Quand on touche à la vie privée, c'est la démocratie qui est menacée (2/3)

Voici enfin la suite des conférences d'Eben Moglen sur les révélations d'Edward Snowden. Pour vous remettre dans le bain, reportez-vous à la première partie. Ce texte a été publié avant que le Congrès des États-Unis ne refuse de proroger tels quels les amendements à la loi dite FISA (Foreign Intelligence Surveillance Act) donnant une grande latitude à la NSA pour surveiller les citoyens et résidents des États-Unis (la surveillance du reste de la planète restant inchangée).

Mais l'Union européenne et en particulier la France semblent suivre le chemin inverse ; il semble qu'elles n'aient rien appris des révélations de Snowden. Faites lire ce texte à vos proches, pour qu'à leur tour ils voient les conséquences de ce qui se trame et puissent nous aider à faire pression pour essayer d'éviter le pire.

Source : The Guardian, Privacy under attack: the NSA files revealed new threats to democracy

Traduction : Thérèse, fatalerrors (Geoffray Levasseur), goofy, audionuma, Diab, Paul, Omegax, lumi

> *En d'autres termes, le respect de la vie privée est requis pour l'exercice de l'autogouvernance démocratique. Les efforts tendant à soumettre la société humaine à ces méthodes de surveillance généralisée sont l'antithèse de la liberté. C'est la conversation que n'ont pas tenue tous ces « N'écoute pas mon téléphone portable ! » trompeurs [1]. Si cela ne tenait qu'aux gouvernements nationaux, le débat en resterait*

à ce niveau de charlatanisme pour toujours.

Le gouvernement des États-Unis et ses grandes oreilles n'ont pas avancé un seul argument pouvant nous convaincre que ce qu'il font est compatible avec l'éthique de la liberté, les lois constitutionnelles américaines ou les droits de l'homme internationaux. Au lieu de cela, ils essaient autant que possible de changer de sujet, et s'ils ne parviennent pas à en changer, à accuser le messager.

Personne n'a besoin d'accéder à des documents classés secrets pour voir comment les forces armées et les stratèges se sont adaptés à la fin de la Guerre froide en planifiant la surveillance invasive des sociétés du monde. Depuis le début des années 90, la documentation publique concernant la politique de défense américaine montre que les planificateurs et stratèges militaires avaient prévu un monde dans lequel les États-Unis n'auraient pas d'adversaire étatique significatif. Par conséquent, nous serions forcés de nous engager dans un ensemble de « conflits asymétriques », ce qui signifiait des « guérillas » impliquant des « acteurs non étatiques ».

Au cours de la redéfinition du comportement stratégique des États-Unis, les stratèges militaires et leurs collègues de la communauté du renseignement en sont venus à voir les droits américains à la vie privée dans les communications comme l'équivalent d'un asile pour les groupes terroristes. Ils étaient convaincus que les forces armées des États-Unis, les grandes oreilles, devraient nécessairement s'attaquer à ces asiles.

Puis, à l'avènement du 21e siècle, une administration américaine qui restera dans l'Histoire pour sa tendance à tirer d'abord et réfléchir ensuite a tout gobé – hameçon,

ligne et plomb [2] – du plan comportant « refus d'asile », surveillance invasive et « totale connaissance de l'information ». Dans un intervalle de temps vraiment court, depuis janvier 2002, principalement en secret, ils ont mis tout ça sur pied.

Les conséquences partout dans le monde n'ont pas été controversées, c'est à noter. Dans une large mesure, les États ont approuvé ou accepté. Après septembre 2001, le gouvernement des États-Unis a fait une démonstration de force tout à fait extraordinaire aux yeux du monde : vous étiez soit avec nous, soit contre nous. Par ailleurs, beaucoup d'autres gouvernements en étaient venus à fonder de manière capitale leurs propres services de renseignement sur la coopération avec les oreilles des États-Unis.

Une fois l'actuelle administration américaine bien installée, des responsables politiques de haut niveau ont considéré qu'il y avait un consensus multilatéral concernant les écoutes ayant pour objet les autres sociétés : elles ne pouvaient être arrêtées et donc ne devaient pas être limitées. Les Chinois ont approuvé. Les États-Unis ont approuvé. Les Européens ont approuvé ; leur position était quelque peu réticente, mais ils étaient dépendants des écoutes effectuées par les États-Unis et n'avaient pas tellement le pouvoir d'objecter.

Personne ne l'a annoncé aux peuples du monde. Depuis la fin de la première décennie du 21ème siècle, un fossé s'est ouvert entre les droits que les peuples du monde pensent posséder et ceux qui ont été bradés par leurs gouvernements en contrepartie d'un renseignement qui n'est utile qu'aux gouvernements eux-même. Ce fossé est si profond, si fondamental pour la signification de la démocratie, que les opérateurs de ce système ont commencé à douter de sa légitimité – ce qu'ils auraient dû faire plus tôt.

Snowden a vu ce qui est arrivé aux autres lanceurs d'alerte et a agi en conséquence. Sa théorie politique est tout à fait

exacte et totalement cohérente. Il dit que l'existence de ces programmes, non révélée au peuple américain, est une violation fondamentale des valeurs démocratiques des États-Unis. Assurément, il ne peut y avoir d'argument pour le contester.

La position de Snowden est qu'un effort si global, si massivement puissant et si propice aux abus ne devrait pas être entrepris sans consentement démocratique. Il a exprimé à maintes reprises sa croyance que le peuple des États-Unis a le droit de donner ou refuser ce consentement *informé*. Mais Snowden a également identifié le fait de soumettre la population mondiale à ces programmes comme une action problématique méritant une forme d'analyse morale et éthique qui va bien au-delà de la simple raison d'État [3].

Snowden veut dire, je pense, que nous devrions prendre ces décisions, non pas dans l'intérêt étroit et égoïste d'une nation, mais avec un sens moral particulièrement élevé de ce qui est approprié de la part d'une nation qui voudrait se faire passer pour le symbole de la liberté aux yeux de l'humanité.

Nous pouvons parler, naturellement, des lois constitutionnelles des États-Unis et de l'importance de l'appareil législatif américain – règles, protections, droits, devoirs – avec le respect qui leur est dû. Mais il doit être clair dans notre esprit que, lorsque nous parlons des traditions constitutionnelles des États-Unis en matière de liberté et d'esclavage, nous ne parlons pas seulement de ce qui est écrit dans les livres de droit.

Nous sommes confrontés à deux affirmations – on les entend partout – qui résument bien les orientations contre lesquelles nous travaillons. La première dit : « C'est sans espoir, la vie privée n'existe plus, à quoi bon lutter ? » ; la seconde : « Je ne fais rien de mal, pourquoi devrais-je m'en soucier ? » Ce sont là les objections les plus significatives qui nous sont opposées lorsque nous faisons ce que nous savons devoir

faire.

Si nous ne faisons rien de mal,

alors nous avons le droit de résister

Tout d'abord, notre lutte pour la survie de la vie privée est loin d'être sans espoir. Snowden nous a décrit quelle protection était encore efficace. Son souci était de différencier les formes de communication en réseau définitivement corrompues et inutilisables, de celles qui sont mises en danger par les assauts continuels d'une agence dévoyée et de celles que, même avec son immense pouvoir, son poids financier, ses ambitions déplacées et ses efforts consciencieux, cette agence n'arrive pas à casser.

Le désespoir est seulement une maladie qu'ils veulent vous voir attraper, pas une maladie inéluctable.

Quant à la seconde affirmation, nous nous devons d'y répondre tout à fait clairement : « Si nous ne faisons rien de mal, alors nous avons le droit de résister. » Si nous ne faisons rien de mal, alors nous avons le droit de faire tout notre possible pour maintenir l'équilibre traditionnel entre nous et le pouvoir qui écoute. Nous avons le droit d'être invisibles. Nous avons le droit de parler de manière inaudible. Nous avons le droit de parler des langues qu'ils ne comprennent pas. Nous avons le droit de nous rencontrer aux endroits, aux moments et de la manière qui nous conviennent.

Nous avons une tradition constitutionnelle aux États-Unis contre les mandats de portée générale. Elle est née au 18e siècle pour de bonnes raisons. Nous limitons la capacité de l'État à perquisitionner des lieux et à saisir des objets à ce qu'un juge indépendant estime raisonnable d'autoriser.

Ce principe qui lui était cher, le Premier Congrès l'a placé dans notre Déclaration des droits parce qu'il était cher aux Nord-Américains britanniques ; parce qu'au cours du 18ème

siècle, ceux-ci avaient appris de quelle manière le pouvoir exécutif pouvait se servir des mandats de portée générale pour tout fouiller, partout, à la recherche d'une chose qui lui déplaisait et en forçant les pouvoirs locaux à l'y aider. Ce fut un problème au Massachusetts en 1761 [4] et cela resta un problème jusqu'à la fin de l'autorité britannique en Amérique du Nord. Et même alors le problème demeura parce que les présidents, sénateurs et *chancellors* (juges) étaient eux aussi sans scrupules dans leurs comportements. Thomas Jefferson aussi, comme le président actuel, a annoncé un jeu bien meilleur qu'il n'avait en réalité.

Ce principe est assez clair. Mais il n'y a que neuf votes à la Cour suprême des États-Unis, et ce sont les seuls qui comptent pour le moment [5]. Nous devons attendre de voir combien d'entre eux sont prêts à reconnaître la simple inconstitutionnalité d'un système scélérat beaucoup trop gros pour faire faillite. Mais puisque ces neuf votes sont les seuls qui ont de l'importance, le reste d'entre nous devons mener nos activités d'une autre façon.

La tradition constitutionnelle des États-Unis que nous admirons a principalement été établie par des personnes qui ont fui l'Europe et sont venues en Amérique du Nord pour être libres. Ce sont leurs activités politiques et intellectuelles que nous retrouvons traduites dans les documents qui ont construit la République.

Mais il y a une seconde tradition constitutionnelle. Elle fut établie par des personnes qui ont été amenées ici contre leur gré ou qui sont nées dans l'esclavage et ont dû fuir pour pouvoir être libre, ici même. Cette seconde tradition constitutionnelle est légèrement différente par sa nature de la première, même si elle a conduit, en fin de compte, à des conclusions similaires.

Fuir l'esclavage est une activité de groupe. Fuir l'esclavage requiert l'assistance de ceux qui pensent que l'esclavage est une mauvaise chose. Les gens, aux États-Unis, ont oublié ce que notre tradition constitutionnelle doit au contact entre des personnes qui avait besoin de fuir pour devenir libres et des personnes qui savaient qu'elles devaient les aider, parce que l'esclavage est mal.

Nous avons maintenant oublié que durant l'été 1854, quand Anthony Burns – qui avait fui l'esclavage depuis Richmond en Virginie – fut renvoyé en esclavage par un juge d'État agissant comme commissaire fédéral pour le *Second Fugitive Slave Act* [6], Boston dut être placée sous la loi martiale pendant trois jours entiers. Les troupes fédérales bordaient les rues alors que Burns était conduit sous escorte vers le port de Boston et placé à bord d'un bateau pour le renvoyer à l'esclavage. Si Boston n'avait pas été contenue par la force, il y aurait eu une émeute.

Quand Frederick Douglass a fui l'esclavage en 1838, il eut

l'aide de sa chère Anna Murray, qui lui envoya une partie de ses économies et les vêtements de marin qu'il porta. Il eut l'aide d'un marin noir libre qui lui donna des papiers d'identité. De nombreuses personnes prirent beaucoup de risques pour l'aider à atteindre New York.

