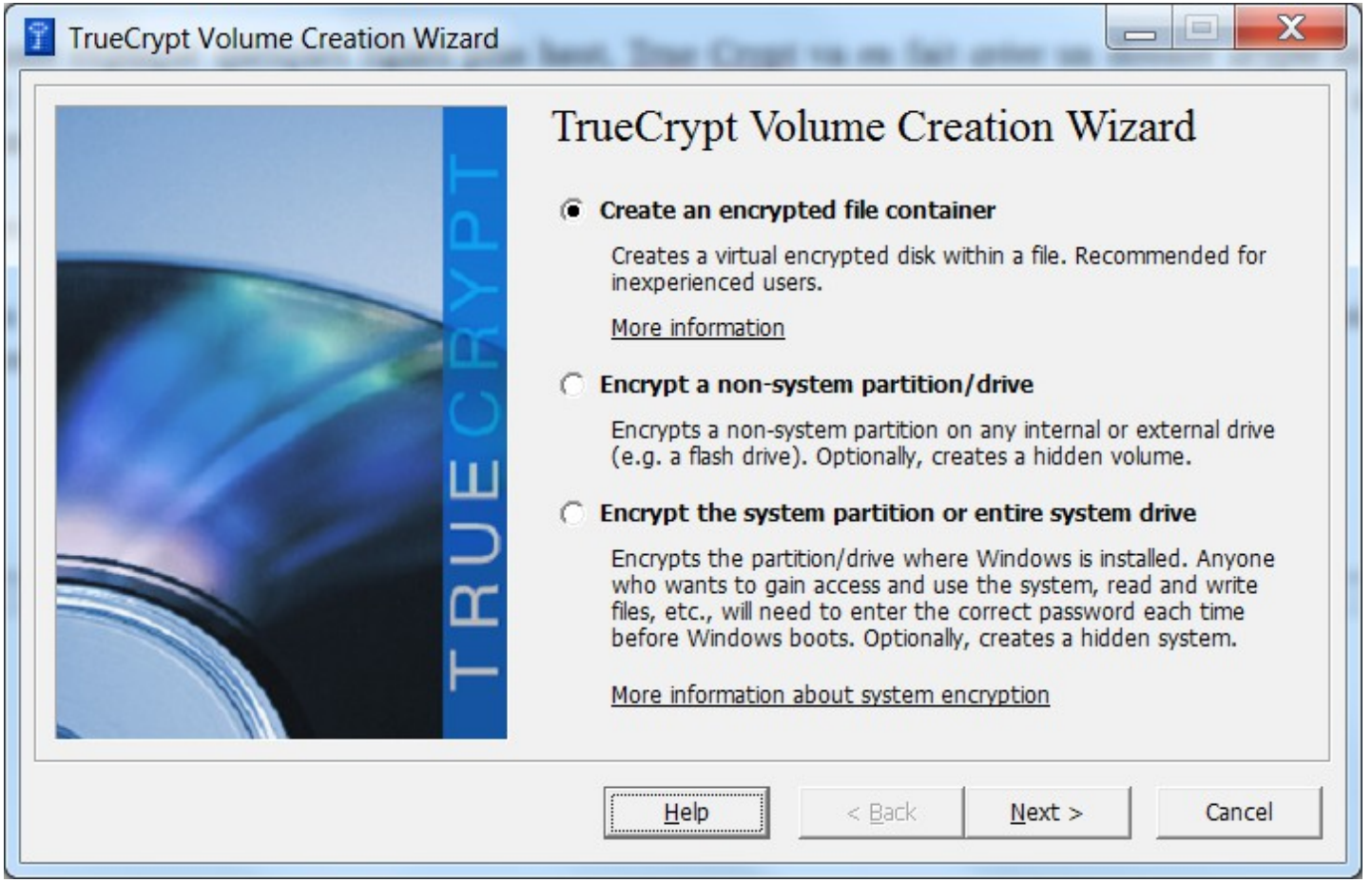
2. Options pour choisir le dossier crypté.

