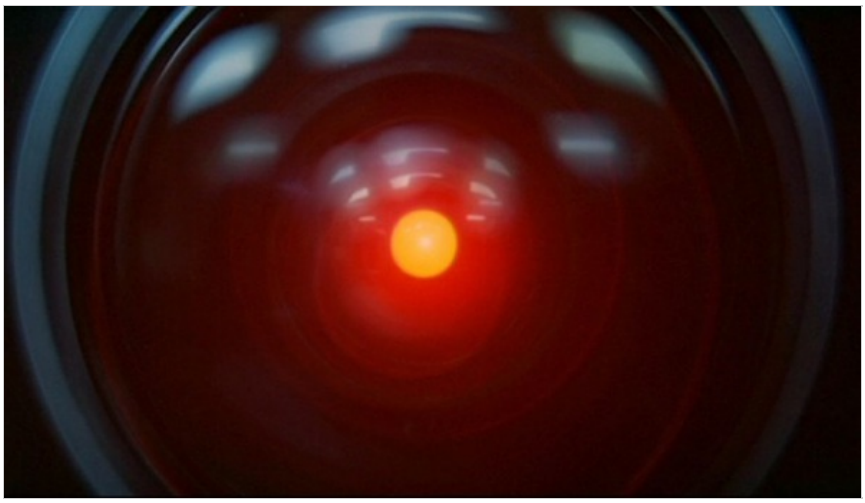
[Hollandie] Demain, Tous Suspects !



Publié le 21 juillet 2013 | par **Lurinas**

Les révélations de Snowden (sur l'ampleur des opérations d'espionnage et de surveillance des télécommunications de la National Security Agency (NSA) via le projet Prism) ont rappelé que cela pouvait aussi concerner des Français*. Mais qu'est-ce qui est espionné, stocké, analysé exactement ? Quelles en sont les conséquences et les projections à long terme ? Qu'en penser ? (quand penser ?!…). Lurinas vous explique.

La chaine de contacts

Contrairement aux écoutes téléphoniques classiques, ce qui intéresse la NSA, ce n'est pas tant le contenu des télécommunications que leur contenant, ce que l'on appelle des méta-données : qui communique avec qui, quand, d'où, au sujet de quoi, en utilisant quels logiciels, passerelles, fournisseurs d'accès, adresses IP, etc.

L'objectif est en effet de constituer un « graphe social » des personnes et organisations ciblées en constituant une chaine de contacts. En général, l'analyse des réseaux est portée à deux degrés de séparation de la cible.

Autrement dit, la NSA espionne aussi ceux qui communiquent avec ceux qui communiquent avec ceux qui sont espionnés.

Cette chaine de contacts peut amener à une réflexion intéressante, et permettrait de soupeser l'ampleur du danger potentiel pour la totalité de l'humanité.

L'hypothèse était émise, confirmée par Migram dans les années 70, qu'il n'existerait que six degrés de séparation entre tous les êtres humains (**https://fr.wikipedia.org/wiki/Six_degr%C3%A9s_de_s%C3%A9paration** ; **https://fr.wikipedia.org/wiki/%C3%89tude_du_petit_monde**).

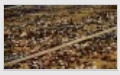
En 2011, allant plus loin, une étude portant sur les utilisateurs de Facebook révélait que ses utilisateurs ne sont séparés, en moyenne, que de 4,74 degrés (soit moins de 4 personnes). Sur Twitter, il ne serait que de 4,67 degrés.

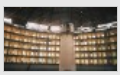
Votre papa, votre maman, vos grands-parents, vos enfants, collègues, amis n'ont peut-être

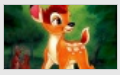
Mots-clés

démocratie (24)
internet (39)
prism (2)
surveillance (3)

Du même auteur


[Hollandie] Un Accord Transatlantique encore Transcendant


[Hollandie] Panoptique, nous voilà !


L'Acte Subversif de Manifestation Numérique

Sur le même sujet


DÉPUTÉS SOUS CONTROLE


Les Informaticiens Changent la Démocratie


[ITV] Chantal Jouanno, la Droite Responsable


La Bataille d'ACTA


Pirates 2.0 – La Démocratie leur Tient Hacker

« rien à se reprocher ». Mais ils connaissent très probablement quelqu'un qui connaît quelqu'un qui a été en contact avec Mohamed Merah !

Et comme ce degré de recherche pour produire la chaine de contacts ne saurait rester intangible, tout prédispose à espionner tout le monde dans un proche avenir dès que les règles seront un peu plus élargies (l'expérience législative des fichiers FNAEG and co. n'est pas là pour nous rassurer).

D'ordinaire, on tend à considérer que l'homme qui a vu l'homme qui a vu l'ours n'est guère crédible. Pour les services de renseignement, c'est différent : leur objectif est de « tout savoir sur tout, tout le temps ».

Les méta-données

Les méta-données de vos télécommunications ne sont pas considérées comme relevant de votre vie privée par les autorités américaines, mais révèlent pourtant énormément d'indices sur vous.