Notre tradition constitutionnelle ne repose pas seulement sur les droits négatifs qui se trouvent dans la Déclaration des droits. Elle repose également sur l'histoire d'une lutte de la communauté, souvent illégale d'un point de vue formel, pour la liberté et contre l'esclavage. Cette partie de notre tradition dit que la libération du contrôle oppressif doit être accordée à tous les peuples, partout, comme un droit. Elle dit que l'esclavage est tout simplement immoral, qu'il ne peut être toléré, ni justifié par la peur du maître ou un besoin de sécurité.

Par conséquent, la tradition constitutionnelle que les Américains devraient défendre actuellement est une tradition qui va bien au-delà de toute limitation spatiale ou temporelle pouvant s'appliquer au quatrième amendement [7]. Le peuple des États-Unis ne doit pas se contenter de défendre le droit d'être libre des intentions oppressives du gouvernement national, il ne doit pas simplement se battre pour une chose qui est incarnée par la clause de procédure régulière [8] du quatorzième amendement. Nous devrions plutôt nous battre contre les processus totalitaristes ; car l'esclavage est mal. Parce que soumettre l'ensemble du genre humain à la surveillance du maître est mal. Parce que fournir l'énergie, l'argent, la technologie, le système pour assujettir la vie privée de tous dans le monde – pour détruire l'asile de la liberté de parole américaine – est mal.

Snowden nous a donné la chose la plus précieuse qu'un peuple jouissant de l'autonomie démocratique puisse avoir, l'information sur ce qui se passe. Si nous voulons exercer nos droits en tant que peuple autogouverné en exploitant les

informations qu'il nous a livrées, nous devons avoir clairement à l'esprit les fondements politiques de notre action. Elles ne se limitent pas seulement aux paroisses, ou aux nations, ou à ce que l'on trouve dans les archives des décisions de la Cour suprême.

Une nation conçue dans la liberté et dévouée à la proposition que tous les hommes sont nés égaux a réduit en esclavage des millions de personnes. Elle s'est lavée de ce péché dans une terrible guerre. Le peuple des États-Unis devrait en tirer la leçon et est appelé à le faire aujourd'hui.

chaque gouvernement doit subordonner ses écoutes domestiques

aux principes de l'État de droit

À la lumière de ce que nous savons grâce à Snowden, les citoyens, partout, doivent exiger deux choses de leur gouvernement. En premier lieu, nous devons dire à nos dirigeants « Vous avez la responsabilité, le devoir, de protéger nos droits en nous protégeant de l'espionnage venant de l'extérieur ». Tout gouvernement a cette responsabilité. Il doit protéger le droit de ses citoyens à être libres de la surveillance intrusive de masse d'autres États. Aucun gouvernement ne peut prétendre à la souveraineté et à la responsabilité à moins de tout mettre en œuvre, dans la mesure de son pouvoir et de ses moyens, pour garantir ce résultat.

En second lieu, chaque gouvernement doit subordonner ses écoutes domestiques aux principes de l'État de droit. L'arrogance monumentale des grandes oreilles et la stupidité de la dernière administration ont laissé le gouvernement des États-Unis dans un piège qui n'avait pas lieu d'être. Avant que la dernière administration n'affranchisse ses oreilles de la loi, le gouvernement américain aurait pu regarder le monde en face et proclamer que seules ses oreilles étaient soumises aux règles de l'État de droit. Cela aurait été une prétention

exacte. Mais pour presque rien, l'histoire s'en souviendra, ils ont jeté cela aux orties.

Aux citoyens américains revient une plus grande responsabilité. Le gouvernement projette l'immensité de son pouvoir dans la destruction de la vie privée au sein des autres sociétés du monde. Il le fait sans aucun contrôle ni supervision démocratique et son peuple doit l'arrêter. Le rôle des Américains comme symbole de liberté dans le monde n'exige rien de moins.

La liberté a été pourchassée tout autour du globe. L'Asie et l'Afrique l'ont expulsée depuis longtemps. L'Europe a été harcelée pour que cette liberté soit traitée comme une étrangère et le Royaume-Uni l'arrêterait à Heathrow s'il la voyait arriver. Le président des États-Unis a exigé que personne n'accepte la fugitive et il n'est peut-être que la présidente brésilienne, Dilma Rousseff, pour souhaiter préparer le moment venu un asile pour l'humanité.

Les dirigeants politiques du monde entier ont eu beaucoup de choses à dire depuis que Snowden a commencé ses révélations, mais pas une fois on n'a entendu une déclaration du genre « Je regrette d'avoir soumis mon propre peuple à ces procédés ». La chancelière allemande, malgré une réélection triomphale sans un nuage dans son ciel politique, n'est pas en position de dire « J'ai été d'accord avec les Américains pour autoriser l'interception de 40 millions d'appels téléphoniques par jour ; je veux juste qu'ils arrêtent d'écouter mon téléphone ! »

Les grandes oreilles américaines ont affaire à une crise politique allant bien au delà de ce qu'ils avaient pu imaginer. Elles n'apprécient pas d'apparaître au grand jour, ni même d'être simplement visibles. Elles ont perdu leur crédibilité auprès de l'industrie de la cybersécurité, car cette dernière a pris conscience qu'elles ont trahi leurs promesses implicites sur ce qu'elles ne pirateraient pas.

L'industrie de la finance mondiale est envahie de peur à la vue de ce qu'elles ont fait. Les autres agences du gouvernement des États-Unis, sur le soutien desquelles elles peuvent habituellement compter, les fuient.

ils sont en train de faire du net un espace de guerre perpétuelle

Nous n'aurons plus jamais un tel moment de désarroi politique dans le camp qui agit contre la liberté. Non seulement ils ont rendu ce problème évident pour tout le monde – non seulement ils ont fait des martyrs de nos camarades résidant à Fort Leavenworth [9], à l'ambassade d'Équateur à Londres [10] et dans un endroit secret de Moscou [11] – non seulement ils ont allumé un incendie qu'ils ne peuvent plus éteindre en pissant dessus, mais ils ont aussi perdu leur armure. Ils se tiennent devant nous dans la totalité de qui ils sont réellement. Il nous appartient de montrer que nous les reconnaissons pour ce qu'ils sont.

Ce qu'ils ont fait, c'est de créer un état de guerre permanent sur le net. Douze années d'une guerre qui semble sans fin ; ils sont en train de faire du net un espace de guerre perpétuelle. Nous devons imaginer à nouveau de quoi aurait l'air un Internet en paix – la cyberpaix. Les jeunes gens de par le monde qui travaillent en ce moment sur la théorie de la cyberpaix font le travail politique le plus important de notre temps. Il nous faudra désormais assurer ce que les démocraties assurent le mieux, la paix. Nous devons être disposés à déclarer la victoire et rentrer chez nous. Quand nous le ferons, nous laisserons derrière nous un Internet qui ne sera plus en état de guerre, un Internet qui n'utilisera plus la surveillance pour détruire la vie privée, fondement de la démocratie.

C'est une question de droit public international. Au final, c'est semblable à l'interdiction des armes chimiques ou des

mines antipersonnel, une question de traités de désarmement, une question de maintien de la paix.

La difficulté, c'est que nous n'avons pas seulement affaire à nos concitoyens, bons et patriotes, pour qui des élections sont un remède suffisant, mais également à une immense structure de surveillance privée qui est devenue réalité. Cette structure a tout à fait le droit d'exister dans un marché libre, mais elle génère maintenant un désastre écologique dont seuls les gouvernements ont bénéficié. Par conséquent nous ne devons pas seulement réfléchir à ce que sont nos politiques vis-à-vis des États mais également vis-à-vis des entreprises.

En fait, nous en sommes encore à un spectacle de marionnettes où les objets légitimes de la surveillance internationale – nommément les politiciens, chefs d'état, cadres de l'armée et diplomates – sont en train de pleurer en nous disant *qu'ils* ne devraient pas être écoutés. Comme s'ils étaient *nous* et avaient le droit d'être laissés tranquilles.

Et ceci, bien sûr, c'est ce qu'ils veulent. Ils veulent nous induire en erreur. Ils veulent que nous pensions qu'ils *sont* nous – qu'ils ne sont pas les personnes qui ont permis à tout ceci d'arriver, qui l'ont applaudi, qui en ont fait commerce.

Nous devons faire face aux problèmes que leurs duperies ont créés. Les grandes oreilles ont détruit la politique de liberté d'Internet du gouvernement des États-Unis. Ils ont eu une bonne main tant qu'ils ont pu jouer des deux côtés à la fois. Et à présent, nous avons des collègues et camarades partout dans le monde qui travaillent pour la liberté du net dans les sociétés dangereuses ; ils dépendent du support matériel et de l'assistance du gouvernement des États-Unis et ils ont maintenant toutes les raisons d'être effrayés.

Que se serait-il passé si les chemins de fer clandestins [12] avaient été constamment soumis à un effort de pénétration de

la part du gouvernement des États-Unis au nom de l'esclavage ? Que se serait-il passé si tous les livres des 500 dernières années avaient signalé leurs lecteurs à la maison mère ?

Lorsque nous décidons de donner des informations personnelles,

nous fragilisons également la vie privée d'autres personnes.

La mauvaise nouvelle pour les peuples de la planète, c'est que tout le monde nous a menti de manière éhontée pendant près de vingt ans. La bonne nouvelle, c'est que Snowden nous a dit la vérité.

Edward Snowden a révélé des problèmes auxquels nous devons trouver des solutions. La vaste organisation industrielle de surveillance qui s'est développée depuis 2001 n'aurait pas pu se construire sans les sous-traitants du gouvernement ni l'industrie de l'extraction de données. Tous deux sont impliqués dans une crise écologique causée par la surenchère industrielle. Nous avons échoué à saisir la nature de cette crise parce que nous avons mal compris la nature de la vie privée. Les entreprises ont cherché à profiter de notre confusion et les gouvernements en ont profité encore davantage, ce qui menace la survie même de la démocratie.

Dans ce contexte, nous devons nous souvenir que la vie privée concerne notre environnement social, pas les interactions isolées que nous avons individuellement avec d'autres. Lorsque nous décidons de donner des informations personnelles, nous

fragilisons également la vie privée d'autres personnes. Par conséquent, la vie privée est toujours une relation entre de nombreuses personnes, plutôt qu'une transaction entre deux d'entre elles.

Beaucoup de gens vous prennent de l'argent en occultant cette distinction. Par exemple, ils vous proposent des services de messagerie gratuits. En retour, ils vous demandent de les laisser lire tous vos messages. Leur objectif affiché est de vous envoyer des publicités. Ce n'est qu'un échange entre deux parties. Ou alors, ils vous offrent un hébergement gratuit pour vos communications sociales, puis ils observent tout ce que regarde tout le monde.

C'est pratique pour eux, mais frauduleux. Si vous acceptez cette supposée offre bilatérale de service de messagerie qui vous est fourni gratuitement pour autant qu'ils puissent tout lire, alors chaque personne qui correspond avec vous est soumise à ce marché. Si dans votre famille il y a quelqu'un qui reçoit ses messages avec Gmail, alors Google obtient une copie de toutes les correspondances de votre famille. Si un autre membre de votre famille reçoit ses messages à l'aide de Yahoo, alors Yahoo reçoit également les correspondances de toute votre famille.

