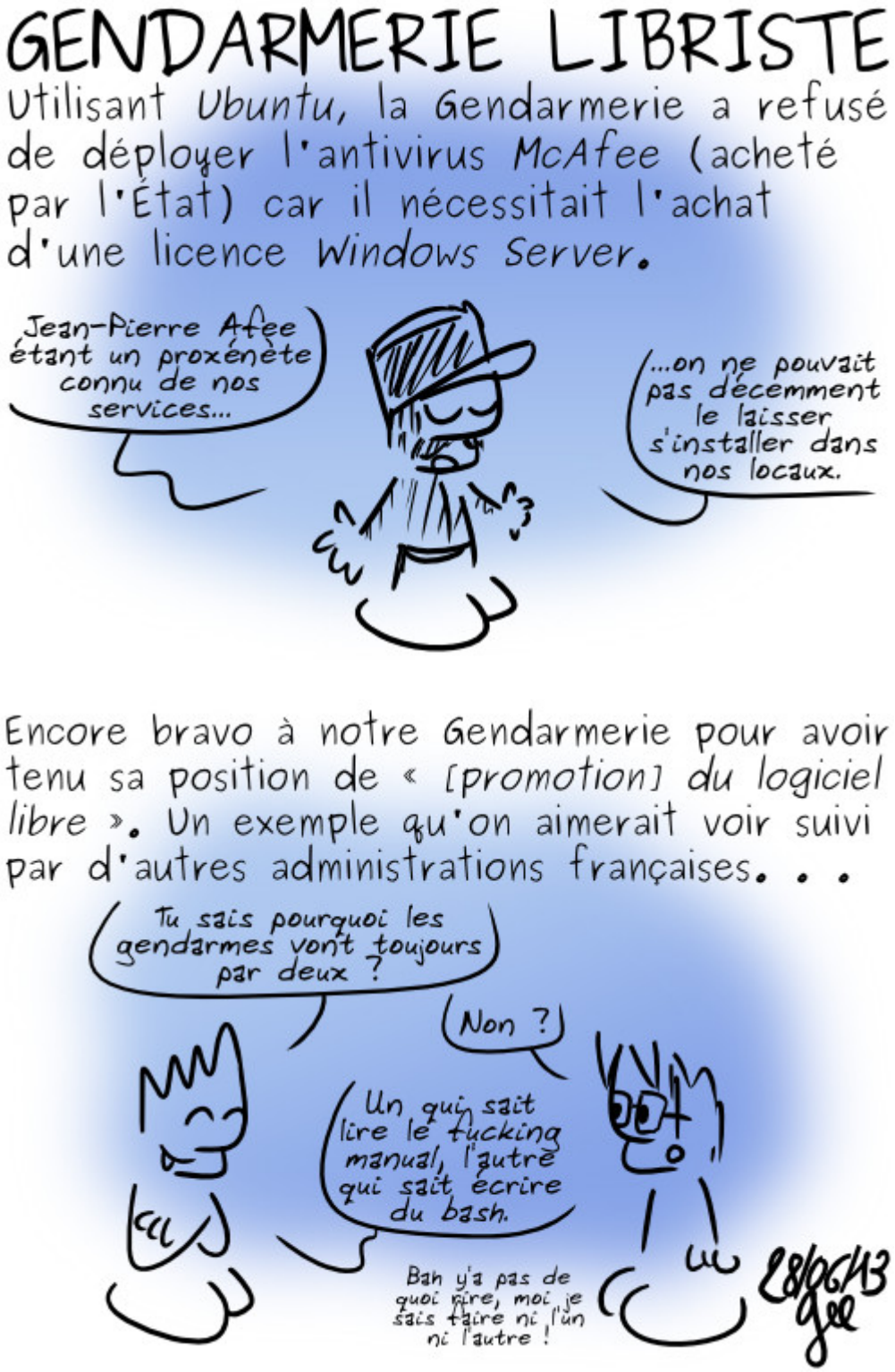
Geektionnerd : Gendarmerie libriste



Ce n'est pas la première fois que la Gendarmerie Nationale mérite un coup de chapeau des libristes, souvenez-vous de la migration massive vers Ubuntu.

Source :

- Comment la Gendarmerie a envoyé bouler Microsoft et McAfee (Numérama)

Crédit : Simon Gee Giraudot (Creative Commons By-Sa)

---

13 points que les gens détestent sur la documentation de votre projet libre

Qu'il s'agisse de son code ou de son utilisation, la faiblesse de la documentation d'un logiciel libre est souvent montrée du doigt.

Voici, selon Andy Lester, 13 défauts ou lacunes communément rencontrés, qui sont autant d'écueils que l'on peut contourner avec un minimum d'efforts aujourd'hui pour gagner demain un temps précieux.

13 choses que les gens détestent sur vos documentations open source

13 Things People Hate about Your Open Source Docs

Andy Lester – 10 janvier 2013 – SmartBear Blog
(Traduction : Lamessen, calou, Shanx, sinma, Asta + anonymes)

La plupart des développeurs open source aiment penser à la qualité du logiciel qu'ils développent, mais la qualité de la documentation est souvent laissée de côté. Il est rare de voir vanter la documentation d'un projet, et pourtant elle a un impact direct sur sa réussite. Sans une bonne documentation, les utilisateurs n'utiliseront pas votre projet, ou ils n'y prendront pas de plaisir. Les utilisateurs comblés sont ceux qui diffusent des infos à propos de votre projet – ce qu'ils ne font qu'après avoir compris comment il fonctionne. Et ils apprennent cela à partir de la documentation du projet.

Malgré tout, de trop nombreux projets ont une documentation

décevante. Et cela peut être décevant de plusieurs manières.

Les exemples que je donne ci-dessous sont purement arbitraires, je ne veux pas cibler un projet en particulier. Ce sont seulement ceux que j'ai utilisés récemment, cela ne veut pas dire qu'ils représentent les pires atrocités. Chaque projet a commis au moins quelques-uns de ces péchés. Que vous soyez utilisateur ou développeur, à vous d'évaluer à quel point votre logiciel préféré est ou non coupable, et comment vous pouvez aider à y remédier le cas échéant.

1. Le manque d'une bonne introduction ou d'un README/LISEZ-MOI

Le README/LISEZ-MOI est la première impression que les utilisateurs potentiels ont de votre projet. Si le projet est sur GitHub, le README/LISEZ-MOI est automatiquement affiché sur la page d'accueil du projet. Si vous l'avez mal rédigé, ils peuvent ne jamais revenir.

Vous voulez capter l'attention du lecteur et l'encourager à continuer la découverte de votre projet ? Le README/LISEZ-MOI devrait alors au moins expliquer :

- ce que le projet fait
- pour qui il est fait
- sur quel matériel ou plateforme il tourne
- toutes les dépendances majeures, comme « Requiert Python 2.6 et libxml »
- comment l'installer, ou un accompagnement de chaque étape à la suivante.

Tout cela doit pouvoir être compris par quelqu'un qui n'a jamais entendu parler de votre projet, et peut-être même jamais imaginé un projet pouvant s'en rapprocher. Si le projet possède un module calculant la distance de Levenshtein, ne partez pas du principe que n'importe qui lisant votre README/LISEZ-MOI sait ce que c'est. Expliquez que la distance de Levenshtein est utilisée pour comparer deux chaînes de

caractères, et ajoutez quelques renvois vers des explications plus poussées pour celui qui aimerait approfondir le sujet.

Ne décrivez pas votre projet par rapport à un autre projet, comme « NumberDoodle est comme BongoCalc, mais meilleur ! » Ça n'est d'aucune aide pour quelqu'un qui n'a jamais entendu parlé de BongoCalc.

2. La documentation non disponible en ligne

Bien que je n'ai pas lu d'études à ce sujet, je serais prêt à parier que 90% des recherches de documentation sont faites avec Google et un navigateur sur Internet. La documentation de votre projet doit être en ligne, et disponible. Partant de là, il serait embarrassant que la documentation de mon propre projet, ack, ne soit pas disponible à l'endroit où la majorité des gens vont la chercher. Mon hypothèse est basée sur ma propre expérience, à savoir que si je veux connaître le fonctionnement d'un outil en ligne de commande, je vais vérifier sa page man.

Comment je m'en suis aperçu ? Les utilisateurs m'écrivaient pour me poser des questions dont les réponses se trouvaient dans la FAQ. Ce qui m'a ennuyé : ils ne lisaient pas ma FAQ. Il se trouve qu'ils avaient cherché sur le site internet, mais je n'avais pas mis la FAQ à cet endroit. C'est une erreur facile à faire. Je suis proche du projet et je n'ai jamais eu besoin d'utiliser moi-même la FAQ, je n'avais donc pas remarqué qu'elle n'était pas présente en ligne. Beaucoup de problèmes sont dus à ce piège : les auteurs ne se mettent pas à la place des utilisateurs.

3. La documentation disponible uniquement en ligne

Le revers de ce problème est d'avoir la documentation disponible uniquement en ligne. Certains projets ne distribuent pas la documentation avec les livrables du projet, ou incluent une version médiocre de la documentation.

Le moteur de recherche Solr, par exemple, a un excellent wiki qui sert à la documentation du projet. Malheureusement, la documentation liée au téléchargement comporte 2200 pages de Javadoc d'API auto-générées. Au final, la seule documentation pour l'utilisateur est une unique page de tutoriel.

Le langage PHP n'est distribué avec aucune documentation. Si vous voulez la documentation, vous devez aller sur une page séparée pour les obtenir. Pire, seule la documentation du cœur est disponible au téléchargement, sans les annotations utiles des utilisateurs (voir « Ne pas accepter les remarques des utilisateurs » plus bas), et ce n'est pas le même format facile à parcourir que celui qui est disponible en ligne.

Les projets open source ne peuvent pas supposer que les utilisateurs ont accès à Internet quand ils ont besoin de la documentation. Le mode avion existe toujours. De toute façon, vous ne souhaitez pas que l'utilisateur dépende uniquement du fait que votre site web est disponible ou non. Au moins à deux reprises durant les derniers mois, le wiki de Solr était indisponible au beau milieu de ma journée de travail alors que je recherchais des informations sur un problème de configuration épineux.