3. Monter le dossier crypté.

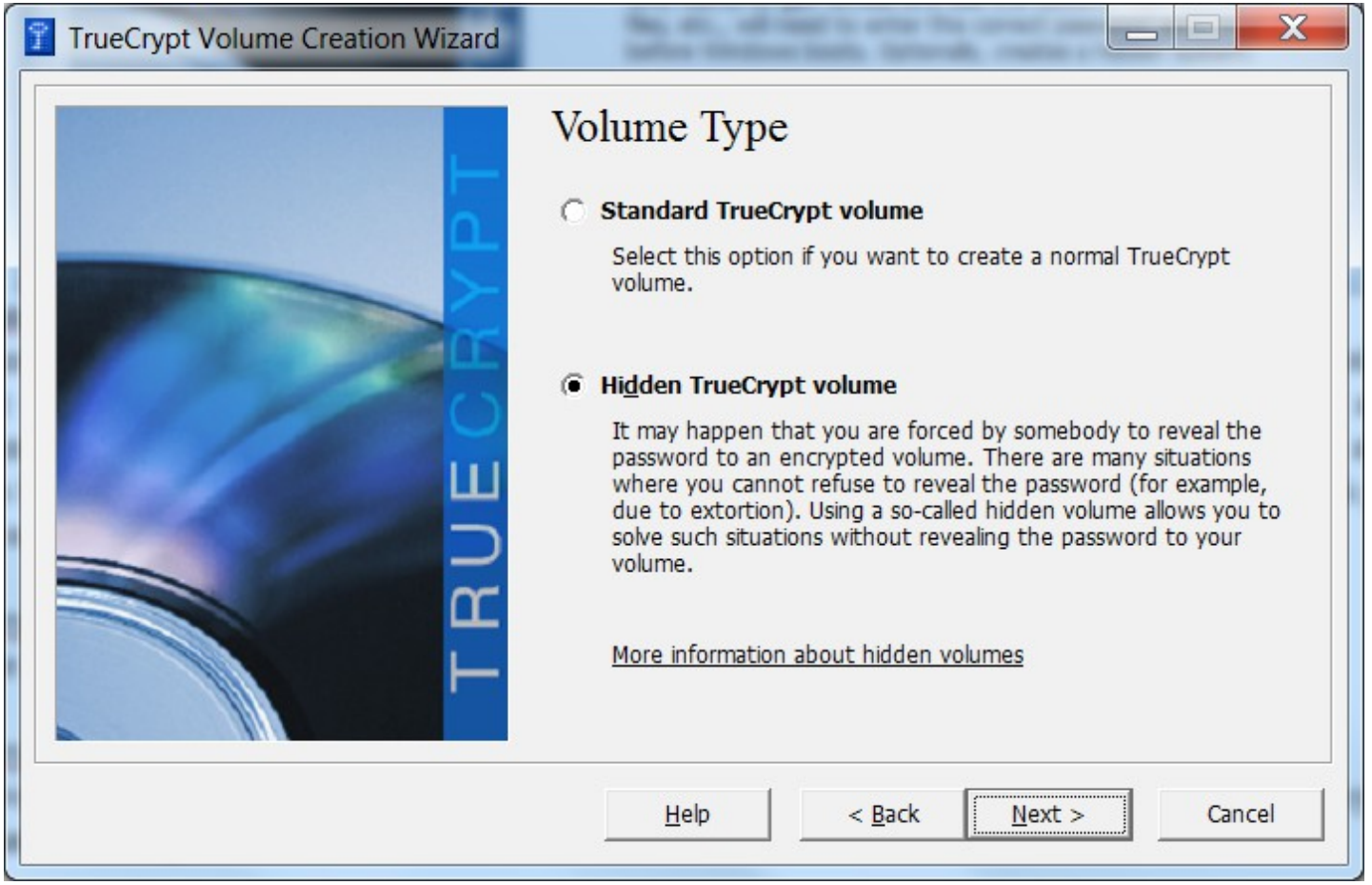
4. Démonter le dossier crypté.