Peut-être que déjà ce niveau de surveillance des messages de votre famille par des grandes entreprises est trop pour vous. Mais comme les révélations de Snowden ont pu le montrer, à la déconfiture des gouvernements et de ces entreprises, elles ont aussi partagé tout ces courriers avec le pouvoir – qui les achète, obtient des tribunaux des injonctions à les produire ou les vole – que cela leur plaise ou non.

Ce sera la même chose si vous décidez de vivre votre vie sociale sur un site Internet géré par un abruti qui surveille toute interaction sociale en gardant une copie de tout ce qui est dit et en regardant tout le monde regarder tous les autres. Si vous amenez de nouveaux « amis » vers ce service,

vous les attirez dans cette inspection dégueulasse, en les forçant à subir tout cela avec vous.

C'est un problème *écologique* parce que nos choix individuels aggravent l'état du groupe dans son ensemble. L'intérêt des entreprises de service, mais pas le nôtre, est de cacher cet aspect du problème et de se concentrer sur l'obtention de consentements individuels. D'un point de vue juridique, l'essence d'une transaction est le consentement. Si la vie privée est transactionnelle, votre consentement à l'espionnage est tout ce dont l'espion commercial a besoin. Mais si la vie privée est comprise correctement, le consentement est généralement hors sujet et se focaliser dessus est fondamentalement inapproprié.

En ce qui concerne la pureté de l'air et de l'eau, nous ne fixons pas les limites acceptables de pollution par consentement ; la société a établi des normes de propreté que tout le monde doit respecter. Les lois environnementales ne sont pas des lois de consentement. Mais pour ce qui est du respect de la vie privée, on nous a autorisés à nous faire des illusions ; ce qui est véritablement un sujet de réglementation environnementale nous a été vendu comme un simple problème de négociation bilatérale. Les faits montrent que ceci est totalement faux.

(à suivre…)

Notes

[1] Référence aux protestations de dirigeants politiques, notamment d'Angela Merkel.

[2] Il y a ici double référence ; *swallow something hook, line and sinker* pourrait se traduire en « gober n'importe quoi », mais aussi il y a référence au roman d'espionnage en trois parties, *Spy Hook*, *Spy Line* et *Spy Sinker* de Len Deighton.

[3] En français dans le texte.

[4] En 1761 eurent lieu les toutes premières révoltes d'une colonie britannique d'Amérique du Nord, suite au Navigation Act limitant le commerce colonial et à l'insistance du roi Charles II pour y établir l'église anglicane. Le roi réagira en ordonnant des perquisitions, saisies et exécutions massives. Ces révoltes seront considérés comme les prémisses de la Guerre d'Indépendance.

[5] Aux États-Unis, la Cour suprême n'est pas seulement la plus haute autorité judiciaire, elle statue également sur la constitutionnalité de la loi, comme le fait notre Conseil constitutionnel.

[6] « Deuxième loi sur les esclaves fugitifs » votée par le Congrès le 18 septembre 1850, annulée de facto par le vote du 13ème amendement en 1865 abolissant l'esclavage.

[7] Amendement fixant le cadre de la juridiction fédérale des États-Unis et les limites du droit de vote ou d'éligibilité, ainsi que l'invalidation de toutes dettes financières en rapport avec des activités de rébellion ou esclavagistes.

[8] *Due process clause* : cette clause interdit à l'État toute condamnation sans procédure judiciaire régulière.

[9] Lieu de détention de Chelsea Manning.

[10] Lieu de retranchement de Julian Assange.

[11] Résidence actuelle d'Edward Snowden.

[12] *Underground railroad* : réseaux de fuite des années 1850 pour les esclaves aux États-Unis.

Crédits images

- Eben Moglen par Doc Searls (CC-BY-2.0)

- François-Auguste Biard *Abolition de l'esclavage* (détail) – Domaine public
- Logo NSA inside par Bruce Sterling (CC-BY-2.0)

Ce que cache la gratuité des photos embarquées de Getty Images (et des autres)

Le Parisien nous annonce que YouTube a connu une panne mondiale hier soir 13 mars 2014, entraînant avec lui la pléthore de sites qui proposent ses vidéos à mêmes leurs pages web via le lecteur embarqué. On remarquera que pour *mieux* nous informer l'article en question intègre deux tweets (paresse de journaliste ?).

Vidéos YouTube, encarts Twitter, musiques Soundcloud, boutons Facebook… nos pages web deviennent de plus en plus souvent un *savant* mélange entre notre propre contenu et celui des autres, apporté *sur un plateau* par des multinationales à forte dominante américaine.

C'est pratique et gratuit. Il y a un juste à faire un copier/coller avec un bout de code pour que, ô magie, le contenu des autres apparaisse instantanément sur votre page, l'enrichissant ainsi à moindre frais.

Mais il y a un risque et un prix à payer. Le risque c'est que comme rien n'est éternel, le jour où YouTube, Facebook, Twitter… disparaîtront (si, si, ça leur arrivera à eux aussi), on se retrouvera avec des pages pleines de zones vides qui n'auront plus de sens. Avant de disparaître, ces sociétés en difficulté auront pris le soin de modifier le contenu même de

toutes ces (frêles) embarcations avec, qui sait, toujours plus de publicité. Elles en ont parfaitement le droit, c'est un accord tacite que vous signez avec elles lorsque vous recopiez leur code. Google peut ainsi très bien du jour au lendemain ne faire afficher qu'une seule et unique vidéo dans tous les milliards lecteurs YouTube embarqués avec, disons, une pub pour Coca-Cola : impact marketing garanti !

Quant au prix à payer il est lourd à l'ère de l'informatique post Snowden, c'est celui de **votre vie privée** car, comme on le verra plus bas, ces intégrations collectent de nombreuses informations vous concernant.

Ici donc c'est au tour de l'énorme banque Getty Images de vous proposer d'embarquer ses photos. Et vous avez le choix parmi… 35 millions d'images ! D'un côté cela rend service et sensibilise au respect du crédit, de la licence et du lien vers le document d'origine. De l'autre ça participe à la fameuse citation « si c'est gratuit, c'est que c'est vous le produit »…

À comparer avec ce qu'a fait la British Library, l'équivalent britannique de la BnF, en décembre dernier : verser 1 million d'images du domaine public en haute résolution sur Flickr. Un autre monde, un monde à défendre, promouvoir et encourager.

Getty Images autorise l'incorporation gratuite, mais quel en est le prix pour la vie privée ?

Getty Images Allows Free Embedding, but at What Cost to Privacy?

[MàJ du 8 mars 2016] Par recommandé reçu au siège de Framasoft le 07 mars 2016, la société GETTY IMAGE, par l'intermédiaire

de son conseil juridique, met Framasoft en demeure de supprimer la majeure partie des éléments du billet de blog présent sur cette page. Sont en particulier concernés les propos issus de la traduction de l'article de Parker Higgins de l'Electronic Frontier Foundation, intitulé « Getty Images Allows Free Embedding, but at What Cost to Privacy ? ». Le billet ayant été publié en mars 2014 (il y a deux ans !), le délai légal du délit de presse n'ayant pu être retenu, c'est sur le thème du dénigrement que s'attache le cabinet de conseil de GETTY IMAGE.
Nous aurions pu à notre tour nous tourner vers notre propre conseil, qui n'aurait pas manqué, par exemple, de relever les injonctions non conformes au droit présentes dans cette lettre, ou la grande faiblesse des arguments (intimidants en apparence).

Aller au bout d'une procédure se concluant très certainement en queue de poisson ? Cela aurait été de notre part une perte d'énergie, de temps et d'argent ; nous estimons que les généreux dons des contributeurs n'ont pas à servir à de vaines procédures portant sur l'image de telle ou telle société, gagne-pain laborieux de quelques conseils juridiques à défaut d'avoir de vraies causes à défendre.

Nous préférons donc censurer ce billet et laisser nos lecteurs juges de la teneur du courrier en question que nous reproduisons ici. Évidemment, les propos que nous supprimons sur cette page ne sortiront pas pour autant d'Internet, n'est-ce pas ?



Grâce à Wikileaks on a la confirmation que l'accord TPP est pire qu'ACTA

Merci à Wikileaks d'avoir révélé hier une version de travail tenue secrète de l'accord Trans-Pacific Strategic Economic Partnership, plus connu sous l'acronyme TPP.

La France ne faisant pas partie des pays directement concernés, on n'en parle pas beaucoup dans nos médias. Mais on sait depuis longtemps que ce sont les USA qui donnent le la dans tout ce qui touche au copyright international.

Plus que donner le la, ils dictent la loi. Et celle qui se prépare ici est tout simplement scélérate…

La fuite du chapitre sur la propriété intellectuelle du Partenariat Trans-Pacifique confirme que cet accord est pire qu'ACTA

TPP IP Chapter Leaked, Confirming It's Worse Than ACTA

Glyn Moody – 13 novembre 2013 – TechDirt.com
(Traduction : Barbidule, Penguin, Genma, MFolschette, baba, mlah, aKa, Alexis Ids, Scailyna, @paul_playe, Mooshka, Omegax)

par le service du pas-étonnant-que-le-secret-soit-si-bien-gardé

Cela fait longtemps que nous attendions une fuite majeure du Partenariat Trans-Pacifique (TPP) rédigé en secret ; grâce à Wikileaks, nous en avons enfin une (voir aussi directement le pdf). Le texte est long et lourd à lire, en partie à cause de toutes les parties entre parenthèses sur les points où les

négociateurs ne se sont pas encore mis d'accord. Même si le brouillon est assez récent – il est daté du 30 août 2013 – un grand nombre de ces points y restent ouverts. Heureusement, KEI a déjà rassemblé une analyse détaillée mais facilement compréhensible, que je vous encourage vivement à lire en entier. En voici un résumé :

> *Le document confirme les craintes sur le fait que les différentes parties sont prêtes à étendre les limites du droit de la propriété intellectuelle, et à restreindre les droits et libertés du consommateur.*
>
> *En comparaison des accords multilatéraux existants, l'accord du TPP sur la propriété intellectuelle propose l'octroi de nouveaux brevets, la création d'une propriété intellectuelle sur les données, l'extension des termes de protection pour les brevets et copyrights, l'accroissement des privilèges des ayants droit, et l'augmentation des peines pour infraction à la propriété intellectuelle. Le texte du TPP réduit le champ des exceptions pour tous les types de propriété intellectuelle. Négocié dans le secret, le texte proposé est néfaste pour l'accès au savoir, néfaste pour l'accès aux soins, et profondément néfaste pour l'innovation.*

Bien que de nombreux domaines soient concernés par les propositions de la copie de travail – l'accès aux soins vitaux seraient restreints, tandis que la portée des brevets serait étendue aux méthodes chirurgicales par exemple – les effets sur le copyright sont particulièrement significatifs et troublants :

> *Collectivement, les dispositions du droit d'auteur (dans le TPP) sont configurées de manière à étendre les termes du droit d'auteur de la convention de Berne au-delà de la vie plus 50 ans, créant de nouveaux droits exclusifs, et fournissant bon nombre de nouvelles directives spécifiques pour gérer le copyright dans l'environnement numérique.*

Voici quelques-unes des extensions de durée proposées :

> *Concernant les durées de copyright, le TPP définit les bases comme suit. Les États-Unis, l'Australie, le Pérou, Singapour et le Chili proposent une durée de 70 ans après la mort de l'auteur pour les personnes physiques. Pour des œuvres appartenant à une entreprise, les États-Unis proposent 95 ans de droits exclusifs, alors que l'Australie, le Pérou, Singapour et le Chili proposent 70 ans. Le Mexique veut une durée de 100 ans après la mort de l'auteur pour les personnes physiques et 75 ans après la mort de l'auteur pour des œuvres appartenant à une entreprise. Pour des travaux non publiés, les États-Unis veulent une durée de 120 ans.*