Un projet qui fait les choses bien est Perl et son dépôt de module CPAN. La documentation pour chaque module est disponible soit à search.cpan.org ou metacpan.org dans un format hypertexte facile à lire. Pour la consultation hors-ligne, la documentation de chaque module est intégrée dans le code lui-même, et quand le module est installé sur le système d'un utilisateur, la documentation locale est créée sous forme de pages man. Les utilisateurs peuvent aussi utiliser « perldoc Module::Name » pour obtenir la documentation depuis le shell. En ligne ou hors-ligne : c'est votre choix.

4. La documentation non installée avec le paquet

Ce problème est généralement une erreur des paquageurs, pas

des auteurs du projet. Par exemple, sur Ubuntu Linux, la documentation du langage Perl est séparée, ce sont des paquets optionnels pour le langage lui-même. L'utilisateur doit savoir qu'il doit explicitement installer la documentation de la même façon que le langage principal ou il n'y aura pas accès quand il en aura besoin. Ce compromis de quelques mégabites d'espace disque au détriment de la documentation à portée de main de l'utilisateur dessert tout le monde.

5. Le manque de captures d'écran

Il n'y a pas de meilleur moyen d'obtenir l'attention potentielle d'un utilisateur, ou d'illustrer un usage correct, qu'avec des captures d'écran judicieuses. Une image vaut mieux qu'un long discours, c'est encore plus important sur Internet parce que vous ne pouvez obtenir d'un lecteur de lire plus de quelques centaines de mots en tout.

Les captures d'écran accompagnant le texte sont inestimables pour guider l'utilisateur voulant faire les choses au mieux. Une capture d'écran lui permet de comparer visuellement ses résultats à ceux de la documentation et va le rassurer d'avoir exécutée la tâche correctement ou l'aidera à trouver facilement ce qui ne va pas.

Il est de plus en plus commun de trouver des vidéos sur le site internet d'un projet pour en donner un aperçu, et c'est génial. Tout autant que le fait d'avoir une vidéo pour chaque étape d'un processus complexe. Le projet Plone, par exemple, a un site entier dédié aux tutoriels vidéos. Cependant, les vidéos ne peuvent pas remplacer les captures d'écran. Un utilisateur veut voir rapidement l'allure des captures d'écran sans s'arrêter devant une vidéo. Les vidéos n'apparaissent également pas dans une recherche *Google Image*, à l'inverse des captures d'écran.

6. Le manque d'exemples réalistes

Pour les projets basés sur du code, l'analogue des captures

d’écran sont de bons et solides exemples du code en action. Ces exemples ne devraient pas être abstraits, mais directement issus du monde réel. Ne créez pas d’exemples bateaux plein de « nom de la démo ici » et lorem ipsum. Prenez le temps de créer des exemples signifiants avec une histoire d’utilisateur qui représente la façon dont votre logiciel résout un problème.

Il y a de bonnes raisons de vous embêter avec des problèmes de maths en classe. Ils permettent d’appliquer ce que vous avez appris.

Disons que j’ai écrit un module d’un robot Web, et que j’explique la méthode follow_link. Je pourrais montrer la définition de la méthode ainsi :

```
$mech->follow_link( text_regex => $regex_object, n => $link_index );
```

Mais admirez à quel point cela devient évident en ajoutant de la réalité dans l’exemple.

```
# Suit le 2e lien où la chaîne de caractères « download » apparait
$mech->follow_link( text_regex => qr/download/, n => 2 );
```

Les noms des variables $regex_object et $link_index sont maintenant compréhensibles par le lecteur.

Bien entendu, vos exemples ne doivent pas être aussi brefs. Comme Rich Bowen du projet Apache le souligne, « Un exemple correct, fonctionnel, testé et commenté l’emporte sur une page de prose, à chaque fois. »

Montrez autant que possible. L’espace n’est pas cher. Créez une section dédiée aux exemples dans la documentation, ou même un livre de cuisine. Demandez aux utilisateurs d’envoyer du code qui fonctionne, et publiez leurs meilleurs exemples.

7. Liens et références inadéquats

Vous avez les hyperliens. Utilisez-les.

Ne pensez pas, parce que quelque chose est expliquée dans une certaine partie de la documentation, que le lecteur a déjà lu cette partie, ou bien qu'il sait où elle se trouve. Ne vous contentez pas de signaler que cette partie du code manipule des objets frobbitz. Expliquez brièvement lors du premier usage de ce terme ce qu'est un objet frobbitz, ou donnez le lien vers la section du manuel l'expliquant. Encore mieux, faites les deux !

8. Oublier les nouveaux utilisateurs

Il arrive trop souvent que l'écriture de la documentation soit rédigée à partir du point de vue de son auteur, alors que es nouveaux utilisateurs ont besoin de documentation d'introduction pour les aider.

L'introduction devrait être une page séparée de la documentation, idéalement avec des exemples qui permettent à l'utilisateur de réussir quelques manipulations avec le logiciel. Pensez à l'excitation que vous ressentez quand vous commencez à jouer avec un nouveau logiciel et qu'il vous permet de faire quelque chose de cool. Faites que ça arrive aux nouveaux utilisateurs également.

Par exemple, un package graphique pourrait présenter une série de captures d'écran qui montrent comment ajouter des données dans un fichier, comment faire intervenir le grapheur, et ensuite montrer les graphes obtenus. Une bibliothèque de codes pourrait montrer quelques exemples d'appels à la bibliothèque, et montrer le résultat obtenu. Pensez simplicité. Offrez une victoire facile. Le texte devrait introduire les termes aux endroits appropriés, avec des liens vers une documentation plus détaillée sur le long terme.

Un document de démarrage séparé donne à l'utilisateur une

compréhension rapide du logiciel. Il garde aussi les explications d'introduction en dehors de la partie principale de votre documentation.

9. Ne pas écouter les utilisateurs

Les développeurs doivent écouter les utilisateurs de la documentation. La chose évidente est d'écouter les suggestions et requêtes des personne qui utilisent activement votre logiciel. Quand un utilisateur prend le temps d'écrire un mail ou de poster quelque chose comme « ça aurait pu m'aider à mieux installer le programme s'il y avait eu une explication ou des liens au sujet des pilotes de la base de données », prenez ce message au sérieux. Pour chaque utilisateur vous envoyant un mail pour un problème, vous devez vous attendre à ce que dix utilisateurs silencieux aient le même problème.

Il est important d'écouter les problèmes des utilisateurs et d'en chercher les causes. S'ils ont souvent des problèmes pour effectuer des mises à jour groupées de bases de données, la première chose à faire est d'ajouter une question à la FAQ (vous avez bien une FAQ, n'est-ce pas ?) qui traite de ces questions-là. Cependant, la question peut aussi indiquer que la section traitant des mises à jour de base de données n'est pas assez claire. Ou peut-être qu'il n'y a pas de référence à cette section depuis la vue d'ensemble introductive du document, avec pour conséquence que vos utilisateurs ne pensent jamais à lire le reste du manuel.

En plus d'aider plus de gens à découvrir à quel point votre projet est utile, ça diminuera aussi la frustration de la communauté déjà existante. Si votre liste de diffusion, forum ou canal IRC est remplie de personnes qui posent toutes les mêmes questions idiotes (ou pas si idiotes) au point que tout le monde devient lassé d'y répondre, sachez reconnaître que ce sont des questions récurrents pour la FAQ, et mettre les réponses à un endroit facile à trouver aidera tout le monde à se concentrer sur des choses plus amusantes.

Gardez aussi un œil sur les questions des forums externes. Consultez les sites comme StackOverflow régulièrement, et placez une Google Alert sur votre nom de projet pour être maintenu au courant des discussions concernant votre projet sur Internet.

10. Ne pas accepter les entrées des utilisateurs

Si votre projet a une base d'utilisateur assez grande, il peut être judicieux d'incorporer les commentaires des utilisateurs directement dans la documentation. Le meilleur exemple que j'ai pu voir est celui donné par PHP. Chaque page de la documentation permet aux utilisateurs authentifiés d'ajouter des commentaires sur la page, aidant ainsi à clarifier certains points ou ajoutant des exemples qui ne sont pas dans la documentation principale. L'équipe PHP laisse aussi le choix au lecteur de lire la doc avec ou sans les commentaires des autres utilisateurs.

Aussi pratique cela soit-il, cela nécessite de la maintenance. Les commentaires doivent être éliminés de temps en temps pour éviter la prolifération. Par exemple, la page de la documentation PHP sur comment lancer PHP depuis la ligne de commande inclut 43 commentaires d'utilisateurs qui remontent à 2001. Les commentaires écrasent la documentation principale. Les commentaires devraient être archivés ou supprimés, tout en incluant les points les plus importants dans la documentation principale.

Un wiki est également une bonne approche. Cependant, si votre wiki ne permet pas à l'utilisateur de télécharger toutes les pages en une seule grosse archive (cs. point n°3 ci-dessus), alors vos utilisateurs sont à la merci de votre connexion internet et du serveur hébergeant le projet.

11. Impossibilité de voir ce que fait le logiciel sans l'installer

Au minimum, chaque projet de logiciel nécessite une liste de

fonctionnalités et une page de captures d'écran pour permettre au potentiel utilisateur intéressé de savoir pourquoi il devrait l'essayer. Aidez l'utilisateur, comparant les différents paquets à utiliser, à voir pourquoi cela vaut la peine de prendre le temps de le télécharger et de l'installer.

Les images sont un bon moyen de faire cela. Votre projet devrait avoir une page « Captures d'écran » qui montre des exemples de l'outil en action (cf. point n°5 ci-dessus). Si votre projet se résume uniquement à du code, comme une librairie, alors il devrait y avoir une page d'exemples montrant ce code utilisant le projet.

12. S'appuyer sur la technologie pour votre rédaction

Trop souvent, les auteurs de logiciels utilisent des systèmes de documentation automatisés pour faire leur travail. Ce système automatisé rend les choses plus facile à maintenir, mais il ne supprime pas la nécessité d'un travail d'écriture humain.