5. Sortie du programme.

Créer un dossier crypté - 2

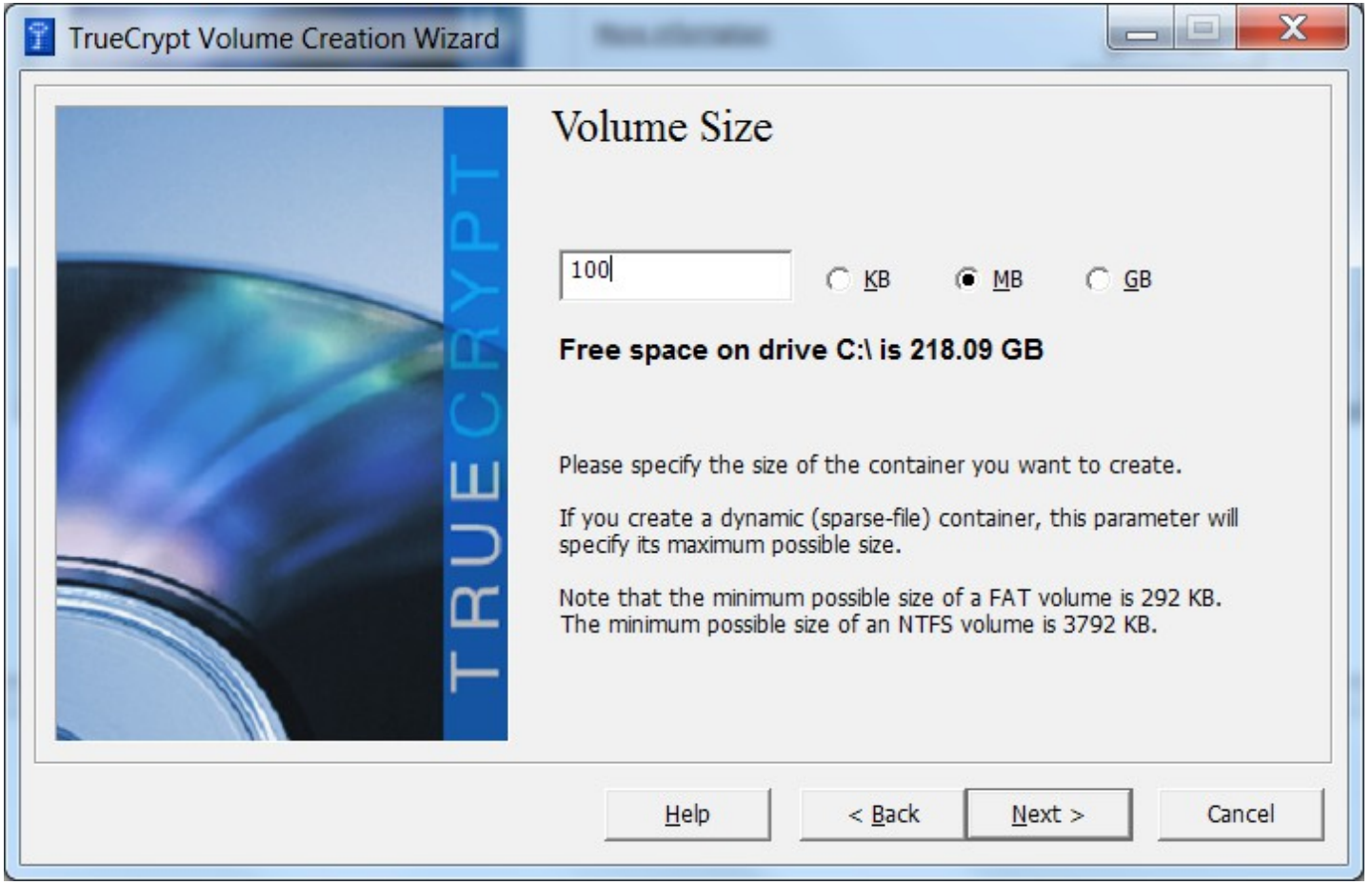