Un problème plus technique concerne l'utilisation du « test en trois étapes » qui agira comme une contrainte supplémentaire sur de possibles exceptions au copyright :

> *Dans sa forme actuelle, l'espace des exceptions tel que défini par le TPP est moins vaste et plus restrictif que celui du traité 2012 de l'OMPI à Pékin ou celui du traité 2013 de l'OMPI à Marrakech, et bien pire que l'accord ADPIC. Bien que cela implique des problèmes légaux complexes, les ramifications politiques sont simples. Les gouvernements auraient une marge de manœuvre plus restreinte pour évaluer les exceptions dans l'éducation, dans les citations, dans les affaires publiques, dans les actualités et dans les autres exceptions « spéciales » de la Convention de Berne ? Pourquoi un gouvernement voudrait-il abandonner son autorité générale pour réfléchir à l'aménagement de nouvelles exceptions, ou pour contrôler les abus des détenteurs de droits ?*

Ceci est un bon exemple de comment le TPP n'essaie pas seulement de changer le copyright en faveur de ceux qui veulent l'étendre au maximum, mais essaie aussi d'instaurer un copyright qui serait facile à renforcer à l'avenir. En voici un autre, dans lequel le TPP veut empêcher le retour à un

système de copyright qui nécessite une inscription – ce genre de système ayant été proposé comme un moyen de pallier aux problèmes qui surviennent à cause de la nature automatique de l'attribution du copyright :

> *Le TPP va au-delà de l'accord ADPIC pour ce qui est de l'interdiction de l'instauration de formalités pour le copyright. Bien que le problème des formalités puisse sembler être un problème facile à résoudre, il y a un bon nombre de flexibilités qui seront éliminées par le TPP. À l'heure actuelle, il est possible d'avoir des exigences de formalités pour des œuvres appartenant à la sphère nationale et d'imposer des formalités à de nombreux types de droits liés, incluant ceux protégés par la Convention de Rome. Ces dernières années, les créateurs et les théoriciens de la politique du copyright ont commencé à remettre en question les bénéfices de l'enregistrement des œuvres et autres formalités, en particulier à la lumière des problèmes liés aux durées de copyright étendues sur de nombreuses oeuvres orphelines.*

Comme vous pouvez vous en douter, le TPP demande à ce qu'il y ait des protections solides de type DRM ; mais ici encore, il cherche à rendre les choses pires qu'elles ne le sont déjà :

> *La section sur le droit d'auteur inclut également un long discours sur les mesures de protection technique, et en particulier, la création d'un motif de poursuites spécifique contre le fait de casser les mesures techniques de protection. Les USA veulent que ce motif de poursuites spécifique s'étende même aux cas où le droit d'auteur n'est pas applicable, comme par exemple les œuvres du domaine public, ou bien les données qui ne sont pas protégées par le droit d'auteur.*

Cela rendrait illégal le fait de contourner les DRM, même si ceux-ci sont appliqués à du contenu qui se trouve dans le

domaine public – les enfermant alors une fois de plus, de façon efficace et permanente. Enfin, il est intéressant de remarquer que dans la sous-section fixant les dommages et intérêts pour violation de copyright, on peut y lire ce qui suit :

> *Pour déterminer le montant des dommages et intérêts en vertu du paragraphe 2, les autorités judiciaires seront habilitées à examiner, entre autres, toute mesure légitime de valeur que le détenteur du droit soumet, ce qui peut comprendre les bénéfices perdus, la valeur des biens ou des services concernés, mesurée en se basant sur le prix du marché, ou sur le prix de vente au détail suggéré.*

C'est exactement la tournure qui a été utilisée pour ACTA, et qui a été retrouvée dans le récent accord de libre-échange entre l'UE et Singapour. Cela résume assez bien comment le TPP s'appuie directement sur ACTA, tandis que les autres mesures évoquées ci-dessus montrent comment il va bien au-delà et ce à plusieurs égards.

Voilà pour les mauvaises nouvelles. La bonne nouvelle, c'est que nous avons maintenant une version très récente de ce qui pourrait être la partie la plus controversée de l'accord. Dans les semaines à venir, nous sommes susceptibles de voir de nombreuses analyses détaillées exposant au grand jour le caractère ô combien pernicieux cet accord pour le public des pays participant aux négociations.

L'espoir étant qu'une fois qu'il en sera informé, il fera connaître son sentiment à ses représentants politiques comme il l'a fait avec SOPA et ACTA – et avec le même résultat final.

Geektionnerd : 11 milliards

Source :

- Les USA consacrent 11 milliards de dollars au déchiffrement des communications (Numerama)

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

Google et le gouvernement des États-Unis main dans la main selon Julian Assange

Qu'il est loin le temps où Google se résumait à deux étudiants dans leur garage…

Julian Assange nous expose ici les accointances fortes entre

Google et le gouvernement des États-Unis, ce qui devrait faire réflechir quiconque utilise leurs services.

Google et la NSA : Qui tient le « bâton merdeux » désormais ?

Google and the NSA: Who's holding the 'shit-bag' now?

Julian Assange – 24 août 2013 – The Stringer
(Traduction : gaetanm, GregR, LeCoyote, Peekmo, MalaLuna, FF255, La goule de Tentate, fbparis + anonymes)

On nous a révélé, grâce à Edward Snowden, que Google et d'autres sociétés technologiques étatsuniennes ont reçu des millions de dollars de la NSA pour leur participation au programme de surveillance de masse PRISM.

Mais quel est au juste le degré de connivence entre Google et

la *sécuritocratie* américaine ? En 2011 j'ai rencontré Eric Schmidt, alors président exécutif de Google, qui était venu me rendre visite avec trois autres personnes alors que j'étais en résidence surveillée. On aurait pu supposer que cette visite était une indication que les grands pontes de Google étaient secrètement de notre côté, qu'ils soutenaient ce pour quoi nous nous battons chez Wikileaks : la justice, la transparence du gouvernement, et le respect de la vie privée. Mais il s'est avèré que cette supposition est infondée. Leur motivation était bien plus complexe et, comme nous l'avons découvert, intimement liée à celle du département d'État des États-Unis *(NdT : l'équivalent du ministère des Affaires étrangères, que nous appellerons DoS par la suite pour Department of State)*. La transcription complète de notre rencontre est disponible en ligne sur le site de Wikileaks.

Le prétexte de leur visite était que Schmidt faisait alors des recherches pour un nouveau livre, un ouvrage banal qui depuis a été publié sous le titre *The New Digital Age*. Ma critique pour le moins glaciale de ce livre a été publiée dans le *New York Times* fin mai de cette année. En quatrième de couverture figure une liste de soutiens antérieure à la publication : Henry Kissinger, Bill Clinton, Madeleine Albright, Michael Hayden (ancien directeur de la CIA et de la NSA) et Tony Blair. Henry Kissinger apparaît aussi dans le livre, recevant une place de choix dans la liste des remerciements.

L'objectif du livre n'est pas de communiquer avec le public. Schmidt pèse 6.1 milliards de dollars et n'a pas besoin de vendre des livres. Ce livre est plutôt un moyen de se vendre auprès du pouvoir. Il montre à Washington que Google peut être son collaborateur, son visionnaire géopolitique, qui l'aidera à défendre les intérêts des USA. Et en s'alliant ainsi à l'État américain, Google consolide sa position, aux dépens de ses concurrents.

Deux mois après ma rencontre avec Eric Schmidt, WikiLeaks avait des documents en sa possession et un motif juridique

valable de contacter Hillary Clinton. Il est intéressant de noter que si vous appelez le standard du DoS et que vous demandez Hillary Clinton, vous pouvez en fait vous en rapprocher d'assez près, et nous sommes devenus plutôt bons à ce petit jeu-là. Quiconque a vu *Docteur Folamour* se souviendra peut-être de la scène fantastique où Peter Sellers appelle la Maison Blanche depuis une cabine téléphonique de la base militaire et se trouve mis en attente alors que son appel gravit progressivement les échelons. Eh bien une collaboratrice de WikiLeaks, Sarah Harrison, se faisant passer pour mon assistante personnelle, m'a mis en relation avec le DoS, et comme Peter Sellers, nous avons commencé à franchir les différents niveaux pour finalement atteindre le conseiller juridique senior de Hillary Clinton qui nous a dit qu'on nous rappellerait.

Peu après, l'un des membres de notre équipe, Joseph Farrell, se fit rappeler non pas par le DoS, mais par Lisa Shields, alors petite amie d'Eric Schmidt, et qui ne travaille pas officiellement pour le DoS. Résumons donc la situation : la petite amie du président de Google servait de contact officieux de Hillary Clinton. C'est éloquent. Cela montre qu'à ce niveau de la société américaine, comme dans d'autres formes de gouvernement oligarchique, c'est un jeu de chaises musicales.

Cette visite de Google pendant ma période de résidence surveillée se révéla être en fait, comme on le comprit plus tard, une visite officieuse du DoS. Attardons-nous sur les personnes qui accompagnaient Schmidt ce jour-là : sa petite amie Lisa Shields, vice-présidente à la communication du CFR (Council on Foreign Relations) ; Scott Malcolmson, ancien conseiller sénior du DoS ; et Jared Cohen, conseiller de Hillary Clinton et de Condoleezza Rice (ministre du DoS sous le gouvernement Bush fils), sorte de Henry Kissinger de la génération Y.

Google a démarré comme un élément de la culture étudiante

californienne dans la région de la baie de San Francisco. Mais en grandissant Google a découvert le grand méchant monde. Il a découvert les obstacles à son expansion que sont les réseaux politiques et les réglementations étrangères. Il a donc commencé à faire ce que font toutes les grosses méchantes sociétés américaines, de Coca Cola à Northrop Grumann. Il a commencé à se reposer lourdement sur le soutien du DoS, et, ce faisant il est entré dans le système de Washington DC. Une étude publiée récemment montre que Google dépense maintenant plus d'argent que Lockheed Martin pour payer les lobbyistes à Washington.

Jared Cohen est le co-auteur du livre d'Eric Schmidt, et son rôle en tant que lien entre Google et le DoS en dit long sur comment le « besoin intense de sécurité » des États-Unis fonctionne. Cohen travaillait directement pour le DoS et était un conseiller proche de Condolezza Rice et Hillary Clinton. Mais depuis 2010, il est le directeur de Google Ideas, son think tank interne.

Des documents publiés l'an dernier par WikiLeaks obtenus en sous-main via le sous-traitant US en renseignement Stratfor montrent qu'en 2011, Jared Cohen, alors déjà directeur de Google Ideas, partait en mission secrète en Azerbaïdjan à la frontière iranienne. Dans ces courriels internes, Fred Burton, vice-président au renseignement chez Stratfor et ancien officiel senior au DoS, décrivait Google ainsi :

« Google reçoit le soutien et la couverture médiatique de la présidence et du DoS. En réalité ils font ce que la CIA ne peut pas faire… Cohen va finir par se faire attraper ou tuer. Pour être franc, ça serait peut-être la meilleure chose qui puisse arriver pour exposer le rôle caché de Google dans l'organisation des soulèvements. Le gouvernement US peut ensuite nier toute implication et Google se retrouve à assumer le bordel tout seul. »

Dans une autre communication interne, Burton identifie par la

suite ses sources sur les activités de Cohen comme étant Marty Lev, directeur de sécurité chez Google, et… Eric Schmidt.