Le pire des cas concerne le changelog, qui n'est rien de plus qu'un dump des messages de commit du système de gestion de version, mais sans un résumé qui l'explique. Un changelog devrait lister les nouvelles fonctionnalités, les problèmes résolus et les incompatibilités potentielles. Sa cible est l'utilisateur final. Un log de commit est pratique et simple à générer pour les personnes travaillant sur le projet, mais ce n'est pas ce dont l'utilisateur a besoin.

Jetez un œil à cette page de la documentation de Solarium, une interface PHP pour le moteur de recherche Solr. Tout d'abord, l'avertisemment prend la moitié supérieure de l'écran, ne donnant aucune information au lecteur. Ensuite, il n'y a vraiment rien de véritablement descriptif sur la page que la liste des noms de fonctions. Il n'y a aucune explication sur les différentes méthodes, ni de liens indiquant où trouver

l'explication. Les pages générées automatiquement sont jolies, et elles pourraient ressembler à de la documentation, mais elles n'en sont pas.

13. Arrogance et hostilité vis-à-vis de l'utilisateur

L'attitude du type RTFM (Read The Freaking Manual) est mauvaise pour votre projet et votre documentation.

C'est le summum de l'arrogance que de croire que tous les problèmes qui ont trait au fait que quelqu'un ne sache pas utiliser votre logiciel sont de la faute de l'utilisateur.

Même s'il est probablement vrai que les utilisateurs peuvent trouver leurs réponses dans votre documentation mais ne le font pas, il est stupide de penser que c'est la faute de l'utilisateur. Peut-être votre documentation est-elle mal écrite, ou difficile à lire, ou présente mal à l'écran. Peut-être avez-vous besoin d'améliorer la section « Mise en route » (lien #8 ci-dessus) qui explique ce que le logiciel a pour but de faire. Peut-être que certaines parties d'information nécessitent d'être répétées à de multiples endroits de la documentation.

N'oubliez pas que les nouveaux utilisateurs de votre logiciel peuvent arriver sur votre projet sans rien n'en savoir. Votre documentation doit faire de son mieux pour s'assurer que cette ignorance soit facilement résolue.

Synthèse

Je suis sûr que vous avez déjà eu affaire à quelques-uns de ces problèmes listés ci-dessous, et peut-être que pour d'autres vous n'y avez pas pensé. Faites-nous connaître les problèmes que vous avez rencontrés dans les commentaires ci-dessous, sachant qu'il ne s'agit pas de pointer du doigt certains projets en particulier.

Surtout, j'espère que si vous reconnaissez un problème dans la documentation de vos projets, vous prendrez la peine d'améliorer la situation. Heureusement, améliorer la documentation est une manière idéale de faire participer les nouveaux arrivants dans votre projet. On me demande souvent : « Comment puis-je commencer dans l'open source », et je recommande des améliorations dans la documentation comme une bonne manière de commencer.

Faites-en sorte que ce soit aussi facile que possible, pour les novices comme les plus anciens, de savoir où il est nécessaire de travailler la documentation. Créez une liste des tâches, par exemple dans votre système de suivi des bogues, qui explique ce qui a besoin d'être amélioré. Soyez précis dans ce que sont vos besoins. Ne vous contentez pas de dire que vous avez besoin d'exemples, sans plus de précision. Créez des tâches spécifiques, comme « ajoutez un code d'exemple sur le fonctionnement de la tâche X », « ajouter une capture d'écran du générateur de rapports » ou « ajouter des informations de dépendances au fichier README/LISEZ-MOI ». Les contributeurs souhaitent aider mais trop souvent ils ne savent pas par où commencer.

La documentation n'est pas la partie la plus glamour d'un projet open source, et pour la plupart d'entre nous ce n'est pas amusant. Mais sans une bonne documentation, les utilisateurs ne sont pas servis comme ils pourraient l'être, et votre projet en souffrira sur le long terme.

Crédit photo : Rosalux Stiftung (Creative Commons By)

Framanews : libérez vos flux ! (RIP Google Reader)

Le 1er juillet prochain (J-4, donc !), **Google Reader** fermera ses portes.

Lancé en 2005, ce service permettait aux utilisateurs d'organiser et de lire des flux d'actualités (appelés « flux RSS ») issus de multiples sites en un seul endroit.

Plusieurs dizaines (centaines ?) de milliers d'utilisateurs se retrouvent donc « victimes » de cette fermeture annoncée il y a trois mois. Cela nous amène à nous poser deux questions :

- Quelle confiance accorder à Google[1], qui centralise vos données en ligne ?
- Quelle réponse le monde du logiciel libre a-t-il à proposer aux utilisateurs « mis à la porte » par Google Reader ?

De nombreuses applications libres permettant de lire des flux RSS ont vu leur développement s'accélérer ces derniers mois. Certaines nous ont semblé être d'excellentes alternatives à Google Reader. Mais comment les faire connaitre au grand public ? Comment inciter les utilisateurs a tester et valider une solution libre, plutôt que de foncer tête baissée dans la gueule grande ouverte d'un autre service privé ? Feedly, Digg, Yahoo!, et même … AOL (!) sont sur les rangs pour exploiter vos données sous forme de publicité classique ou de revente à des tiers. Pour au final fermer le service dans quelques mois ?

À sa modeste échelle, Framasoft annonce donc la mise en place de **Framanews**, un service de lecture de flux RSS basé sur le logiciel libre Tiny Tiny RSS. Il ne s'agit pas ici d'en faire un « concurrent » de Google Reader, qui ne résoudrait pas la question de la centralisation des données, mais bien de proposer à tout un chacun de pouvoir évaluer une alternative libre et gratuite, sans publicité, sans exploitation de vos données personnelles et que vous pouvez vous-même installer (pour une académie, un centre de recherche, etc.).

Notez bien que le projet est en bêta, que les inscriptions s'ouvrent peu à peu (afin de nous permettre de dimensionner l'infrastructure technique), et que nous prévoyons d'améliorer la documentation sur l'installation[2].

Pour vous faire patienter, nous vous proposons ici une interview de **Luc**, le sympathique et dynamique bénévole[3] qui est en charge de la mise en place de ce service.

Bonjour Luc, peux-tu te présenter ?

Bonjour. Mmh, c'est toujours dur de se présenter, mais je vais tenter quand même. Je suis un geek libriste de pas loin de 30 ans, grand fan des manchots, du Dr Who, de livres (romans, bds), du nombre 42 et des vannes pourries. On me connaît parfois sous le pseudo Sky sur le grand Ternet mais c'est plutôt rare (en dehors de LinuxFr ou de framalang, je ne sors pas beaucoup de mon lecteur de flux RSS)

Mon parcours fut assez mouvementé : 2 facs, 3 DUT, 1 Licence, clerc d'huissier, assistant de sénateur et maintenant administrateur systèmes et réseaux dans l'équipe Lothaire de l'Université de Lorraine… C'est moi qui ai appris à Jean-Claude Van Damme à faire le grand écart

Mon premier contact (sans le savoir) avec les logiciels libres date de l'époque où Free envoyait un cd contenant divers logiciels dont un truc qui s'appelait "Suite Mozilla" si je me souviens bien. Quand est sortie la première version de Firefox, j'y ai tout de suite adhéré, mais je n'étais pas encore prêt. C'est en 2005 qu'un ami d'enfance m'a dit « Essaye Linux, c'est vachement bien ! », ce qui m'a poussé à acheter un magazine contenant un cd d'installation d'OpenSuse. Là-dessus mon ami m'a dit « Pff, mais prends donc une Debian, ça déchire[4] ! ». Et là c'était fini, j'étais pris au piège et je n'ai plus quitté Debian, ni tout ce qui a rapport au libre.

3 ans plus tard, j'entrais en DUT d'info. Encore 5 ans de plus et j'organisais les Journées Perl 2013 (qui ont eu lieu à Nancy les 14 et 15 juin dernier).

Je fais actuellement partie de Lorraine Data Network, FAI associatif issu de l'essaimage de FDN qui milite pour un Internet Libre Décentralisé et Neutre en encourageant les gens à héberger eux-même leurs services, ou tout du moins à le faire chez des personnes de confiance… un peu comme quand Framasoft propose Framadate, Framapad, Framacalc et tous les autres Framaservices, non ?

Tu t'es proposé pour mettre en place et animer le projet Framanews. Mais qu'est-ce donc que Framanews ?

Framanews est un lecteur de flux RSS en ligne. Un flux RSS est un fichier contenant les articles du site du flux dans un format normalisé qui permet d'afficher ces articles dans un lecteur, sans tout l'« emballage » du site. Cela permet de suivre l'actualité du site en question, sans y aller, ou parfois d'avoir juste un résumé des articles, ce qui permet de choisir si ça vaut le coup d'aller faire un tour sur le site. Si un certain nombre de médias du Web parlent de la fin du flux RSS car dépassé par Twitter, Google+ et consorts, je trouve qu'au contraire, c'est un excellent moyen de choisir ses sources d'informations plutôt que se laisser enfermer dans un bulle constituée de « on sait mieux que toi ce qu'il te faut ». Je ne suis certainement pas le seul à penser ainsi, vu le tollé qu'a soulevé l'annonce de la fermeture de Google Reader et le nombre de lecteurs de flux libres qu'on a vu (re)surgir ça et là : Kriss Feed, Miniflux, Leed, etc. Et surtout Tiny Tiny RSS (ttrss pour les intimes) qui a vu son développement repartir de plus belle et qui sert de base à Framanews.

J'ai légèrement forké Tiny Tiny Rss pour le franciser au maximum (mais il y a encore des bouts de texte qui m'ont échappé), certains textes comme les emails ne passant pas par

le module d'internationalisation.

Mais Framanews, c'est aussi un projet « éducatif », pour (re)faire découvrir les flux RSS et présenter une alternative aux sites propriévateurs (*merge* de propriétaire et privateur, pour dérouter les trolls) comme (bientôt feu) Google Reader, Feedly et consorts. Le pourquoi du flux RSS, les spécificités de ttrss (interface mobile, partage de flux…), un mode d'emploi, tout ça est expliqué sur la page d'accueil du projet (surtout dans la FAQ).