Choix du type du volume

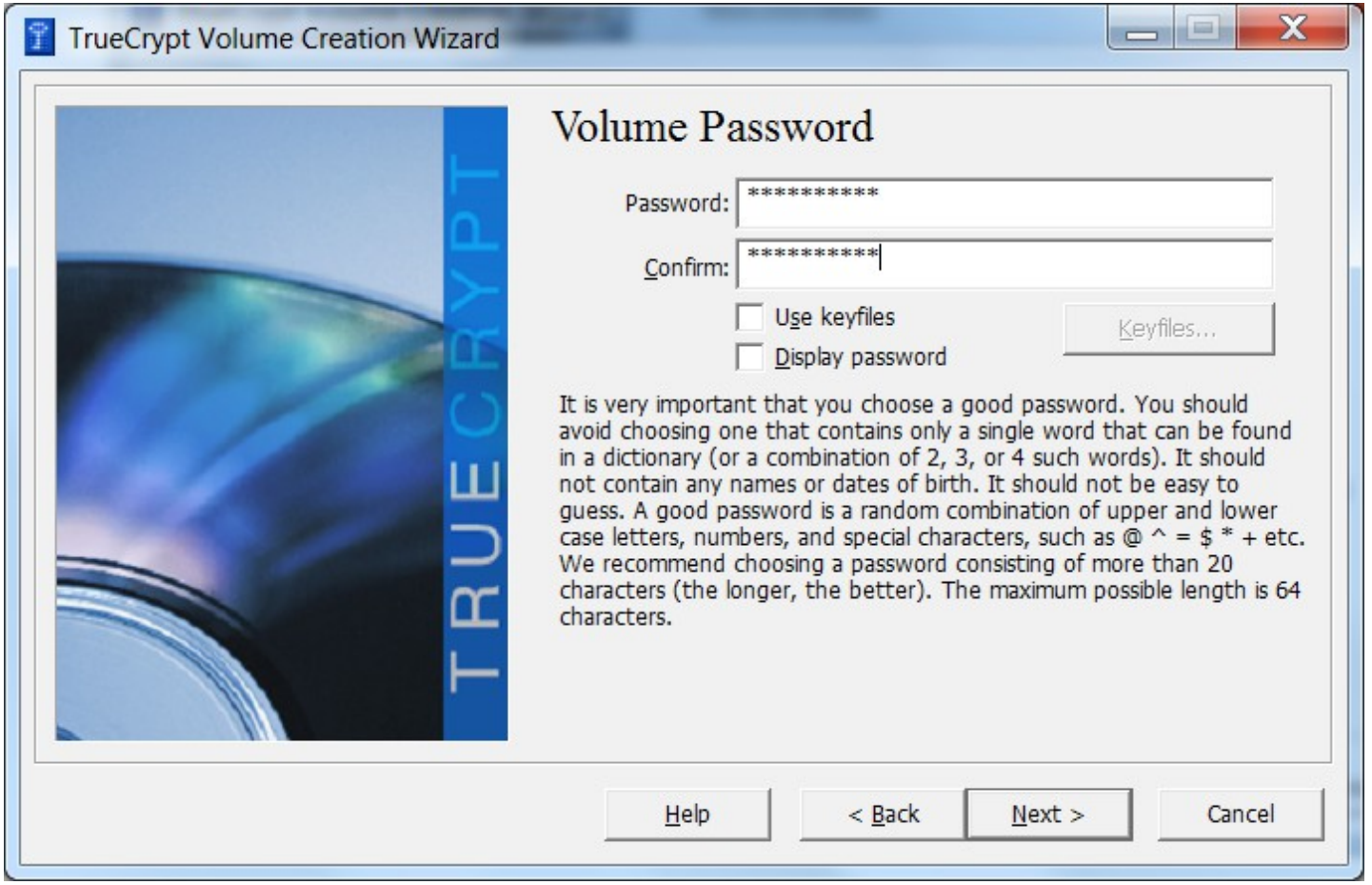


Méthodes de cryptage du dossier