Les câbles de WikiLeaks révèlent également que, Cohen, quand il travaillait pour le Département d'État, était en Afghanistan à essayer de convaincre les quatre principales compagnies de téléphonie mobile afghane de déplacer leurs antennes à l'intérieur des bases militaires américaines. Au Liban il a secrètement travaillé, pour le compte du DoS, à un laboratoire d'idées chiite qui soit anti-Hezbollah. Et à Londres ? Il a offert des fonds à des responsables de l'industrie cinématographique de Bollywood pour insérer du contenu anti-extrémistes dans leurs films en promettant de les introduire dans les réseaux de Hollywood. C'est ça le président de Google Ideas. Cohen est effectivement de fait le directeur de Google pour le changement de régime. Il est le bras armée du Département d'État encadrant la Silicon Valley.

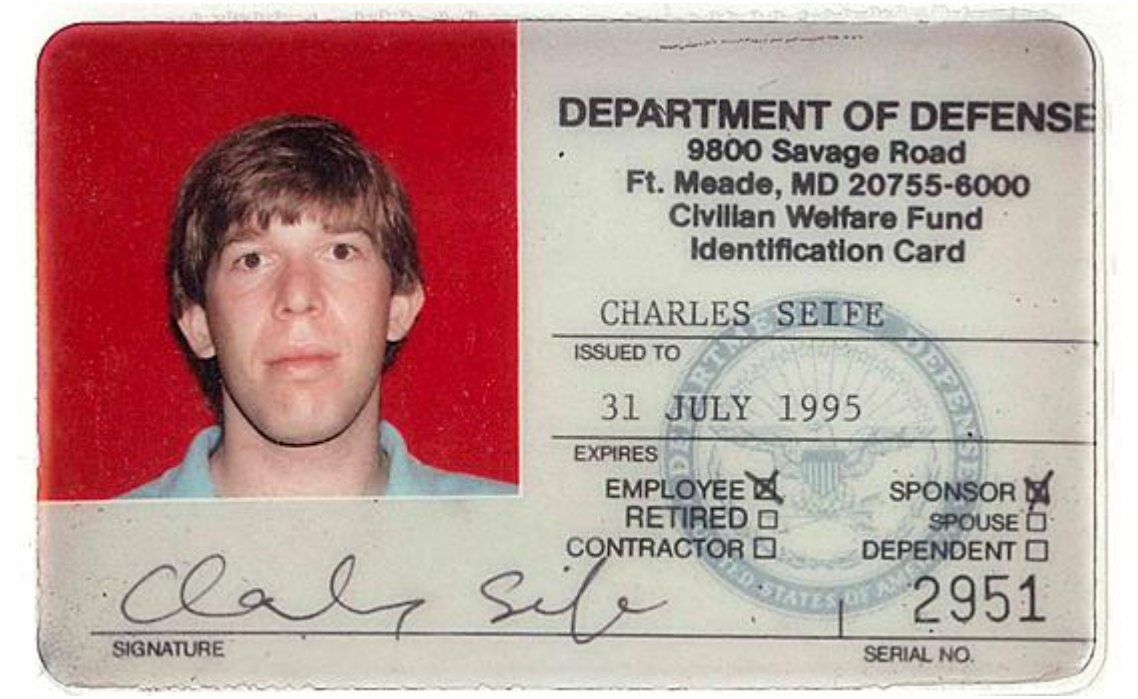
Que Google reçoive de l'argent de la NSA en échange de la remise de données personnelles n'est pas une surprise. Google a rencontré le grand méchant monde et il en fait désormais partie.

Crédit photo : NSA (Domaine Public – Wikimedia Commons)

Lettre ouverte à mes anciens collègues mathématiciens de la NSA

Quand un ancien employé de la NSA s'exprime, visiblement travaillé par sa conscience.

« Il est difficile d'imaginer que vous, mes anciens collègues, mes amis, mes professeurs… puissiez rester silencieux alors que la NSA vous a abusés, a trahi votre confiance et a détourné vos travaux. »



Lettre ouverte à mes anciens collègues de la NSA

Mathématiciens, pourquoi ne parlez-vous pas franchement ?

[An Open Letter to My Former NSA Colleagues]

Charles Seife – 22 août 2013 – Slate
(Traduction : Ilphrin, phi, Asta, @zessx, MFolschette, lamessen, La goule de Tentate, fcharton, Penguin + anonymes)

La plupart des personnes ne connaissent pas l'histoire du hall Von Neumann, ce bâtiment sans fenêtres caché derrière le Princeton Quadrangle Club. J'ai découvert cette histoire lors de ma première année quand, jeune étudiant passionné de mathématiques, je fus recruté pour travailler à la NSA (National Security Agency).

Le hall Von Neumann se situe à l'ancien emplacement du Institute for Defense Analyses, un organisme de recherches en mathématiques avancées travaillant pour une agence dont, à cette époque, l'existence était secrète. J'y découvris que les liens étroits entre l'université de Princeton et la NSA remontaient à plusieurs décennies, et que certains de mes professeurs faisaient partie d'une fraternité secrète composée de nombreux passionnés travaillant sur des problèmes mathématiques complexes pour le bien de la sûreté nationale. J'étais fier de rejoindre cette fraternité, qui était bien plus grande que ce que j'avais pu imaginer. D'après l'expert de la NSA James Bamford, cette agence est le plus grand employeur de mathématiciens de la planète. Il est presque sûr que n'importe quel département réputé de mathématiques a vu un de ses membres travailler pour la NSA.

J'ai travaillé à la NSA de 1992 à 1993 dans le cadre du programme d'été] qui attire les brillants étudiants en mathématiques à travers le pays, chaque année. Après obtention d'une accréditation de sécurité, incluant une session au détecteur de mensonge et une enquête d'agents du FBI chargée de glaner des informations sur moi dans le campus, je me suis présenté avec anxiété à Fort Meade (siège de la NSA), pour des instructions de sécurité.

Cela fait plus de vingt ans que j'ai reçu ces premières instructions, et une grande partie de ce que j'ai appris est maintenant obsolète. À l'époque, bien peu avaient entendu parler d'une agence surnommée « No Such Agency » *(NdT littéralement « pas de telle agence » ou l'agence qui n'existe pas)* et le gouvernement souhaitait que cela reste ainsi. On nous disait de ne pas dire un mot sur la NSA. Si une personne nous posait la question, nous répondions que nous travaillions pour le ministère de la Défense (DoD – Department of Defense). C'est d'ailleurs ce qui était marqué sur mon CV et sur une de mes cartes d'accès officielles de la NSA (cf ci-dessus).

De nos jours, il y a peu d'intérêt à procéder ainsi. L'agence

est sortie de l'ombre et fait régulièrement la Une des journaux. En 1992, on m'a appris que le code de classement des documents confidentiels était un secret bien gardé, que c'était un crime de le révéler à des personnes extérieures. Mais une simple recherche Google montre que les sites internet gouvernementaux sont parsemés de documents, qui furent en leur temps uniquement réservés aux personnes qui devaient le savoir.

Une autre chose qu'ils avaient l'habitude de dire est que la puissance de la NSA ne serait jamais utilisée contre les citoyens américains. À l'époque à laquelle j'ai signé, l'agence affirmait clairement que nous serions employés à protéger notre pays contre les ennemis extérieurs, pas ceux de l'intérieur. Faire autrement était contraire au règlement de la NSA. Et, plus important encore, j'ai eu la forte impression que c'était contraire à la culture interne. Après avoir travaillé là-bas pendant deux étés d'affilée, je croyais sincèrement que mes collègues seraient horrifiés d'apprendre que leurs travaux puissent être utilisés pour traquer et espionner nos compatriotes. Cela a-t-il changé ?

Les mathématiciens et les cryptoanalystes que j'ai rencontrés venaient de tout le pays et avaient des histoires très différentes, mais tous semblaient avoir été attirés par l'agence pour les deux mêmes raisons.

Premièrement, nous savions tous que les mathématiques étaient *sexy*. Ceci peut sembler étrange pour un non-mathématicien, mais outre le pur défi certains problèmes mathématiques dégagent quelque chose, un sentiment d'importance, de gravité, avec l'intuition que vous n'êtes pas si loin que ça de la solution. C'est énorme, et vous pouvez l'obtenir si vous réfléchissez encore un peu plus. Quand j'ai été engagé, je savais que la NSA faisait des mathématiques passionnantes, mais je n'avais aucune idée de ce dans quoi je mettais les pieds. Au bout d'une semaine, on m'a présenté un assortiment des problèmes mathématiques plus séduisants les uns que les

autres. Le moindre d'entre eux pouvant éventuellement être donné à un étudiant très doué. Je n'avais jamais rien vu de tel, et je ne le reverrai jamais.

La seconde chose qui nous a attirés, c'est du moins ce que je pensais, était une vision idéaliste que nous faisions quelque chose de bien pour aider notre pays. Je connaissais suffisamment l'Histoire pour savoir qu'il n'était pas très délicat de lire les courriers de son ennemi. Et une fois que je fus à l'intérieur, je vis que l'agence avait un véritable impact sur la sécurité nationale par de multiples moyens. Même en tant que nouvel employé, j'ai senti que je pouvais apporter ma pierre. Certains des mathématiciens les plus expérimentés que nous avions rencontrés avaient clairement eu un impact palpable sur la sécurité des États-Unis, des légendes presque inconnues en dehors de notre propre club.

Cela ne veut pas dire que l'idéalisme est naïf. N'importe qui ayant passé du temps de l'autre coté du miroir de ce jeu d'intelligence sait à quel point l'enjeu peut être important. Nous savions tous que les (vrais) êtres humains en chair et en os peuvent mourir à cause d'une violation apparemment mineure des secrets que nous nous somme vu confier. Nous réalisions également que le renseignement requiert parfois d'utiliser des tactiques sournoises pour essayer de protéger la Nation. Mais nous savions tous que ces agissements étaient encadrés par la loi, même si cette loi n'est pas toujours noire ou blanche. L'agence insistait, encore et encore, sur le fait que les armes que nous fabriquions, car ce sont des armes même si ce sont des armes de l'information, ne pourraient jamais être utilisées contre notre propre population, mais seulement contre nos ennemis.

Que faire, maintenant que l'on sait que l'agence a depuis trompé son monde ?

Nous savons maintenant que les appels téléphoniques de chaque client Verizon aux USA ont été détournés par l'agence en toute

illégalité alors qu'elle n'est justement pas supposée intervenir sur les appels qui proviennent et qui aboutissent aux États-Unis. Ce mercredi, de nouvelles preuves ont été révélées, montrant que l'agence a collecté des dizaines de milliers de courriels « complètement privés » n'ayant pas traversé les frontières. Nous savions que l'agence a d'importantes possibilités pour épier les citoyens des USA et le faisait régulièrement de manière accidentelle. Or nous disposons aujourd'hui d'allégations crédibles prouvant que l'agence utilise ces informations dans un but donné. Si les outils de l'agence sont réellement utilisés uniquement contre l'ennemi, il semble alors que les citoyens ordinaires en fassent dorénavant partie.

Aucun des travaux de recherche que j'ai effectués à la NSA ne s'est révélé particulièrement important. Je suis à peu près certain que mon travail accumule la poussière dans un quelconque entrepôt classé du gouvernement. J'ai travaillé pour l'agence fort peu de temps, et c'était il y a bien longtemps. Je me sens cependant obligé de prendre la parole pour dire à quel point je suis horrifié. Si c'est la raison d'être de cette agence, je suis plus que désolé d'y avoir pris part, même si c'était insignifiant.