Pourquoi avoir choisi ce projet-là, dans tous les framacartons[5] possibles ?

Parce que j'aime les flux RSS et que je suis un peu opportuniste : je me suis dit que la fermeture de GReader était une bonne occasion de prêcher la bonne parole du Libre. Aussi parce que je connais plutôt pas mal ttrss pour l'avoir installé pendant longtemps sur mon serveur. Je me sers de Framanews maintenant, pour voir les problèmes tout de suite et être encore plus motivé à les résoudre : vos problèmes sont aussi mes problèmes, soyez sûrs que je m'en occupe

> *Ah ! Non ! C'est un peu court jeune homme !*
> *On pouvait dire… oh ! Dieu ! … bien des choses en somme…*
> *En variant le ton, –par exemple, tenez :*
> *Agressif : « moi, monsieur, si j'avais un tel etherpad,*
>
> *Il faudrait sur le champ que je le mette à jour[6] ! »*
> *Amical : « mais il n'y a pas de css framasoft :*
> *laissez-moi donc vous faire un boilerplate ! »*

Et puis, il faut bien commencer quelque part

Techniquement, la mise en place a été plutôt difficile, peux-tu nous en dire plus sur les coulisses de ce projet ?

Oulà ! Alors, en ce moment, le ttrss tourne sur un des serveurs de Framasoft qui héberge d'autres services, avec la

base de données sur un autre serveur, qui sert aussi à faire tourner le script de mise à jour des flux. Je n'avais au départ que le serveur Framasoft pour jouer. J'ai utilisé une base MySQL puisqu'elle était déjà installée dessus, mais avec l'ouverture progressive de la bêta, j'ai vu que ça n'allait plus du tout. Le serveur souffrait de surcharge, et pourtant c'est une bête de course. J'ai donc tuné la base MySQL, mais les problèmes sont revenus quelques jours après. J'ai ensuite tenté quelques essais infructueux de conversion des données MySQL au format PostgreSQL pour une migration en douceur, mais j'ai dû me résoudre à demander à nos courageux testeurs de migrer eux-mêmes leurs comptes, à coup d'export des flux et des préférences. Après quelques jours de répit, de divers essais de réglage des paramètres du script de mise à jours, le serveur était de nouveau en surcharge. C'est Nassim Kacha – un ami lui aussi sysadmin qui s'occupe de pas mal de base de données au boulot – qui m'a montré que la surcharge était due à des accès disques trop lents. Framasoft m'a donc fourni un nouveau jouet : un vps (Serveur Privé Virtuel) avec un disque en SSD. Tout allait bien jusqu'à ce que certains utilisateurs abusent un peu du nombre de flux : plus de 5% du total de flux pour UN utilisateur (représentant 0,5% du nombre d'utilisateurs)…

Dallas, à côté de la saga Framanews, c'est Martine à la plage !

Donc, pour l'instant, le service reste en "beta" ? Quelles sont les limitations ?

Malheureusement, oui. Suite au dernier épisode (trop de flux pour certains utilisateurs), nous avons décidé de limiter le nombre de flux par personnes (je suis en train d'écrire un système de quota de flux pour ttrss). Le système de cache de ttrss a été un peu modifié pour garder le cache plus longtemps (ce qui réduit la vitesse de mise à jour) et on ouvre les inscriptions au compte-goutte, pour nous permettre d'augmenter les capacités de la plateforme au fur et à mesure. Je n'ai pas

envie que tout s'écroule de nouveau ! Une fois que j'aurais dimensionné correctement les besoins (un serveur = xxx utilisateurs), je vais tenter de transformer notre petite base de données en un cluster PostgreSQL, on repart pour des tests et on pourra enfin ouvrir les vannes en grand ! (ou pas)

Ceci dit, tant qu'on est en beta, je ne m'interdis pas de loucher vers d'autres applications de lecture de flux RSS en ligne qui pourraient mieux tenir la charge.

Si tout se passe bien au niveau technique, la prochaine limitation risque d'être le nombre de serveurs que Framasoft pourra louer. Rappelons-le, Framasoft est une association qui ne vit que par les dons de ses sympathisants. C'est pourquoi je vous invite à faire un petit tour sur http://soutenir.framasoft.org (je l'avais dit que j'étais opportuniste ! Hop, pub :D).

Au bout du compte, pourquoi utiliser Framanews plutôt que Feedly, Netvibes ou autre ?

C'te bonne blague ! Parce que c'est libre, tiens !

Mais aussi parce que Framasoft – et donc par définition Framanews aussi – cherche à libérer les internautes, en leur faisant découvrir des services qu'ils peuvent installer eux-mêmes, dans leur placard, sur leur serveur dédié, chez un hébergeur mutualisé associatif, sur un raspberry collé au dos de leur chat… De plus, nous respectons votre vie privée : la seule information dont on se sert, c'est votre adresse mail pour vous tenir au courant des évolutions du services et autres maintenances, et juste pour ça. Je pourrais aussi parler de la qualité de ttrss, de sa fonctionnalité qui permet de partager les articles que l'on aime sur un flux public[7], du superbe plugin que j'ai développé de mes blanches mains pour faciliter la navigation dans les flux (ok, c'est juste un fork d'un autre plugin)…

Je pense que la meilleure raison d'adopter Framanews, c'est de l'essayer et de comparer

Comment vois-tu l'avenir de ce projet ?

Moi et les autres membres de Framasoft sur une plage de sable blanc avec suffisamment d'argent pour racheter Google. Ah c'est pas payant ? Zut alors !

Je verrais bien un espace de partage des flux publics[8] des framanewseurs, un compteur des instances de ttrss que les gens auront montées parce qu'on leur en a donné envie…

Un petit mot pour la fin ?

Internet n'est pas compliqué, Internet est ce que vous en faites.

Rappel des principaux liens :

- Le site Framanews : http://framanews.org
- Les flux Twitter et identi.ca de Framasoft (pour se tenir au courant de l'annonce de nouveaux services) : http://twitter.com/framasoft http://identi.ca/framasoft
- Suivre les nouvelles de Framanews : blog Framacloud/Framanews, Flux RSS Framacloud/Framanews, hashtag #framanews

Crédit photo : Danny Sullivan (Creative Commons By)

Notes

[1] ou tout autre intermédiaire, Framasoft compris.

[2] Les utilisateurs sous Windows souhaitant tester le logiciel en standalone (sur leur poste de travail plutôt qu'en ligne) peuvent même télécharger notre WebApp TT-RSS, mise à jour pour l'occasion.

[3] S'il avait su dans quoi il mettait les doigts, il ne serait peut-être pas venu, d'ailleurs…

[4] Et c'est bien vrai !

[5] Les Framacartons ?! http://lite.framapad.org/p/framatools

[6] Oui, la mise à jour sur le champ a pris du retard à cause de Framanews, je sais, je sais.

[7] Twitter, c'est tellement 2012 !

[8] un flux public Framanews a une URL unique et tarabiscotée. Il faut que la personne vous la communique, sinon vous ne la trouverez jamais ! Par bonheur, les raccourcisseurs d'URLs existent, ce qui donne par exemple pour mon flux public : http://fiat-tux.fr/sh/LucPublRSS

Sortie du framabook #MonOrchide : le livre de l'été sera libre et lesbien !

Avec plus d'impatience encore qu'un(e) adolescent(e) guettant le prochain Harry Potter ou Twilight, nous attendions fébrilement la sortie du second roman de Pouhiou, suite de #Smartarded, que nous avions adoré lire et partager.

C'est désormais chose faite !

Il s'appelle **#MonOrchide**, poursuit donc le cycle des NoéNautes, et il y a toujours autant de sexe, drogues, rock'n'roll et chatons.

Rendez-vous sur le site Framabook pour en savoir plus (et

accéder au livre). En attendant, place à Pouhiou et ses plantes vertes :

Il a été rédigé dans les mêmes conditions que le premier et se retrouve donc plongé lui aussi directement dans le domaine public vivant.

Voici ce qu'il nous dit dans le dossier de presse original et percutant (avec de vraies-fausses critiques du livre de Télérama, Christine Boutin, Richard Stallman, Pascal Nègre et Eric Zemmour dedans !)

« Je ne suis pas libriste. Ce sont mes histoires qui, par nature, sont libres.

Devoir écrire quotidiennement m'a mené à faire face au processus créatif. L'inspiration m'est apparue comme une digestion remixant indifféremment tout ce que je pouvais expérimenter. Écrire implique de jouer avec l'imaginaire des lecteurices, avec leur façon de compiler, d'interpréter les mots dans leurs têtes. Même mon temps de création était libéré – d'une manière ou d'une autre – par une forme de solidarité.

Dès lors, mettre un péage entre l'histoire et celleux qui la font vivre m'est apparu absurde. De quoi le droit d'auteur est-il censé me protéger ? De l'attention donnée ?

Je vis dans une ère où le numérique permet un foisonnement de créations tel que nul ne peut tout suivre… Se couper du lectorat en restreignant l'accès à ce que j'écris, utiliser la loi comme une défiance (voire une arme), c'est une stratégie stupide, passéiste, digne d'un candide au pays des Bisounours !