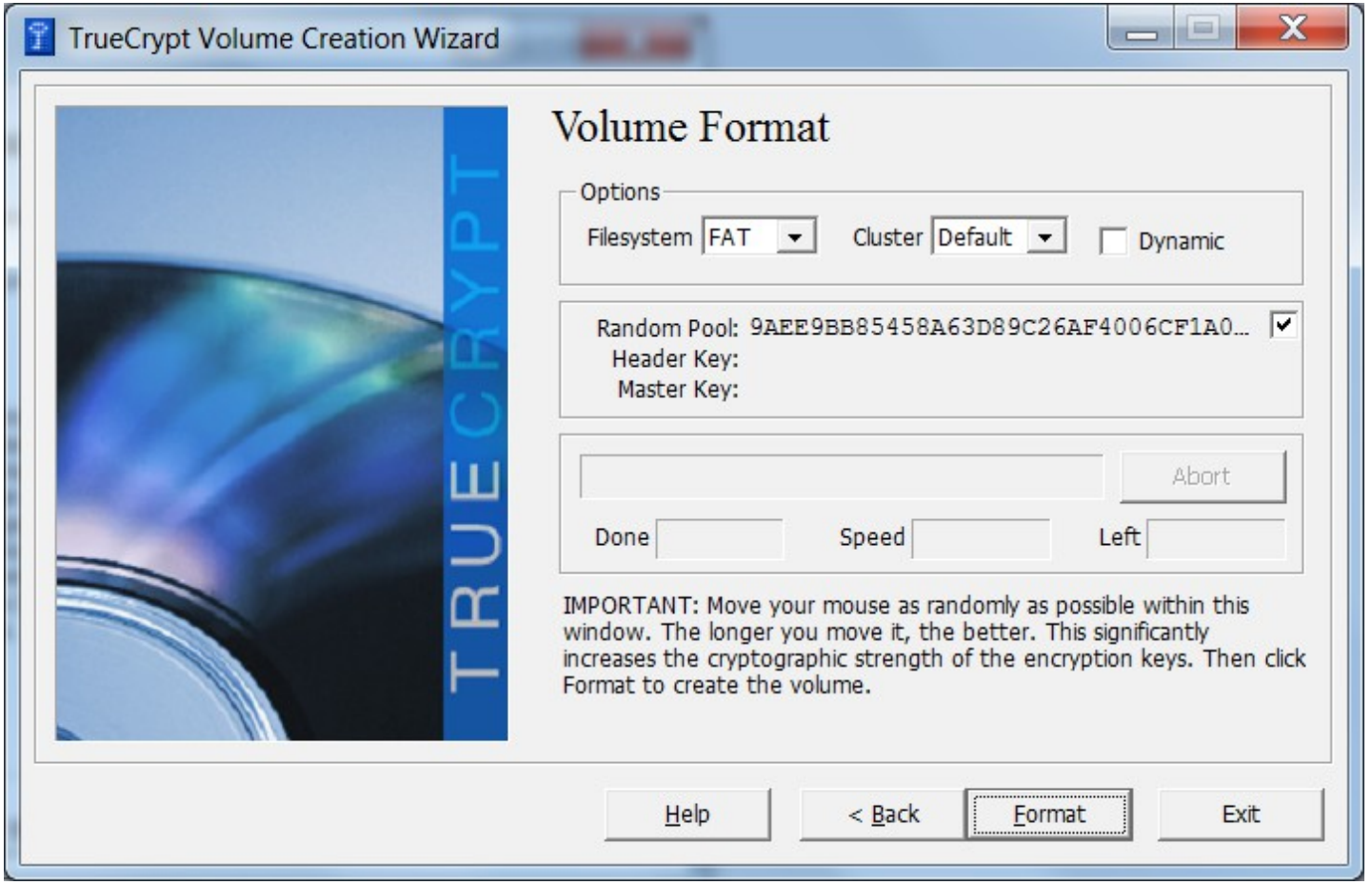
Taille du volume



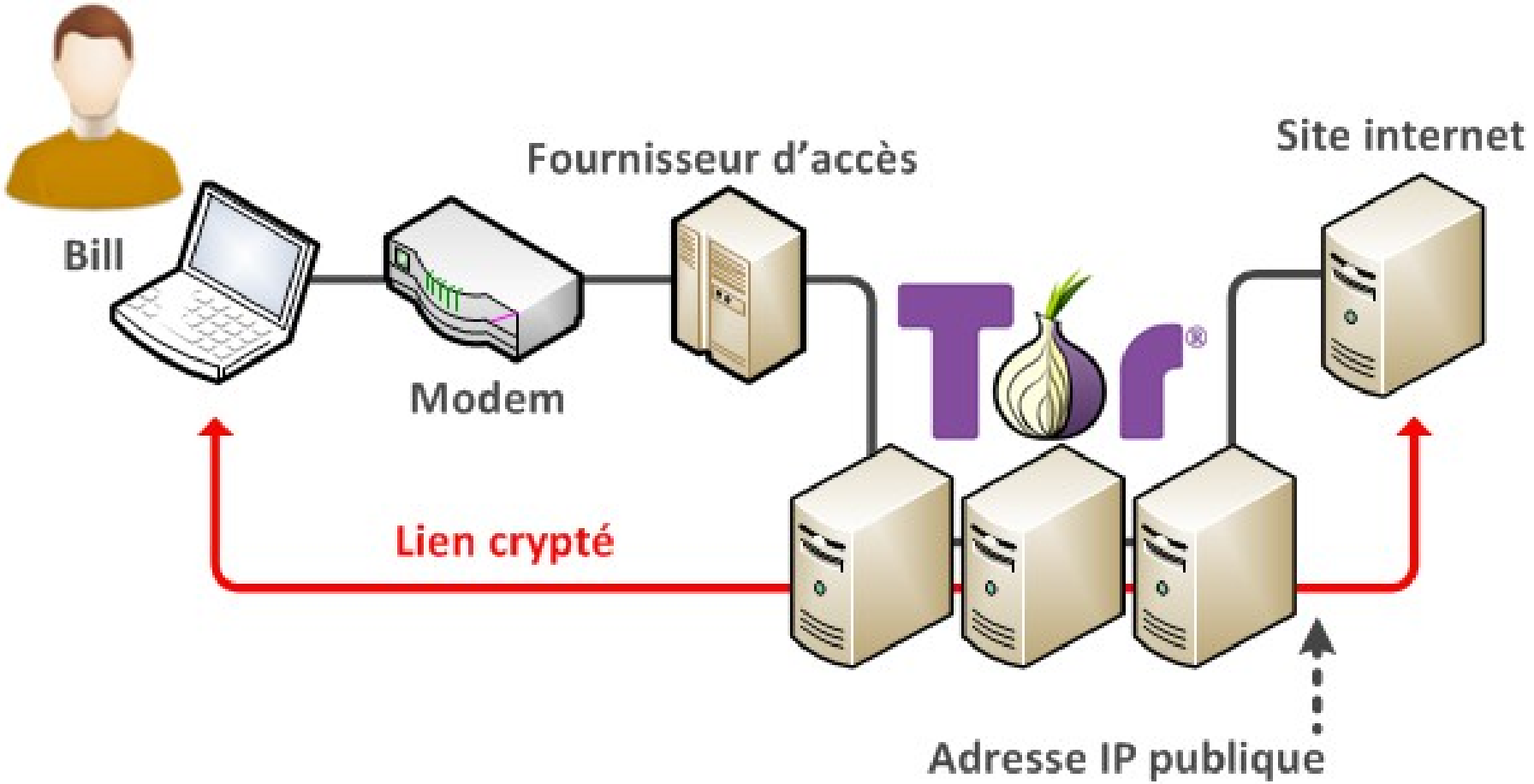
Mots de passe et clés



Formatage du Volume



Comment fonctionne TOR ?