Je peux aujourd'hui difficilement imaginer ce que vous, mes anciens collègues, mes amis, mes professeurs et mes mentors devez ressentir en tant qu'anciens de la NSA. Contrairement à moi, vous vous êtes beaucoup investis, vous avez passé une grande partie de votre carrière à aider la NSA à construire un énorme pouvoir utilisé d'une façon qui n'était pas censé l'être. Vous pouvez à votre tour vous exprimer d'une façon qui ne transgresse ni votre clause de confidentialité ni votre honneur. Il est difficile de croire que les professeurs que j'ai connus dans les universités à travers le pays puissent rester silencieux alors que la NSA les a abusés, a trahi leur confiance et a détourné leurs travaux.

Resterez-vous silencieux ?

Le site Groklaw baisse le rideau à cause de la surveillance de la NSA !

Coup de tonnerre dans la blogosphère ! Le célèbre site Groklaw vient de publier un poignant dernier billet, dont nous vous proposons la traduction ci-dessous.

En cause, la surveillance et l'impossibilité de sécuriser sa communication par courriel, suite aux récentes révélations de Snowden. La spécialité de Groklaw c'est d'expliquer, relater, voire parfois révéler, collectivement des affaires et questions juridiques liées aux nouvelles technologies en général et au logiciel libre en particulier. Comment poursuivre si on se sent ainsi potentiellement violé(e) sans plus pouvoir garantir la confidentialité de ceux qui participent et envoient des informations au site ?

Ce qui fait dire en fin d'article, non sans amertume, à la fondatrice du site Pamela Jones : "But for me, the Internet is over".

Est-ce une décision exagérée ? A-t-elle réagi trop vite, sous la coup de la colère et de l'émotion ? Toujours est-il qu'une telle décision, aussi radicale soit-elle, aide à faire prendre conscience de la gravité de la situation…

Exposition forcée

Forced Exposure

Pamela Jones – 20 août 2013 – Groklaw
(Traduction : farwarx, GregR, aKa, phi, yoLotus, bituur, rboulle, eeva, Asta, Mari, goofy, GregR, Asta, Penguin, Slystone + anonymes)

Le propriétaire de Lavabit nous a récemment annoncé qu'il avait cessé d'utiliser les mails, et que si nous savions ce qu'il sait, nous en ferions autant.

Il n'y a aucun moyen de faire vivre Groklaw sans utiliser le courrier électronique. C'est là où est le casse-tête.

Que faire ?

Alors, que faire ? J'ai passé les deux dernières semaines à essayer de trouver une solution. Et la conclusion à laquelle je suis arrivée est qu'il n'y a aucun moyen de continuer Groklaw, pas sur le long terme, et c'est extrêmement malheureux. Mais il est bon de rester réaliste. Et la simple réalité est la suivante : peu importe les bons arguments en faveur de la collecte et de la surveillance de toutes les informations que nous échangeons avec les autres, et peu importe à quel point nous sommes tous « propres » pour ceux qui nous surveillent, je ne sais pas comment fonctionner dans un tel environnement. Je ne vois pas comment continuer Groklaw ainsi.

Il y a des années de cela, lorsque je vivais seule, je suis arrivée à New York et, comme j'étais encore naïve au sujet des gens malintentionnés dans les grandes villes, j'ai loué un appartement bon marché au sixième et dernier étage d'un bâtiment sans ascenseur, à l'arrière de celui-ci. Cela signifiait bien sûr, comme n'importe quel New-Yorkais aurait pu me le dire, qu'un cambrioleur pouvait monter le long de l'issue de secours incendie ou accéder au dernier étage via les escaliers intérieurs et ensuite sur le toit puis redescendre par une fenêtre ouverte de mon appartement.

C'est exactement ce qui s'est passé. Je n'étais pas là quand c'est arrivé, donc je n'ai été blessée physiquement d'aucune façon. De plus je n'avais rien de valeur et seulement quelques objets furent volés. Cependant tout a été fouillé et jeté au sol. Je ne peux pas décrire à quel point cela peut être dérangeant de savoir que quelqu'un, un inconnu, a farfouillé dans vos sous-vêtements, regardé vos photos de famille et pris quelques bijoux qui étaient dans votre famille depuis des générations.

Si cela vous est déjà arrivé, vous savez qu'il n'était plus possible pour moi de continuer à vivre là, pas une nuit de plus. Il se trouvait que, selon mes voisins, c'était certainement le fils du gardien. Ceci m'a frappée au premier abord mais ne semblait pas surprenant pour mes voisins les plus anciens. La police m'a simplement signifié qu'il ne fallait pas espérer récupérer quelque chose. Je me suis sentie violée. Mes sous-vêtements étaient tout ce qu'il y a de plus normal. Rien d'outrageusement sexy mais c'était l'idée que quelqu'un d'inconnu ait pu les toucher. J'ai tout jeté. ils ne seront plus jamais portés.

C'est comme ça que je me sens maintenant, sachant que des personnes que je ne connais pas peuvent se promener à travers mes pensées, espoirs, et projets, à travers les messages que j'échange avec vous.

Ils nous ont dit que si on envoyait un courriel hors des USA ou si on en recevait un venant de l'extérieur des USA, il serait lu. S'il est chiffré, il sera conservé pendant 5 ans, en espérant sans doute que la technologie aura assez évolué pour pouvoir le déchiffrer, contre notre volonté et sans que nous soyons au courant. Groklaw a des lecteurs partout sur la planète.

Je n'ai pas d'engagement en politique, par choix, et je dois dire qu'en me renseignant sur les derniers affaires, cela m'a convaincue d'une chose : j'ai raison de l'avoir évitée. Selon un texte sacré, il n'appartient pas à l'homme de savoir où mettre son prochain pas. Et c'est vrai. Les humains ne sont des humains et nous ne savons pas quoi faire de nos vies la moitié du temps, encore moins gouverner correctement d'autres humains. Et c'est démontré. Quel régime politique n'a pas été essayé ? Aucun ne satisfait tout le monde. Je pense que nous avons fait cette expérience. Je n'attends pas beaucoup de progrès sur ce point.

Je me souviens très nettement du 11 septembre. Un membre de ma famille était supposé être dans le World Trade Center ce matin-là, et quand j'ai regardé en direct à la télévision les gratte-ciel tomber avec des personnes à l'intérieur, je ne savais pas qu'elle était en retard ce jour et donc en sécurité. Mais est-ce qu'il importe que vous connaissiez quelqu'un en particulier, quand vous regardez des frères humains se tenir par la main et se jeter par des fenêtres de gratte-ciel vers une mort certaine, ou quand vous voyez les buildings tomber en poussière, sachant que de nombreuses personnes comme vous furent également transformées en poussière ?

J'ai pleuré pendant des semaines, comme ça ne m'est jamais arrivé, ni avant, ni depuis, et j'en garderai le souvenir jusqu'à ma mort. Une des choses qui m'angoissait le plus c'est de savoir qu'il y a des gens dans le monde qui ont envie d'infliger la même chose à d'autres, à des frères humains, des

inconnus ou des civils nullement impliqués dans aucune guerre. Cela semble ridicule, je suppose. Mais je vous dis toujours la vérité et c'est ce que je ressentais sur le moment. Alors imaginez ce que je ressens, imaginez ce que je dois ressentir maintenant sur la planète où nous vivons, si les dirigeants du monde entier pensent que la surveillance totale est une bonne chose…

Je sais. Ce n'est peut-être même pas le cas. Mais si ça l'était ? Le savons-nous seulement ? Je l'ignore. Mais ce que je sais, c'est qu'il n'est pas possible d'être pleinement humain si vous êtes surveillé 24h sur 24, 7 jours sur 7.

Le Centre Berkman de l'Université de Harvard, il y a quelques années, avait un cours sur la cyber-sécurité et la vie privée sur internet. Les ressources liées à ce cours sont toujours en ligne. Ce cours expliquait comment protéger sa vie privée dans un monde virtuel, parlant de choses étonnantes, avec des intitulés tels que "Is Big Brother Listening?"

Et comment ?

Vous y trouverez toutes les lois des États-Unis relatives à la vie privée et à la surveillance. Il ne semble pas pour autant que chacun respecte les lois qui se mettent en travers de son chemin de nos jours. Ou bien si les gens trouvent qu'ils ont besoin d'une loi pour rendre un comportement légal, ils vont simplement écrire une nouvelle loi, ou réinterpréter une ancienne loi et passer outre. Ce n'est pas ça, le respect de la loi tel que j'ai appris.

Bref, le cours faisait mention de passages du livre de Janna Malamud Smith, "Private Matters: In Defense of the Personal Life" et je vous encourage à le lire. J'encourage le président et la NSA à le lire également. Je sais. Ils ne me lisent certainement pas. Pas de cette manière-là en tout cas. Mais c'est important, parce que l'idée de ce livre, c'est que la vie privée est vitale pour rester un être humain, c'est la

raison pour laquelle l'une des pires punitions imaginables, c'est la surveillance totale :

> *Pour bien comprendre ce qu'est la vie privée il faut regarder ce qui se passe dans les situations extrêmes où elle est absente. Se remémorant Auschwitz, Primo Levi avait remarqué que « la solitude dans un camp était plus précieuse et rare que le pain ». La solitude est un des aspects de la vie privée et malgré la mort accablante, la famine et l'horreur des camps, Levi savait qu'elle lui manquait… Levi a passé une grande partie de sa vie à essayer de mettre des mots sur son expérience des camps. Comment, se demandait-il à voix haute, dans « Survivre à Auschwitz », décrire la « démolition d'un homme », un processus pour lequel les mots manquent dans notre langage.*
>
> *Nous nous servons de notre vie privée comme d'un espace sûr loin de toute terreur ou d'agression. Lorsque vous enlevez à une personne la possibilité de s'isoler ou de conserver des informations intimes pour elle-même, vous la rendez extrêmement vulnérable…*
>
> *L'état totalitaire surveille tout le monde, mais garde ses plans secrets. La vie privée est vue comme dangereuse car elle favorise la résistance. Espionner continuellement et ensuite poursuivre les gens pour ce qui est souvent de petites transgressions de la loi, voilà une façon de maintenir un contrôle sur la société, d'affaiblir et d'annihiler toute forme d'opposition…*
>
> *Et même quand on se débarrasse de ceux qui nous harcèlent vraiment, il est souvent très difficile de ne pas se sentir soi-même surveillé, c'est pourquoi la surveillance est un moyen de contrôle extrêmement puissant. Cette tendance qu'a l'esprit de se sentir toujours surveillé, même étant seul… peut vous inhiber. Quand ils se sentent surveillés, sans en être vraiment sûrs, sans savoir ni si, ni quand, ni comment, la force de surveillance hostile les frappera, les gens se*

sentent effrayés, contraints, préoccupés.

J'ai déjà cité ce livre, quand les mails des reporters de CNET étaient lus par Hewlette-Packard. Nous avons pensé que c'était horrible. Et ça l'était. HP a fini par leur offrir de l'argent pour essayer de se faire pardonner. Nous en savions vraiment peu à l'époque.