Par contre, assumer le fait que ces histoires appartiennent à qui s'en empare (ne serait-ce qu'en les lisant), compter sur une forme de respect et faire vœu de non violence légale est

une attitude bien plus réaliste qui peut même s'avérer payante… »

-> **Lire le livre (en ligne et/ou après achat)…**

Principes internationaux pour le respect des droits humains dans la surveillance des communications

International Principles on the Application of Human Rights to Communications Surveillance

(Traduction : Slystone, tradfab, hugo, Pascal22, Hubert Guillaud, sinma, big f, Guillaume, Barbidule, Calou, Asta, wil_sly, chdorb, maugmaug, rou, RyDroid, + anonymes)

Version finale du 7 juin 2013

Alors que se développent les technologies qui leur permettent de surveiller les communications, les États ne parviennent pas à garantir que les lois et réglementations relatives à la surveillance des communications respectent les droits humains et protègent efficacement la vie privée et la liberté d'expression *(Ndt : le choix de traduire human rights par « droits humains » – plutôt que « droits de l'homme » – repose sur le choix délibéré de ne pas perpétuer une exception française sujette à caution.)*. Ce document tente d'expliquer comment le droit international des droits humains doit s'appliquer à l'environnement numérique actuel, à un moment où les technologies et les méthodes de surveillance des communications se généralisent et se raffinent. Ces principes peuvent servir de guide aux organisations citoyennes, aux entreprises et aux États qui cherchent à évaluer si des lois et des pratiques de surveillance, actuelles ou en discussion, sont en conformité avec les droits humains.

Ces principes sont le fruit d'une consultation globale d'organisations citoyennes, d'entreprises et d'experts internationaux sur les aspects juridiques, politiques et technologiques de la surveillance des communications.

Préambule

Le respect de la vie privée est un droit humain fondamental, indispensable au bon fonctionnement des sociétés démocratiques. Il est essentiel à la dignité humaine et renforce d'autres droits, comme la liberté d'expression et d'information, ou la liberté d'association. Il est consacré par le droit international des droits humains[1]. Les activités qui restreignent le droit au respect de la vie privée, et

notamment la surveillance des communications, ne sont légitimes que si elles sont à la fois prévues par la loi, nécessaires pour atteindre un but légitime et proportionnelles au but recherché[2].

Avant la généralisation d'Internet, la surveillance des communications par l'État était limitée par l'existence de principes juridiques bien établis et par des obstacles logistiques inhérents à l'interception des communications. Au cours des dernières décennies, ces barrières logistiques à la surveillance se sont affaiblies, en même temps que l'application des principes juridiques aux nouvelles technologies a perdu en clarté. L'explosion des communications électroniques, ainsi que des informations à propos de ces communications (les « métadonnées » de ces communications), la chute des coûts de stockage et d'exploration de grands jeux de données, ou encore la mise à disposition de données personnelles détenues par des prestataires de service privés, ont rendu possible une surveillance par l'État à une échelle sans précédent[3].

Dans le même temps, l'évolution conceptuelle des droits humains n'a pas suivi l'évolution des moyens modernes de surveillance des communications dont dispose l'État, de sa capacité à croiser et organiser les informations obtenue par différentes techniques de surveillances, ou de la sensibilité croissante des informations auxquelles il accède.

La fréquence à laquelle les États cherchent à accéder au contenu des communications ou à leurs métadonnées – c'est-à-dire aux informations portant sur les communications d'une personne ou sur les détails de son utilisation d'appareils électroniques – augmente considérablement, sans aucun contrôle approprié[4]. Une fois collectées et analysées, les métadonnées issues des communications permettent de dresser le profil de la vie privée d'un individu, tel que son état de santé, ses opinions politiques et religieuses, ses relations sociales et

ses centres d'intérêts, révélant autant de détails, si ce n'est plus, que le seul contenu des communications[5]. Malgré ce risque élevé d'intrusion dans la vie privée des personnes, les instruments législatifs et réglementaires accordent souvent aux métadonnées une protection moindre, et ne restreignent pas suffisamment la façon dont les agences gouvernementales peuvent les manipuler, en particulier la façon dont elles sont collectées, partagées, et conservées.

Pour que les États respectent réellement leurs obligations en matière de droit international des droits humains dans le domaine de la surveillance des communications, ils doivent se conformer aux principes exposés ci-dessous. Ces principes portent non seulement sur l'obligation pesant sur l'État de respecter les droits de chaque individu , mais également sur l'obligation pour l'État de protéger ces droits contre d'éventuels abus par des acteurs non-étatiques, et en particulier des entreprises privées[6]. Le secteur privé possède une responsabilité équivalente en termes de respect et de protection des droits humains, car il joue un rôle déterminant dans la conception, le développement et la diffusion des technologies, dans la fourniture de services de communication, et – le cas échéant – dans la coopération avec les activités de surveillance des États. Néanmoins, le champ d'application des présents principes est limité aux obligations des États.

Une technologie et des définitions changeantes

Dans l'environnement moderne, le terme « surveillance des communications » désigne la surveillance, l'interception, la collecte, le stockage, la modification ou la consultation d'informations qui contiennent les communications passées, présentes ou futures d'une personne, ainsi que de toutes les informations qui sont relatives à ces communications. Les « communications » désignent toute activité, interaction et échange transmis de façon électronique, tels que le contenu des communications, l'identité des parties communiquant, les

données de localisation (comme les adresses IP), les horaires et la durée des communications, ainsi que les identifiants des appareils utilisés pour ces communications.

Le caractère intrusif de la surveillance des communications est traditionnellement évalué sur la base de catégories artificielles et formelles. Les cadres légaux existants distinguent entre le « contenu » et le « hors-contenu », les « informations sur l'abonné » ou les « métadonnées », les données stockées et celles en transit, les données restant à domicile et celles transmises à un prestataire de service tiers[7]. Néanmoins, ces distinctions ne sont plus appropriées pour mesurer le niveau d'intrusion causé par la surveillance des communications dans la vie privée des individus. Il est admis de longue date que le contenu des communications nécessite une protection légale importante en raison de sa capacité à révéler des informations sensibles, mais il est maintenant clair que d'autres informations issues des communications d'un individu – les métadonnées et diverses informations autres que le contenu – peuvent révéler encore davantage sur l'individu que la communication elle-même, et doivent donc bénéficier d'une protection équivalente.

Aujourd'hui, ces informations, qu'elles soient analysées séparément ou ensemble, peuvent permettent de déterminer l'identité, le comportement, les relations, l'état de santé, l'origine ethnique, l'orientation sexuelle, la nationalité ou les opinions d'une personne ; ou encore d'établir une carte complète des déplacements et des interactions d'une personne dans le temps[8]., ou de toutes les personnes présentes à un endroit donné, par exemple une manifestation ou un rassemblement politique. En conséquence, toutes les informations qui contiennent les communications d'une personne, ainsi que toutes les informations qui sont relatives à ces communications et qui ne sont pas publiquement et facilement accessibles, doivent être considérées comme des « informations protégées », et doivent en conséquence se voir

octroyer la plus haute protection au regard de la loi.

Pour évaluer le caractère intrusif de la surveillance des communications par l'État, il faut prendre en considération non seulement le risque que la surveillance ne révèle des informations protégées, mais aussi les raisons pour lesquelles l'État recherche ces informations. Si une surveillance des communications a pour conséquence de révéler des informations protégées susceptibles d'accroître les risques d'enquêtes, de discrimination ou de violation des droits fondamentaux pesant sur une personne, alors cette surveillance constitue non seulement une violation sérieuse du droit au respect de la vie privée, mais aussi une atteinte à la jouissance d'autres droits fondamentaux tels que la liberté d'expression, d'association et d'engagement politique. Car ces droits ne sont effectifs que si les personnes ont la possibilité de communiquer librement, sans l'effet d'intimidation que constitue la surveillance gouvernementale. Il faut donc rechercher, pour chaque cas particulier, tant la nature des informations collectées que l'usage auquel elles sont destinées.

Lors de l'adoption d'une nouvelle technique de surveillance des communications ou de l'extension du périmètre d'une technique existante, l'État doit vérifier préalablement si les informations susceptibles d'être obtenues rentrent dans le cadre des « informations protégées », et il doit se soumettre à un contrôle judiciaire ou à un mécanisme de supervision démocratique. Pour déterminer si les informations obtenues par la surveillance des communications atteignent le niveau des « informations protégées », il faut prendre en compte non seulement la nature de la surveillance, mais aussi son périmètre et sa durée. Une surveillance généralisée ou systématique a la capacité de révéler des informations privées qui dépassent les informations collectées prises individuellement, cela peut donc conférer à la surveillance d'informations non-protégées un caractère envahissant,

exigeant une protection renforcée[9].

Pour déterminer si l'État est ou non fondé à se livrer à une surveillance des communications touchant à des informations protégées, le respect de principes suivants doit être vérifié.

Les principes

Légalité: toute restriction au droit au respect de la vie privée doit être prévue par la loi. L'État ne doit pas adopter ou mettre en oeuvre une mesure qui porte atteinte au droit au respect de la vie privée sans qu'elle ne soit prévue par une disposition législative publique, suffisamment claire et précise pour garantir que les personnes ont été préalablement informées de sa mise en oeuvre et peuvent en anticiper les conséquences. Etant donné le rythme des changements technologiques, les lois qui restreignent le droit au respect de la vie privée doivent faire l'objet d'un examen régulier sous la forme d'un débat parlementaire ou d'un processus de contrôle participatif.

Objectif légitime : la surveillance des communications par des autorités étatiques ne doit être autorisée par la loi que pour poursuivre un objectif légitime lié à la défense d'un intérêt juridique fondamental pour une société démocratique. Aucune mesure de surveillance ne doit donner lieu à une discrimination sur le fondement de l'origine, du sexe, de la langue, de la religion, des opinions politiques, de la nationalité, de l'appartenance à un groupe social, de la richesse, de la naissance ou de tout autre situation sociale.

Nécessité : les lois permettant la surveillance des communications par l'État doivent limiter la surveillance aux éléments strictement et manifestement nécessaires pour atteindre un objectif légitime. La surveillance des communications ne doit être utilisée que lorsque c'est l'unique moyen d'atteindre un but légitime donné, ou, lorsque d'autres moyens existent, lorsque c'est le moyen le moins

susceptible de porter atteinte aux droits humains. La charge de la preuve de cette justification, que ce soit dans les procédures judiciaires ou législatives, appartient à l'État.

Adéquation : toute surveillance des communications prévue par la loi doit être en adéquation avec l'objectif légitime poursuivi.