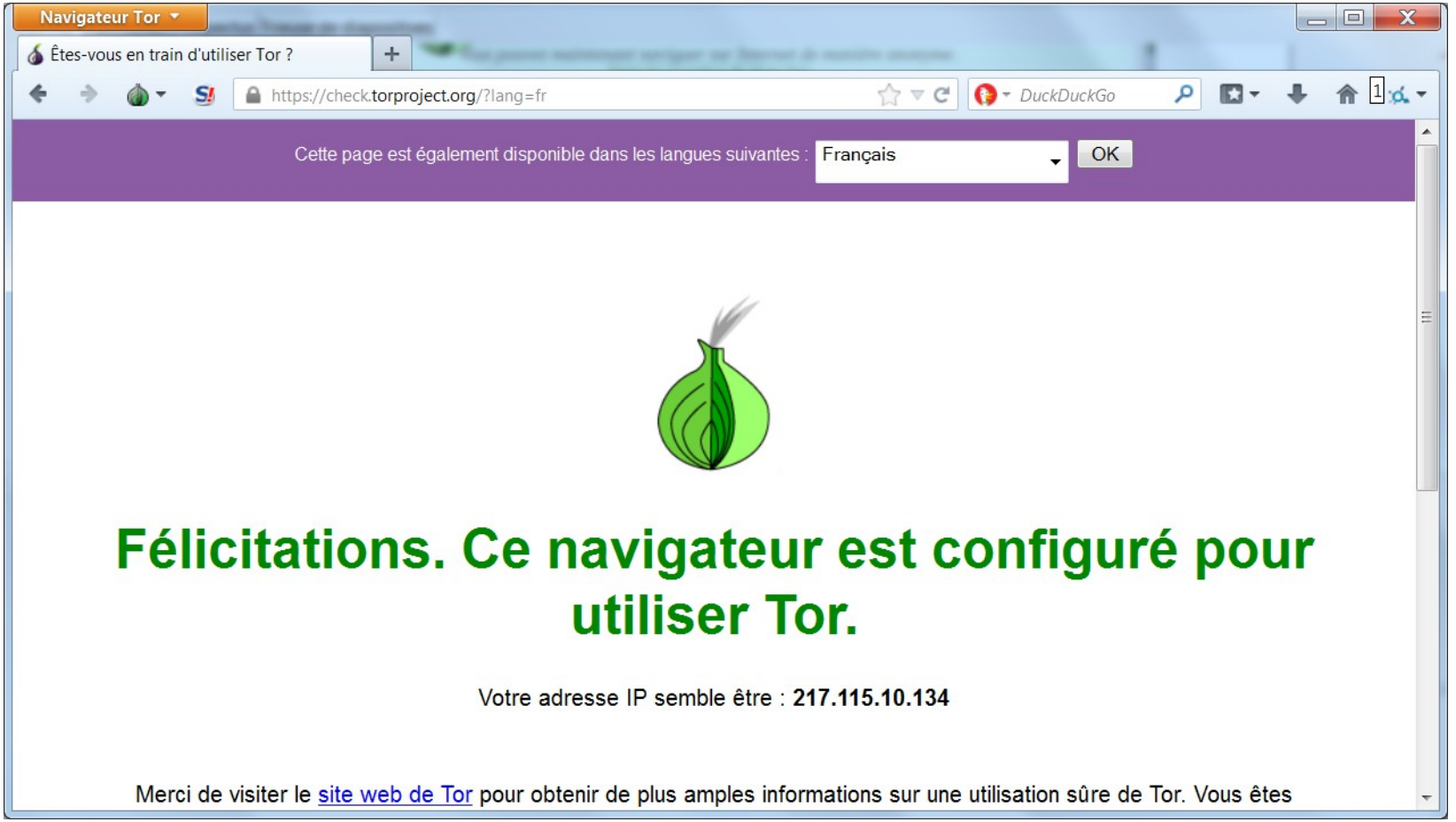


Premiers pas avec TOR

- Utilisation du TOR Software Bundle, prise en main rapide.
- Basé sur Firefox avec différentes extension, prévu pour fonctionner directement après installation.
- Renouvellement de son identité en un clic.

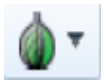
L'interface d'accueil

Vérifier si ça fonctionne



On peut comparer avec votre ip réelle sur un navigateur en surfant sur le site www.whatismyipaddress.com

3 options essentielles :

- Le bouton oignon 
  - Changer d'identité.
  - Gérer les préférences et paramètres réseaux.
- Le bouton No Script 
  - Désactive Javascript.
- Le bouton Https Everywhere 
  - Ou c'est possible, forcer la connexion en https plutôt qu'en http (beaucoup de règles pré-faites).

Aller plus loin

- Cryptez vos mails avec GPG
  - http://wiki.partipirate.org/wiki/Tutoriel:PGP
- Utilisation des VPN
  - http://samoht.fr/tuto/tuto-creer-un-serveur-vpn-sous-windows-gratuit-sans-installation
- Rootage de votre appareil Android
  - http://fsfe.org/campaigns/android/android.html
- Passage sous Linux (Ubuntu est très facile pour les débutants et, une fois les premiers réflexes pris, est plus facile que Windows).
  - http://www.ubuntu.com

Aller plus loin : sensibilisation

- Sensibiliser votre entourage.
- Partage des outils et documents.
- Contacter votre MEP (http://www.respect-my-privacy.eu/fr).
- Support des communautés libristes.

Liens et sources -1

- PRISM/XKEYSCORE
  - http://www.lemonde.fr/technologies/visuel_interactif/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html