Mme Smith continue :

> *Quelle que soit la société qui privilégie l'individualité, l'assurance d'une vie privée est une composante essentielle de l'autonomie, de la liberté et donc du bien-être psychologique des gens. Pour résumer rapidement, à la question « Comment ne pas déshumaniser les gens » nous pourrions répondre : ne terrorisez pas ou n'humiliez pas, n'affamez pas, ne laissez pas souffrir du froid, n'épuisez pas les populations, ne les avilissez pas, ou ne leur imposez pas une soumission dégradante. Ne provoquez pas l'éloignement des gens qui s'aiment, n'exigez rien en vous exprimant dans un langage incorrect, écoutez les gens attentivement, ne réduisez pas la vie privée à néant. Les terroristes de toutes sortes réduisent la vie privée en la condamnant à la clandestinité et en utilisant la surveillance hostile pour profaner cet indispensable sanctuaire.*
>
> *Mais si nous décrivons une norme pour dire comment traiter quelqu'un humainement, pourquoi dépouiller quelqu'un de sa vie privée en est-il une violation ? Et qu'est-ce que la vie privée ? Dans son livre, Privacy and Freedom, Alan Westion cite quatre « états » de la vie privée : solitude, anonymat, réserve, et intimité. Les raisons pour lesquelles nous devons donner de la valeur à la vie privée deviennent plus claires lorsque l'on explore ces quatre états….*
>
> *L'essence de l'intimité est un sentiment de choix et de contrôle. Vous contrôlez qui regarde ou apprend sur vous. C'est vous qui choisissez de partir ou de revenir…*

> *L'intimité est un état interne qui nous permet de moduler notre personnage public, physiquement ou émotionnellement, et parfois les deux. Elle nous permet de nous construire une histoire personnelle, d'échanger un regard, ou de se reconnaître profondément. On peut s'ignorer sans se blesser. On peut faire l'amour. On peut se parler franchement avec des mots qu'on n'utiliserait pas face à d'autres, exprimer des idées et des sentiments, positifs ou négatifs, inacceptables en public. (Je ne pense pas avoir surmonté sa disparition. Elle parait incapable d'arrêter de mentir à sa mère. Il a l'air vraiment trop mou dans ce short de sport. Je me sens excité. En dépit de tout, il me tarde de le revoir. Je suis si en colère contre toi que je pourrais crier. Cette blague est dégoûtante, mais elle est très marrante, etc.). Protégée d'une exposition forcée, une personne se sent souvent plus capable de se livrer.*

J'espère que cela éclaire les raisons de mon choix. Il n'existe dorénavant aucun bouclier contre l'exposition forcée. Rien de ce que nous faisons n'a de rapport avec le terrorisme, mais personne ne peut se sentir assez protégé face à cette exposition forcée, jusqu'au moindre petit échange avec quelqu'un par courriel, particulièrement vers les USA ou en provenance des USA, mais en réalité depuis n'importe où. Vous n'attendez pas d'un étranger qu'il lise votre conversation privée avec un ami. Et une fois que vous savez qu'on peut le faire, que dire de plus ? Contrainte et préoccupée, voilà exactement comment je me sens.

Voilà, nous y sommes. C'est la fin de la fondation Groklaw. Je ne peux pas faire vivre Groklaw sans votre participation. Je n'ai jamais oublié cela lorsque nous avons remporté des victoires. C'était vraiment un effort collectif, or de toute évidence il n'existe plus maintenant de moyen privé pour collaborer.

Je suis vraiment désolée qu'il en soit ainsi. J'aimais

Groklaw, et je crois que nous y avons contribué significativement. Mais même cela s'avère être moins que ce que nous pensions, ou moins que je ne l'espérais en tous cas. Mon souhait a toujours été de vous montrer qu'il y a de la beauté et de la protection à l'intérieur des lois, que la civilisation actuelle en dépend en fait. Quelle naïveté !

Si vous voulez rester sur Internet, mes recherches indiquent qu'une mesure de sécurité à court terme face à la surveillance, dans la mesure où cela reste possible, est d'utiliser un service de courriels comme Kolab, qui est hébergé en Suisse, et par conséquent a une législation différente des USA, avec des lois qui visent à permettre davantage de confidentialité aux citoyens. J'ai maintenant une adresse chez eux, p.jones at mykolab.com, au cas où quelqu'un voudrait me contacter pour quelque chose de vraiment important et qui serait inquiet d'écrire un message vers une adresse sur un serveur américain. Mais mon autre adresse est encore valide. À vous de voir.

Ma décision personnelle est de me retirer d'Internet autant que possible. Je suis simplement une personne ordinaire. Je sais, après toutes mes recherches et des réflexions approfondies, que je ne peux pas rester en ligne sans perdre mon humanité, maintenant que je sais qu'assurer ma vie privée en ligne est impossible. Je me retrouve bloquée pour écrire. J'ai toujours été une personne réservée. C'est pourquoi je n'ai jamais souhaité être célèbre et c'est pourquoi je me suis toujours battue de toutes mes forces pour maintenir ma vie privée et la vôtre.

Si tout le monde faisait comme moi, rester en dehors d'Internet, l'économie mondiale s'effondrerait, je suppose. Je ne peux pas réellement souhaiter ça. Mais pour moi, Internet c'est fini.

Ceci est donc le dernier article de Groklaw. Je n'activerai pas les commentaires. Merci pour tout ce que vous avez fait.

Je ne vous oublierai jamais et n'oublierai jamais le travail que nous avons fait ensemble. J'espère que vous vous souviendrez de moi aussi. Je suis désolée mais je ne peux pas aller contre mes sentiments. Je suis ce que je suis et j'ai essayé, mais je ne peux pas.

PRISM NSA : pourquoi nous devrions nous sentir concernés, par Doctorow

Vous devriez vous sentir concerné par votre vie privée car…

PRISM de la NSA : pourquoi nous devrions nous sentir concernés

The NSA's Prism: why we should care

Cory Doctorow – 14 juin – The Guardian
(Traduction : KaTeznik, fany, b:v, genma, Mowee, Adcaelo, Metal-Mighty, letchesco, Asta, Gatitac, Yaf, tcit + anonymes)

Les politiciens nous disent que ceux qui n'ont rien à se reprocher n'ont rien à craindre des écoutes à leur insu. Pourtant, leurs décisions menacent la vie privée et bien au-delà..

Certains se demandent pourquoi faire tant d'histoires à propos des révélations sur PRISM et des autres formes de surveillance de masse de la NSA. Quand William Hague nous dit que les innocents n'ont rien à craindre de ces écoutes, on est en droit de se poser des questions : à partir de quand la surveillance peut-elle nuire ? que peut-il se produire lorsque l'on est épié ? Voici quelques raisons pour lesquelles vous devriez vous sentir concernés par votre vie privée, sa divulgation et la surveillance.

Nous ne sommes pas forcément sensibles aux problèmes de vie privée parce que les conséquences des révélations sur la vie privée sont éloignées dans le temps et l'espace des révélations elles-mêmes. C'est comme essayer de devenir bon au cricket en balançant la batte et en fermant les yeux avant de voir où part la balle, pour que l'on vous raconte, des mois plus tard, dans un autre lieu, où la balle a finalement atterri. Nous appréhendons mal ces problématiques : la plupart des révélations sur notre vie privée sont inoffensives, mais certaines d'entre elles provoquent des dégâts colossaux et quand cela se produit, c'est tellement éloigné dans le temps que nous ne pouvons en tirer aucune leçon véritable.

Vous devriez vous sentir concerné par votre vie privée car la

vie privée n'est pas secrète. Je sais ce que vous faites aux toilettes, mais pour autant cela ne veut pas dire que vous ne vouliez pas fermer la porte quand vous êtes sur le trône.

Vous devriez vous sentir concerné par votre vie privée car si les données disent que vous faites quelque chose de mal, celui qui les analysera interprétera tout le reste à la lumière de cette information. Le documentaire Naked Citizens *(NdT : Citoyens nus)* montre ainsi plusieurs cas effrayants de policiers alertés par des ordinateurs que quelqu'un pouvait préparer des actes délictueux, et qui ont alors interprété tout ce qu'ils apprenaient par la suite comme des preuves de délit.

Par exemple, quand un programmeur du nom de David Mery est entré dans le métro avec une veste alors qu'il faisait chaud, un algorithme de vidéosurveillance l'a signalé à un opérateur humain comme suspect. Quand Mery a laissé passer un train sans embarquer, l'opérateur a décidé que son comportement était alarmant. Il a été arrêté, a fait l'objet d'une perquisition et on lui a demandé de justifier chaque bout de papier de son appartement. Un gribouillage de traits aléatoires a été interprété comme un plan de la station de métro. Même s'il n'a jamais été reconnu coupable, Mery est toujours sur la liste des terroristes potentiels huit ans après et ne peut obtenir de visa pour quitter son pays. Une fois qu'un ordinateur signale un suspect, tout le reste de sa vie devient louche et presque un faisceau d'indices.

Vous devriez vous sentir concerné par la chape de plomb de la surveillance de masse car dans sa recherche d'aiguilles dans les bottes de foin, la police bénéficie alors de plus grosses bottes et d'aiguilles qui restent proportionnellement moins nombreuses. La Commission d'enquête sur le 11 septembre a relevé que les services secrets des États-Unis avaient toutes les informations pour prédire les attaques, mais que celles-ci ont été perdues dans tout le bruit dû à la trop grande quantité de données collectées. Depuis, la collecte excessive

est passée à la vitesse supérieure : les bottes de foin sont énormes, mais elles contiennent toujours le même nombre d'aiguilles. Je veux que mon ciel soit sûr et je souhaite, tout comme vous, que nos services secrets fassent bien leur travail, mais pas en aspirant toutes les données dans l'espoir qu'elles leur soient un jour utiles.

Vous devriez vous sentir concerné par la surveillance car vous connaissez des gens qui peuvent être exposés : des gays qui sont au placard, des malades en phase terminale, des personnes qui sont liées à une autre qui aurait notoirement commis un crime horrible. Il peut s'agir de vos amis, de vos voisins, peut-être même de vos enfants : ils méritent autant que vous une vie sans tracas et sans cadavre dans le placard.

Vous devriez vous sentir concerné par la surveillance parce qu'une fois que le système de surveillance est intégré au réseau et aux terminaux téléphoniques, des flics corrompus ou mal intentionnés peuvent l'utiliser contre vous. En Grèce, la porte dérobée utilisée par la police pour accéder aux communications de l'opérateur national a été détournée pour mettre sur écoute le Premier ministre durant la candidature aux Jeux Olympiques de 2005. Des services secrets chinois ont hacké le système d'interception légal de Google pour pirater Gmail et découvrir avec qui les dissidents communiquaient. Nos systèmes de communication sont plus sécurisés lorsqu'ils sont conçus pour empêcher les tierces parties d'y accéder – et l'ajout d'une seule porte dérobée à ces systèmes réduit à néant toutes les mesures de sécurité. Vous ne pouvez pas être *à moitié* enceinte, de même les ordinateurs dans votre poche, au bureau ou chez vous ne peuvent être *à moitié* sécurisés. Dès lors que ces appareils sont conçus pour la surveillance, n'importe qui peut soudoyer une autorité policière ou se faire passer pour telle et accéder aux données.

Revenons à M. Hague (Ministre des Affaires Étrangères britannique) : si les innocents n'ont rien à craindre de l'espionnage de leur vie privée, alors pourquoi son propre

gouvernement exige-t-il la mise en place d'un système sans précédent de tribunaux secrets, où l'on pourrait entendre les preuves de l'implication des services secrets britanniques dans des enlèvements illégaux et des actes de torture ? Apparemment, la confidentialité est absolument essentielle pour les puissants mais sans intérêt pour le reste d'entre nous.