Proportionnalité : la surveillance des communications doit être considérée comme un acte hautement intrusif qui interfère avec le droit au respect de la vie privée, ainsi qu'avec la liberté d'opinion et d'expression, et qui constitue de ce fait une menace à l'égard les fondements d'une société démocratique. Les décisions relatives à la surveillance des communications doivent être prises en comparant les bénéfices attendus aux atteintes causées aux droits des personnes et aux autres intérêts concurrents, et doivent prendre en compte le degré de sensibilité des informations et la gravité de l'atteinte à la vie privée.

Cela signifie en particulier que si un État, dans le cadre d'une enquête criminelle, veut avoir accès à des informations protégées par le biais d'une procédure de surveillance des communications, il doit établir auprès de l'autorité judiciaire compétente, indépendante et impartiale, que :

1. il y a une probabilité élevée qu'une infraction pénale grave a été ou sera commise ;
2. la preuve d'une telle infraction serait obtenue en accédant à l'information protégée recherchée ;
3. les techniques d'investigation moins intrusives ont été épuisées ;
4. l'information recueillie sera limitée à ce qui est raisonnablement pertinent au regard de l'infraction concernée et toute information superflue sera promptement détruite ou restituée ;
5. l'information est consultée uniquement par l'instance spécifiquement désignée, et utilisée exclusivement aux

fins pour lesquelles l'autorisation a été accordée.

Si l'État cherche à avoir accès à des informations protégées via une surveillance des communications à des fins qui ne placeront pas une personne sous le risque de poursuites pénales, d'enquête, de discrimination ou de violation des droits de l'homme, l'État doit établir devant une autorité indépendante, impartiale et compétente que :

1. d'autres techniques d'investigation moins intrusives ont été envisagées ;
2. l'information collectée sera limitée à ce qui est raisonnablement pertinent, et toute information superflue sera promptement détruite ou restituée à la personne concernée ;
3. l'information est consultée uniquement par l'instance spécifiquement désignée, et utilisée exclusivement aux fins pour lesquelles l'autorisation a été accordée.

Autorité judiciaire compétente : les décisions relatives à la surveillance des communications doivent être prises par une autorité judiciaire compétente, impartiale et indépendante. L'autorité doit être (1) distincte des autorités qui effectuent la surveillance des communications, (2) au fait des enjeux relatifs aux technologies de la communication et aux droits humains, et compétente pour rendre des décisions judiciaires dans ces domaines, et (3) disposer de ressources suffisantes pour exercer les fonctions qui lui sont assignées.

Le droit à une procédure équitable : Une procédure équitable suppose que les États respectent et garantissent les droits humains des personnes en s'assurant que les procédures relatives aux atteintes aux droits humains sont prévues par la loi, sont systématiquement appliquées et sont accessibles à tous. En particulier, pour statuer sur l'étendue de ses droits humains, chacun a droit à un procès public dans un délai raisonnable par un tribunal établi par la loi, indépendant, compétent et impartial[10] sauf cas d'urgence lorsqu'il y a un

risque imminent de danger pour une vie humaine. Dans de tels cas, une autorisation rétroactive doit être recherchée dans un délai raisonnable. Le simple risque de fuite ou de destruction de preuves ne doit jamais être considéré comme suffisant pour justifier une autorisation rétroactive.

Notification des utilisateurs : les personnes doivent être notifiées d'une décision autorisant la surveillance de leurs communications, avec un délai et des informations suffisantes pour leur permettre de faire appel de la décision, et elles doivent avoir accès aux documents présentés à l'appui de la demande d'autorisation. Les retards dans la notification ne se justifient que dans les cas suivants :

1. la notification porterait gravement atteinte à l'objet pour lequel la surveillance est autorisée, ou il existe un risque imminent de danger pour une vie humaine ; ou
2. l'autorisation de retarder la notification est accordée par l'autorité judiciaire compétente conjointement à l'autorisation de surveillance ; et
3. la personne concernée est informée dès que le risque est levé ou dans un délai raisonnable, et au plus tard lorsque la surveillance des communications prend fin.

À l'expiration du délai, les fournisseurs de services de communication sont libres d'informer les personnes de la surveillance de leurs communications, que ce soit de leur propre initiative ou en réponse à une demande.

Transparence : les États doivent faire preuve de transparence quant à l'utilisation de leurs pouvoirs de surveillance des communications. Ils doivent publier, a minima, les informations globales sur le nombre de demandes approuvées et rejetées, une ventilation des demandes par fournisseurs de services, par enquêtes et objectifs. Les États devraient fournir aux individus une information suffisante pour leur permettre de comprendre pleinement la portée, la nature et l'application des lois autorisant la surveillance des

communications. Les États doivent autoriser les fournisseurs de service à rendre publiques les procédures qu'ils appliquent dans les affaires de surveillance des communications par l'État, et leur permettre de respecter ces procédures ainsi que de publier des informations détaillées sur la surveillance des communications par l'État.

Contrôle public : les États doivent établir des mécanismes de contrôle indépendants pour garantir la transparence et la responsabilité de la surveillance des communications[11]. Les instances de contrôle doivent avoir les pouvoirs suivants : accéder à des informations sur les actions de l'État, y compris, le cas échéant, à des informations secrètes ou classées ; évaluer si l'État fait un usage légitime de ses prérogatives ; évaluer si l'État a rendu publiques de manière sincère les informations sur l'étendue et l'utilisation de ses pouvoirs de surveillance ; publier des rapports réguliers ainsi que toutes autres informations pertinentes relatives à la surveillance des communications. Ces mécanismes de contrôle indépendants doivent être mis en place en sus de tout contrôle interne au gouvernement.

Intégrité des communications et systèmes : Afin d'assurer l'intégrité, la sécurité et la confidentialité des systèmes de communication, et eu égard au fait que toute atteinte à la sécurité pour des motifs étatiques compromet presque toujours la sécurité en général, les États ne doivent pas contraindre les fournisseurs de services, ou les vendeurs de matériels et de logiciels, à inclure des capacités de surveillance dans leurs systèmes ou à recueillir et conserver certaines informations exclusivement dans le but de permettre une surveillance par l'État. La collecte et le stockage des données a priori ne doivent jamais être demandés aux fournisseurs de services. Les personnes ont le droit de s'exprimer anonymement, les États doivent donc s'abstenir d'imposer l'identification des utilisateurs comme condition préalable pour l'accès à un service[12].

Garanties dans le cadre de la coopération internationale : en réponse aux évolutions dans les flux d'information et les technologies de communication, les États peuvent avoir besoin de demander assistance à un fournisseur de services étranger. Les traités de coopération internationale en matière de police et de justice et les autres accords conclus entre les États doivent garantir que, lorsque plusieurs droits nationaux peuvent s'appliquer à la surveillance des communications, ce sont les dispositions établissant la plus grande protection à l'égard des individus qui prévalent. Lorsque les États demandent assistance dans l'application du droit, le principe de double-incrimination doit être appliqué *(NdT : principe selon lequel, pour être recevable, la demande de collaboration doit porter sur une disposition pénale existant à l'identique dans les deux pays)*. Les États ne doivent pas utiliser les processus de coopération judiciaire ou les requêtes internationales portant sur des informations protégées dans le but de contourner les restrictions nationales sur la surveillance des communications. Les règles de coopération internationale et autres accords doivent être clairement documentés, publics, et conformes au droit à une procédure équitable.

Garanties contre tout accès illégitime : les États doivent adopter une législation réprimant la surveillance illicite des communications par des acteurs publics ou privés. La loi doit prévoir des sanctions civiles et pénales dissuasives, des mesures protectrices au profit des lanceurs d'alertes, ainsi que des voies de recours pour les personnes affectées. Cette législation doit prévoir que toute information obtenue en infraction avec ces principes est irrecevable en tant que preuve dans tout type de procédure, de même que toute preuve dérivée de telles informations. Les États doivent également adopter des lois prévoyant qu'une fois utilisées pour l'objectif prévu, les informations obtenues par la surveillance des communications doivent être détruites ou retournées à la personne.

Signataires

- Access Now
- Article 19 (International)
- Bits of Freedom (Netherlands)
- Center for Internet & Society (India)
- Comision Colombiana de Juristas (Colombia)
- Derechos Digitales (Chile)
- Electronic Frontier Foundation (International)
- Open Media (Canada)
- Open Net (South Korea)
- Open Rights Group (United Kingdom)
- Privacy International (International)
- Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (Canada)
- Statewatch (UK)

Notes

[1] Article 12 de la Déclaration universelle des droits de l'homme ; article 14 de la Convention des Nations Unies sur les travailleurs migrants ; article 16 de la Convention des Nations Unies sur la protection des droits de l'enfant ; pacte international relatif aux droits civils et politiques ; article 17 du pacte international relatif aux droits civils et politiques ; conventions régionales dont article 10 de la Charte africaine des droits et du bien-être de l'enfant, article 11 de la Convention américaine des droits de l'Homme, article 4 de la déclaration de principe de la liberté d'expression en Afrique, article 5 de la déclaration américaine des droits et devoirs de l'Homme, article 21 de la Charte arabe des droits de l'Homme et article 8 de la Convention européenne de la protection des droits de l'Homme et des libertés fondamentales ; principes de Johannesburg relatifs à la sécurité nationale, libre expression et l'accès à l'information, principes de Camden sur la liberté d'expression et l'égalité.

[2] Article 29 de la Déclaration universelle des droits de l'homme ; commentaire général numéro 27, adopté par le Comité des droits de l'Homme sous l'article 40, paragraphe 4, par The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, du 2 novembre ; voir aussi de Martin Scheinin, « Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, » 2009, A/HRC/17/34.

[3] Les métadonnées des communications peuvent contenir des informations à propos de notre identité (informations sur l'abonné, information sur l'appareil utilisé), de nos interactions (origines et destinations des communications, en particulier celles montrant les sites visités, les livres ou autres documents lus, les personnes contactées, les amis, la famille, les connaissances, les recherches effectuées et les ressources utilisées) et de notre localisation (lieux et dates, proximité avec d'autres personnes) ; en somme, des traces de presque tous les actes de la vie moderne, nos humeurs, nos centres d'intérêts, nos projets et nos pensées les plus intimes.