  - http://fr.wikipedia.org/wiki/PRISM_(programme_de_surveillance)
  - http://fr.wikipedia.org/wiki/XKeyscore
- Législation sur les télécommunications en Belgique, septembre 2013 et directives européennes
  - http://www.ejustice.just.fgov.be/cgi/article_body.pl?language=nl&pub_date=2013-10-08&numac=2013011510&caller=summary
  - http://eur-lex.europa.eu/legal-content/fr/ALL/;jsessionid=41ylTWJDY9pXW0GBYQV0ny2V7dXGTYyrDVJPCTPQG6yVvDnT9wx8!1663640074?uri=CELEX:32006L0024
  - http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32002L0058
- Moteur de recherche alternatif
  - https://www.duckuckgo.com
- La localisation avec Google
  - https://maps.google.com/locationhistory/b/0/
    https://support.google.com/gmm/answer/3118687?p=maps_location_settings&rd=1
- Le site officiel des cryptoparty
  - https://www.cryptoparty.in/

Liens et sources -2

- Logiciels utilisés :
  - http://www.truecrypt.org/
  - https://www.torproject.org/
  - https://adblockplus.org/fr/firefox
  - https://www.abine.com/index.html
- Sites des associations promouvant le libre, la protection de la vie privée et la neutralité du net :
  - http://www.nurpa.be/
  - http://fsfe.org/index.fr.html
  - https://www.april.org/
  - http://www.laquadrature.net/fr
  - http://www.framasoft.net/

- Autres sources disponibles sur mon blog personnel :
  - http://www.antredugreg.be/

Téléchargements et contacts

- Twitter : @cappadocius
- About.me : http://about.me/greg.siebrand/
- XMPP : greg@xmpp.pirateparty.be
- Mail : g.siebrand@gmail.com
- Téléchargements : http://antredugreg.be/votre-vie-privee/