Crédit photo : Digitale Gesellschaft (Creative Commons By-Sa)

Stop Watching Us, une pétition soutenue par Mozilla suite à l'affaire Prism

Mozilla a lancé hier la pétition **Stop Watching Us** suite à la retentissante affaire de la collecte de données privées d'internautes par le renseignement américain.

Nous en avons traduit la lettre adressée au Congrès qui apparaît en accueil de l'initiative.

Il va sans dire que cela nous concerne tous et pas seulement les Américains (à fortiori si vous avez déjà laissé des traces chez Google, Facebook, Twitter, Apple, Amazon, etc.)

Arrêtez de nous regarder

Stop Watching Us

Mozilla – 11 juin 2013
(Traduction : Mowee, Cyb, MFolschette + anonymes)

Les révélations sur l'appareil de surveillance de la National Security Agency, si avérées, représentent un abus stupéfiant de nos droits fondamentaux. Nous réclamons que le Congrès américain révèle l'étendue des programmes d'espionnage de la NSA.

Chers membres du Congrès,

Nous vous écrivons pour exprimer notre préoccupation à propos des rapports récemment publiés dans le Guardian et le Washington Post, et reconnus par l'administration Obama, qui révèlent l'espionnage secret par la NSA d'enregistrements téléphoniques et de l'activité sur Internet du peuple des États-Unis.

Le Washington Post et le Guardian ont récemment publié des rapports basés sur les informations fournies par un agent du renseignement, montrant comment la NSA et le FBI peuvent aisément accéder aux données collectées par neuf des principales sociétés américaines de l'Internet et partager ces données avec les gouvernements étrangers. Le rapport mentionne l'extraction par le gouvernement américain de données audio, vidéo, de photos, de courriels, de documents et d'historiques de connexion permettant aux analystes de suivre les mouvements et contacts des personnes au cours du temps. Il en résulte que les contenus des communications des personnes aussi bien résidant aux États-Unis qu'étrangères peuvent être parcourus sans aucune suspicion de crime ou d'association avec une organisation terroriste.

Ces rapports, également publiés par le Guardian et avérés par l'administration, révèlent que la NSA tire abusivement profit d'une section controversée du Patriot Act pour collecter les enregistrements d'appels de millions d'utilisateurs de Verizon. Les données collectées par la NSA incluent chaque appel, l'heure à laquelle il a été effectué, sa durée, et d'autres « informations d'identification » pour ces millions d'utilisateurs de Verizon, et ce pour l'ensemble des appels internes aux États-Unis, que les utilisateurs soient ou non suspectés de crime. Le Wall Street Journal rapporte que certains des principaux fournisseurs d'accès à Internet comme AT&T ou Sprint, sont sujets à de tels agissements secrets.

Ce type de collecte généralisée de données par le gouvernement est en contradiction avec le fondement des valeurs américaines de liberté et de vie privée. Cette surveillance massive viole le Premier et le Quatrième Amendement de la Constitution des États-Unis, laquelle protège le droit de parole des citoyens et leur anonymat et prémunit contre les perquisitions et saisies afin de protéger leur droit à la vie privée.

Nous appelons le Congrès à prendre des mesures immédiates pour mettre fin à cette surveillance et fournir publiquement toutes

les données collectées par le programme de la NSA et du FBI. Nous appelons donc le Congrès à immédiatement et publiquement :

1. Réformer la section 215 du Patriot Act, le privilège du secret d'état ainsi que les amendements de la loi FISA. L'objectif est de bien faire comprendre que la surveillance de l'activité sur Internet ainsi que l'enregistrement de toutes les conversations téléphoniques de toute personne résidant au sein des États-Unis sont interdits par la loi et constituent des violations pouvant être jugées par des autorités compétentes tel qu'un tribunal public.
2. Mettre en place une commission spéciale qui, après investigation, publiera de façon publique l'étendue de cet espionnage domestique. Cette commission devrait de plus recommander des réformes juridiques et règlementaires spécifiques afin de mettre un terme à cette surveillance inconstitutionnelle.
3. Demander des comptes aux principaux fonctionnaires responsables de cette surveillance.

Je vous remercie de l'attention que vous porterez à ce sujet.

Cordialement,

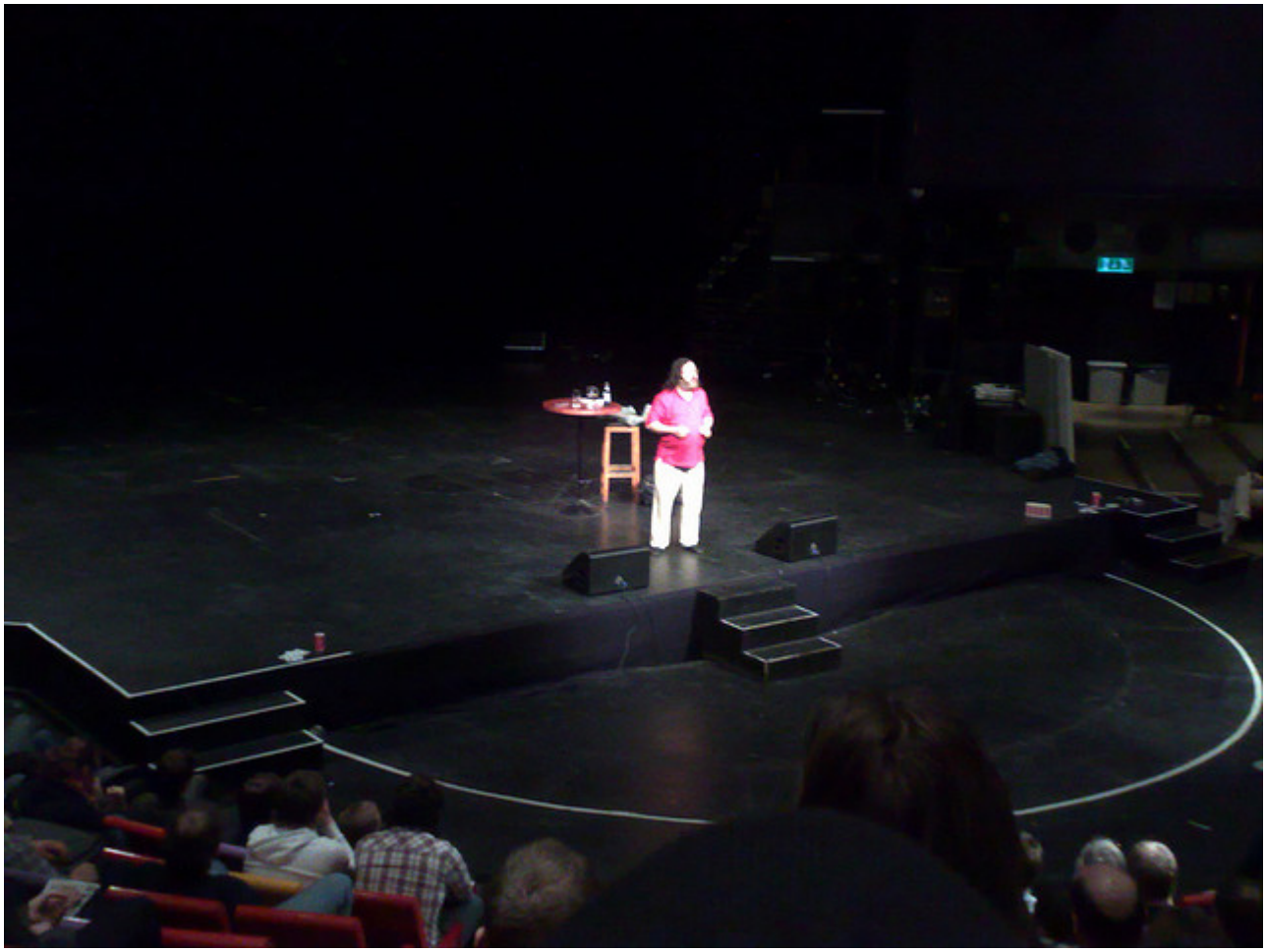
Crédit photo : Digital Cat (Creative Commons By)

Des milliers de morts, des millions privés de libertés

civiles ? Stallman (2001)

À l'heure où les USA sont empêtrés dans une sombre histoire d'espionnage généralisé à grande échelle, il nous a paru intéressant de déterrer et traduire un article de Richard Stallman rédigé en 2001 juste après le 11 septembre.

Force est de reconnaître qu'une fois de plus il avait pressenti les conséquences néfastes que nous subissons aujourd'hui.



Des milliers de morts, des millions privés de libertés civiles ?

Thousands dead, millions deprived of civil liberties?

Richard Stallman – 2001 – Site personnel

(Traduction : Lamessen, Slystone, Sky, Amine Brikci-N, Asta)

Dans de nombreux cas, les dommages les plus sévères que cause une lésion nerveuse sont secondaires ; ils se produisent dans les heures qui suivent le traumatisme initial, car la réaction du corps à ces dommages tue davantage de cellules nerveuses. Les chercheurs commencent à découvrir des façons de prévenir ces lésions secondaires et réduire les dommages ultimes.

Si nous ne faisons pas attention, les attaques meurtrières sur New York et Washington vont conduire à des effets secondaires bien pire encore, si le congrès étasunien adopte des « mesures préventives » qui écartent la liberté que l'Amérique représente.

Je ne parle pas de fouilles dans les aéroports ici. Les fouilles de personnes ou de bagages, tant qu'ils ne cherchent pas autre chose que des armes et ne gardent pas de traces de ces fouilles, est juste un désagrément : elles ne mettent pas en danger vos libertés civiles. C'est la surveillance massive de tous les aspects de nos vies qui m'inquiète : de nos appels téléphoniques, nos courriels et nos déplacements physiques.

Ces mesures sont susceptibles d'être recommandées indépendamment du fait qu'elles seraient efficaces pour leur objectif déclaré. Un dirigeant d'une entreprise développant un logiciel de reconnaissance faciale est dit avoir annoncé à des journalistes que le déploiement massif de caméras embarquant un système de reconnaissance faciale aurait empêché les attaques. Le New York Times du 15 septembre cite un congressiste prônant cette « solution ». Étant donné que la reconnaissance humaine du visage effectuée par les agents d'accueil n'a pas permis de stopper les pirates, il n'y a pas de raison de penser que les caméras à reconnaissance faciale informatisée aurait été d'une quelconque aide. Mais cela n'arrête pas les agences qui ont toujours voulu mettre en place plus de surveillance de pousser ce plan aujourd'hui, ainsi que beaucoup d'autres plans similaires. Il faudra

l’opposition du public pour les stopper.

Encore plus inquiétant, une proposition visant à exiger des portes dérobées gouvernementales dans les logiciels de chiffrement a déjà fait son apparition.

Pendant ce temps, le Congrès s’est empressé de voter une résolution donnant à Bush les pleins pouvoirs d’utilisation de la force militaire en représailles des attaques. Les représailles peuvent être justifiées, si les auteurs des attaques peuvent être identifiés et ciblés avec soin, mais le Congrès a le devoir d’examiner les mesures spécifiques lorsqu’elles sont proposées. Donner carte blanche au président dans un moment de colère est exactement l’erreur qui a conduit les États-Unis dans la guerre du Vietnam.

S’il vous plait, laissez vos représentants élus et votre président non élu savoir que vous ne voulez pas que vos libertés civiles deviennent les prochaines victimes du terrorisme. N’attendez pas, Les lois sont déjà en cours d’écriture.

Crédit photo : Sigg3net (Creative Commons By)