[4] Par exemple, uniquement pour le Royaume-Uni, il y a actuellement environ 500 000 requêtes sur les métadonnées des communications chaque année, sous un régime d'auto-autorisation pour les agences gouvernementales, qui sont en mesure d'autoriser leurs propres demandes d'accès aux informations détenues par les fournisseurs de services. Pendant ce temps, les données fournies par les rapports de transparence de Google montrent qu'aux États-Unis, les requêtes concernant des données d'utilisateurs sont passées de 8 888 en 2010 à 12 271 en 2011. En Corée, il y a eu environ 6 millions de requêtes par an concernant des informations d'abonnés et quelques 30 millions de requêtes portant sur d'autres formes de communications de métadonnées en 2011-2012, dont presque toutes ont été accordées et exécutées. Les données de 2012 sont accessibles ici.

[5] Voir par exemple une critique du travail de Sandy Pentland, « Reality Minning », dans la Technology Review du MIT, 2008, disponible ici, voir également Alberto Escudero-Pascual et Gus Hosein « Questionner l'accès légal aux données de trafic », Communications of the ACM, volume 47, Issue 3, mars 2004, pages 77-82.

[6] Rapport du rapporteur spécial des Nations Unies sur la liberté d'opinions et d'expression, Frank La Rue, 3 juin 2013, disponible ici.

[7] « Les gens divulguent les numéros qu'ils appellent ou textent à leurs opérateurs mobiles, les URL qu'ils visitent et les adresses courriel avec lesquelles ils correspondent à leurs fournisseurs d'accès à Internet, et les livres, les courses et les médicaments qu'ils achètent à leurs boutiques en ligne… On ne peut présumer que toutes ces informations, volontairement divulguées à certaines personnes dans un but spécifique, sont, de ce seul fait, exclues de la protection du 4e amendement de la Constitution. » United States v. Jones, 565 U.S, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[8] « La surveillance à court terme des déplacements d'une personne sur la voie publique est compatible avec le respect de la vie privée », mais « l'utilisation de systèmes de surveillance GPS à plus long terme dans les enquêtes sur la plupart des infractions empiète sur le respect de la vie privée. » United States v. Jones, 565 U.S., 132 S. Ct. 945, 964 (2012) (Alito, J. concurring).

[9] « La surveillance prolongée révèle des informations qui ne sont pas révélées par la surveillance à court terme, comme ce que fait un individu à plusieurs reprises, ce qu'il ne fait pas, et ce qu'il fait à la suite. Ce type d'informations peut en révéler plus sur une personne que n'importe quel trajet pris isolément. Des visites répétées à l'église, à une salle de gym, à un bar ou à un bookmaker racontent une histoire que

ne raconte pas une visite isolée, tout comme le fait de ne pas se rendre dans l'un de ces lieux durant un mois. La séquence des déplacements d'une personne peut révéler plus de choses encore ; une seule visite à un cabinet de gynécologie nous en dit peu sur une femme, mais ce rendez-vous suivi quelques semaines plus tard d'une visite à un magasin pour bébés raconte une histoire différente. Quelqu'un qui connaîtrait tous les trajets d'une personne pourrait en déduire si c'est un fervent pratiquant, un buveur invétéré, un habitué des clubs de sport, un mari infidèle, un patient ambulatoire qui suit un traitement médical, un proche de tel ou tel individu, ou de tel groupe politique – il pourrait en déduire non pas un de ces faits, mais tous. » U.S. v. Maynard, 615 F.3d 544 (U.S., D.C. Circ., C.A.) p. 562; U.S. v. Jones, 565 U.S (2012), Alito, J., participants. « De plus, une information publique peut entrer dans le cadre de la vie privée quand elle est systématiquement collectée et stockée dans des fichiers tenus par les autorités. Cela est d'autant plus vrai quand ces informations concernent le passé lointain d'une personne. De l'avis de la Cour, une telle information, lorsque systématiquement collectée et stockée dans un fichier tenu par des agents de l'État, relève du champ d'application de la vie privée au sens de l'article 8 (1) de la Convention. » (Rotaru v. Romania, (2000) ECHR 28341/95, paras. 43-44.

[10] Le terme « Due process » (procédure équitable) peut être utilisé de manière interchangeable avec « équité procédurale » et « justice naturelle », il est clairement défini dans la Convention européenne pour les droits de l'Homme article 6(1) et article 8 de la Convention américaine relative aux droits de l'Homme.

[11] Le commissaire britannique à l'interception des communications est un exemple d'un tel mécanisme de contrôle indépendant. L'ICO publie un rapport qui comprend des données agrégées, mais il ne fournit pas de données suffisantes pour examiner les types de demandes, l'étendue de chaque demande

d’accès, l’objectif des demandes et l’examen qui leur est appliqué. Voir ici.

[12] Rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d’opinion et d’expression, Frank La Rue, 16 mai 2011, A/HRC/17/27, para 84.

Quelle entreprise peut encore faire confiance à Microsoft ? par Glyn Moody

Le titre se suffit à lui-même ici. On pourrait ajouter aux entreprises, les institutions et les particuliers, bref tout le monde.

Non content d’avoir été accusé par le passé de réserver dans Windows des portes dérobées à la NSA, non content d’être fortement suspecté de laisser les autorités américaines collecter nos données dans Skype, Microsft est maintenant soupçonné de différer la publication de ses patchs de sécurité pour en informer d’abord les mêmes autorités américaines !

Tout DSI normalement constiué(e) devrait lire cet article et en tirer avec sa direction ses propres conclusions.

Quelle entreprise peut encore faire confiance à Microsoft ?

How Can Any Company Ever Trust Microsoft Again?

Glyn Moddy – juin 2013 – Open Enterprise (Computer World)
(Traduction : Slystone, Luo, lamessen, Antoine, sinma, Pouhiou, Sky, Fe-lor, aKa, Asta, audionuma + anonymes)

Quels que soient les détails des récentes révélations sur l'espionnage de masse de la part des États-Unis fournis par Edward Snowden dans le Guardian, il y a déjà un énorme bénéfice collatéral. D'un côté, le gouvernement des États-Unis se replie sur lui-même, niant certaines allégations en offrant sa propre version de l'histoire. Cela, et pour la première fois, nous donne des détails officiels sur des programmes dont nous n'étions (au mieux) informés que par fuites et rumeurs, voire pas du tout. De plus, la précipitation indécente et l'histoire sans cesse changeante des autorités américaines est une confirmation, si elle était encore nécessaire, que ce que

Snowden a révélé est important – vous ne provoquez pas un tel tapage pour rien.

Mais peut-être encore plus crucial, d'autres journalistes, poussés par la honte et leur culpabilisation, ont finalement posé des questions qu'ils auraient dû poser des années voire des décennies plus tôt. Cela a abouti à une série d'articles extrêmement intéressants à propos de l'espionnage de la NSA, dont beaucoup contiennent des informations auxiliaires qui sont aussi intéressantes que l'histoire principale. Voici un bel exemple de ce qui est apparu durant le week-end sur le site de Bloomberg.

Entre autres choses, il s'agit de Microsoft, et d'évaluer dans quelle mesure ils ont aidé la NSA à espionner le monde. Bien sûr, cette crainte n'est pas nouvelle. Dès 1999, il était déjà dit que des portes dérobées avaient été codées dans Windows :

> *Une erreur d'inattention de programmeurs Microsoft a révélé qu'un code d'accès spécial préparé par l'agence nationale de sécurité étasunienne (NSA) avait été secrètement implémenté dans Windows. Le système d'accès de la NSA est implémenté sous toutes les versions de Windows actuellement utilisées, à l'exception des premières versions de Windows 95 (et ses prédécesseurs). La découverte suivait de près les révélations survenues un peu plus tôt cette année concernant un autre géant du logiciel étasunien, Lotus, qui avait implémenté une trappe « d'aide à l'information » pour la NSA dans son système Notes. Des fonctions de sécurité dans d'autres logiciels systèmes avaient été délibérément paralysées.*

Plus récemment, il y eut des craintes au sujet de Skype, racheté par Microsoft en mai 2011. En 2012, il y a eu des discussions pendant lesquelles on s'est demandé si Microsoft avait changé l'architecture de Skype pour rendre l'espionnage plus facile (l'entreprise a même un brevet sur l'idée). Les récentes fuites semblent confirmer que ces craintes étaient

bien fondées, comme le signale Slate :

> *Le scoop du Washington Post sur PRISM et ses possibilités présente plusieurs points frappants, mais pour moi un en particulier s'est démarqué du reste. The Post, citant une diapositive Powerpoint confidentielle de la NSA, a écrit que l'agence avait un guide d'utilisation spécifique « pour la collecte de données Skype dans le cadre du programme PRISM » qui met en évidence les possibilités d'écoutes sur Skype « lorsque l'un des correspondants utilise un banal téléphone et lorsque deux utilisateurs du service réalisent un appel audio, vidéo, font du chat ou échangent des fichiers. »*

Mais même cela devient dérisoire comparé aux dernières informations obtenues par Bloomberg :

> *D'après deux personnes qui connaissent bien le processus, Microsoft, la plus grande compagnie de logiciels au monde, fournit aux services de renseignement des informations sur les bogues dans ses logiciels populaires avant la publication d'un correctif. Ces informations peuvent servir à protéger les ordinateurs du gouvernement ainsi qu'à accéder à ceux de terroristes ou d'armées ennemies.*
>
> *La firme de Redmond basée à Washington, Microsoft, ainsi que d'autres firmes œuvrant dans le logiciel ou la sécurité, était au courant que ce genre d'alertes précoces permettaient aux États-Unis d'exploiter des failles dans les logiciels vendus aux gouvernements étrangers, selon deux fonctionnaires d'État. Microsoft ne demande pas et ne peut pas savoir comment le gouvernement utilise de tels tuyaux, ont dit les fonctionnaires, qui ne souhaitent pas que leur identité soit révélée au vu de la confidentialité du sujet.*
>
> *Frank Shaw, un porte-parole de Microsoft, a fait savoir que ces divulgations se font en coopération avec d'autres agences, et sont conçues pour donner aux gouvernements « une longueur d'avance » sur l'évaluation des risques et des*

mitigations.

Réfléchissons-y donc un moment.

Des entreprises et des gouvernements achètent des logiciels à Microsoft, se reposant sur la compagnie pour créer des programmes qui sont sûrs et sans risque. Aucun logiciel n'est complètement exempt de bogues, et des failles sérieuses sont trouvées régulièrement dans le code de Microsoft (et dans l'open source, aussi, bien sûr). Donc le problème n'est pas de savoir si les logiciels ont des failles, tout bout de code non-trivial en a, mais de savoir comment les auteurs du code réagissent.

Ce que veulent les gouvernements et les compagnies, c'est que ces failles soient corrigées le plus vite possible, de manière à ce qu'elles ne puissent pas être exploitées par des criminels pour causer des dégâts sur leurs systèmes. Et pourtant, nous apprenons maintenant que l'une des premières choses que fait Microsoft, c'est d'envoyer des informations au sujet de ces failles à de multiples agences, en incluant sans doute la NSA et la CIA. En outre, nous savons aussi que « ce type d'alerte précoce a permis aux U.S.A. d'exploiter des failles dans les logiciels vendus aux gouvernements étrangers »

Et rappelez-vous que « gouvernements étrangers » signifie ceux des pays européens aussi bien que les autres (le fait que le gouvernement du Royaume-Uni ait espionné des pays « alliés » souligne que tout le monde le fait). Il serait également naïf de penser que les agences de renseignement américaines exploitent ces failles « jour 0 » seulement pour pénétrer dans les systèmes des gouvernements ; l'espionnage industriel représentait une partie de l'ancien programme de surveillance Echelon, et il n'y a aucune raison de penser que les U.S.A. vont se limiter aujourd'hui (s'il y a eu un changement, les choses ont empiré).

Il est donc fortement probable que les faiblesses des produits Microsoft soient régulièrement utilisées pour s'infiltrer et pratiquer toutes sortes d'espionnage dans les gouvernements et sociétés étrangères. Ainsi, chaque fois qu'une entreprise installe un nouveau correctif d'une faille majeure provenant de Microsoft, il faut garder à l'esprit que quelqu'un a pu avoir utilisé cette faiblesse à des fins malveillantes.

Les conséquences de cette situation sont très profondes. Les entreprises achètent des produits Microsoft pour plusieurs raisons, mais toutes supposent que la compagnie fait de son mieux pour les protéger. Les dernières révélations montrent que c'est une hypothèse fausse : Microsoft transmet consciencieusement et régulièrement des informations sur la manière de percer les sécurités de ses produits aux agences américaines. Ce qui arrive à ces informations plus tard est, évidemment, un secret. Pas à cause du « terrorisme », mais parce qu'il est presque certain que des attaques illégales sont menées contre d'autres pays (et leurs entreprises) en dehors des États-Unis.

Ce n'est rien d'autre qu'une trahison de la confiance que les utilisateurs placent en Microsoft, et je me demande comment un responsable informatique peut encore sérieusement recommander l'utilisation de produits Microsoft maintenant que nous sommes presque sûrs qu'ils sont un vecteur d'attaques par les agences d'espionnage américaines qui peuvent potentiellement causer d'énormes pertes aux entreprises concernées (comme ce qui est arrivé avec Echelon).

Mais il y a un autre angle intéressant. Même si peu de choses ont été écrites à ce sujet – même par moi, à ma grande honte – un nouvel accord législatif portant sur les attaques en ligne est en cours d'élaboration par l'Union Européenne. Voici un aspect de cet accord :

> *Ce texte demandera aux États membres de fixer leur peine maximale d'emprisonnement à au moins deux ans pour les crimes*

> *suivants : accéder à ou interférer illégalement avec des systèmes d'informations, interférer illégalement avec les données, intercepter illégalement des communications ou produire et vendre intentionnellement des outils utilisés pour commettre ces infractions.*

« Accéder ou interférer illégalement avec des systèmes d'informations » semble être précisément ce que le gouvernement des États-Unis fait aux systèmes étrangers, dont probablement ceux de l'Union Européenne. Donc, cela indiquerait que le gouvernement américain va tomber sous le coup de ces nouvelles réglementations. Mais peut-être que Microsoft aussi, car c'est lui qui en premier lieu a rendu possible l'« accès illégal ».

Et il y a un autre aspect. Supposons que les espions américains utilisent des failles dans les logiciels de Microsoft pour entrer dans un réseau d'entreprise et y espionner des tiers. Je me demande si ces entreprises peuvent elles-mêmes se trouver accusées de toute sorte d'infractions dont elles ne savaient rien ; et finir au tribunal. Prouver son innocence ici risque d'être difficile, car en ce cas les réseaux d'entreprise seraient effectivement utilisés pour espionner.

Au final, ce risque est encore une autre bonne raison de ne jamais utiliser des logiciels de Microsoft, avec toutes les autres qui ont été écrites ici ces dernières années. Ce n'est pas uniquement que l'open source est généralement moins cher (particulièrement si vous prenez en considération le prix de l'enfermement livré avec les logiciels Microsoft), mieux écrit, plus rapide, plus sûr et plus sécurisé. Mais par-dessus tout, le logiciel libre respecte ses utilisateurs, les plaçant solidement aux commandes.

Cela vous ôte toute crainte que l'entreprise vous ayant fourni un programme donne en secret à des tiers la possibilité de

retourner contre vous ce logiciel que vous avez payé assez cher. Après tout, la plupart des résolutions des bogues dans l'open source est effectuée par des codeurs qui ont un peu d'amour pour l'autorité verticale, de sorte que la probabilité qu'ils donnent régulièrement les failles à la NSA, comme le fait Microsoft, doit être extrêmement faible.

Crédit photo : Cambodia4kidsorg (Creative Commons By)

Never work for money ? Du Libre dans une copie du BAC d'anglais !

Nous avons reçu ce mail qui nous a particulièrement touché.

Cela mérite une bonne note, non ?

Bonjour Framasoft,

Je m'appelle *XXX* et j'ai maintenant passé le BAC (en espérant l'avoir réussi pour décrocher l'INSA à Rouen). Il se trouve que l'un des sujets d'expression d'Anglais LV1[1] était :

"I once promised myself I would never work for money," (Document B, 1.12). How easy is it to stick to such a decision?

Fervent croyant en le logiciel libre que je suis, j'ai écrit un texte sur la culture libre et le logiciel libre. Je me permets aujourd'hui de vous en faire part.

Vous êtes bien sûr libre d'en faire ce que vous voulez, comme me le « corriger », me le commenter, le publier (message subliminal).

Cependant, je dois vous prévenir que comme le nom de votre association se trouve dans mon texte, le correcteur de doit

pas être capable de m'identifier, ce qui implique que soit l'hypothétique publication ne doit pas se trouver avant la date des résultats du BAC (5 juillet) ou que mon nom ne soit figuré nul part, du moins jusqu'aux résultats (si vous avez besoin d'un pseudonyme, utilisez « minijackson »)

Voici donc le contenu du dit texte, quelque peu altéré suite à une courte réflexion postérieure :

> *In our commercial society, where everybody is looking for a well-paid job, not too much painful, and maybe if possible that we like, is there a place for "not for money" works ?*
>
> *I would like to explain this issue through an underestimated and under-explained topic : the free culture.*
>
> *The free culture was at first named "free software" for it was applied to softwares only. But this situation has evolved and now is extent to books, pictures and musics.*
>
> *But what is it ? It is the idea of giving freely informations or culture. But this "free" doesn't mean "free" like in "free shipping", but "free" like in "freedom" or "free speech".*
>
> *It gives the person the ability to share, remix and share the remix of a piece of culture. It is very rare to see an artist giving the ability to share and remix his piece of work. And so was created the community of free culture.*
>
> *Concerning the free softwares, developers works hard to give a good software knowing that they do not work for money. How do they do? There is mainly three cases : Either the developer has a work and spend his free time developing, or the person works for a non-profit organization that provides free software(s) like Mozilla or The Linux Foundation.*
>
> *But it is very rare to see someone living with donations only. It is also very hard for free software developers because of organizations like Microsoft or Apple who makes*

> *everything to make the user believe that they are the only ones who can make such products.*
>
> *But it isn’t true. Every free software developers works hard to give free and best softwares with one goal : make an open world.*
>
> *Windows and Mac are beaten by Linux, Microsoft Office is beaten by LibreOffice and Internet Explorer is beaten by Firefox.*
>
> *Some associations are also trying to spread the word, getgnulinux or Framasoft.*
>
> *Finally I would say that it is always hard to stick to that promise but we are trying. And because we are a huge community we will succeed.*

En espérant que cela vous plaise et que je n’aie pas écrit de bêtises, toute critique constructive est acceptée avec plaisir.

Merci et bonne continuation,

minijackson

Crédit photo : Official U.S. Navy Imagery (Creative Commons By)

Notes

[1] Le sujet dans son intégralité sur Sribd.

Sortie du documentaire Terms And Conditions May Apply

Terms And Conditions May Apply, est le titre d'un documentaire qui semble tout aussi intéressant que salutaire, a fortiori après l'affaire PRISM.

Lorsque l'on crée *gratuitement* un compte sur Google, YouTube, Facebook, Twitter, Amazon (dont la typographie compose le titre de l'image ci-dessous), on accepte également de souscrire à un contrat d'utilisation qui, s'il était lu et compris jusqu'au bout, devrait normalement nous faire rebrousser chemin.

Mais comme « personne ne lit ces contrats » et que « tout le monde se trouve sur ces réseaux sociaux », alors on participe nous aussi à nourrir ces *monstres* qui sucent en toute légalité nos données.

En attendant sa sortie le mois prochain, nous en avons traduit l'accueil sur le site officiel. Et peut-être même, qui sait, que nous participerons à son sous-titrage.

Termes et conditions applicables

Terms And Conditions May Apply

(Traduction : Lamessen, sinma, calou, Asta)

En cliquant sur le bouton de la page précédente, vous avez accepté de regarder la bande-annonce suivante :