Les appels téléphoniques que vous faites peuvent révéler beaucoup de choses, et à mesure que nos vies sont de plus en plus médiatisées par l'Internet, nos traces IP (identifiant unique sur le réseau) dressent comme une carte en temps réel de votre vie : ce que vous lisez, ce qui vous intéresse, les publicités ciblées auxquelles vous répondez, les discussions auxquelles vous participez…

Surveiller les traces que vous laissez sur l'Internet (d'autant plus en les exploitant au moyen d'outils d'analyse très sophistiqués) est une façon de rentrer dans votre tête qui est à bien des égards comparable au fait de lire votre journal intime.

Il a récemment été démontré que, même avec des méta-données anonymisées, « il suffisait de 4 informations de localisation dans le temps et l'espace (c'est-à-dire connaître 4 antennes d'où un utilisateur s'est connecté pour téléphoner ainsi que la date et l'heure, données qui sont par essence compilées dans les méta-données de nos appels téléphoniques) pour identifier précisément 95 % des utilisateurs et que 2 informations suffisent à les identifier à 50%.

Toutes ces méta-données sont stockées (en France aussi) sur des années et des années, et quand les services s'intéressent à une adresse IP ou à un numéro de téléphone, il suffit de chercher dans les bases de données, et la liste des correspondants permet de reconstituer tout son réseau.

En attendant, personne ne pourra plus dire que puisqu'elle n'a rien à se reprocher, elle n'a rien à cacher !

D'un autre côté, l'usage et le tri de ces méta-données ont de quoi donner des sueurs froides aux services en charge de leur exploitation. Pour se faire une idée de l'usine à gaz stockée dans les serveurs des renseignements, je ne saurai trop vous conseiller la lecture de cet article bien documenté : **http://www.slate.fr/story/74433/metadonnees-terroriste-retrouver**

Un projet qui exclut les amerlockes ?

Prism est loin d'être le premier réseau du genre, mais il va toutefois beaucoup plus loin que ses prédécesseurs en rendant possible la surveillance d'un individu n'importe où sur le globe, pourvu qu'il utilise des services de géants du Net tels que ceux de Facebook, Google, Microsoft, Yahoo ou encore Apple.

A une exception près : le citoyen américain, sur son territoire, en serait exclu.

Vraiment ? En théorie, ils sont protégé par le 4ème Amendement. La NSA doit alors s'assurer qu'au moins un des deux interlocuteurs qu'elle écoute est situé hors des Etats-Unis. C'est ce que prévoit le Foreign Intelligence Surveillance Act (FISA), une loi qui autorise l'écoute de toute télécommunication émise depuis les Etats-Unis vers l'étranger ou vice-versa.

C'était sans compter sur l'existence du programme Stellar Wind qui permettrait aux grandes oreilles de la NSA de mettre sur écoute des citoyens américains "at home ».

Dès 2002, Bush Junior a voulu créer des exceptions à la loi, qu'il jugeait peu adaptée à un climat de guerre contre le terrorisme. Et le système perdure encore aujourd'hui. Rebaptisé Ragtime, le dispositif se découpe en quatre segments :

- Ragtime-A se concentre sur les interceptions à l'étranger ;
- Ragtime-B s'intéresse aux données des gouvernements étrangers qui transitent dans les câbles américains ;
- Ragtime-C se focalise sur la contre-prolifération ;
- Ragtime-P est tout dédié à la surveillance sur le territoire américain.

Comme si cela ne suffisait pas, depuis quelques années déjà, les opérateurs téléphoniques et les FAI locaux collaborent avec la NSA. En 2003, un ingénieur de AT&T découvrait la "Room 641A", une petite pièce servant à intercepter les appels effectués via l'opérateur américain.

Cet épisode sera couvert d'une immunité juridique rétroactive !

En sus, l'administration Obama a amendé FISA en 2008 (récemment prolongé jusqu'en 2017) : le texte autorise désormais la surveillance domestique au nom de la lutte contre Al-Qaida.

Si vous êtes étranger, hors du territoire américain, a priori, que vous soyez suspect ou non, vous êtes le cœur de cible de FISA et du réseau Prism. Si vous êtes européen, aucune législation n'est susceptible d'empêcher réellement des entreprises américaines telles que Google ou Microsoft de rapatrier des infos personnelles vous concernant sur leurs serveurs aux Etats-Unis. Et donc, de tomber dans ceux de la NSA.

Cette procédure pourrait d'ailleurs être rendue légale aux Etats-Unis par le Cispa, un texte très controversé toujours en cours de discussion, qui autorise le transfert de données personnelles entre les entreprises et le gouvernement américain, au nom de la cybersécurité (**http://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act**).

M'en fout, j'ai rien à cacher !

On entend souvent dire, et pas seulement par Hortefeux, que…

> ***»seuls ceux qui ont quelque chose à se reprocher ont quelque chose à cacher »***

Pourtant, nous ne devrions pas considérer les paranoïaques du côté de ceux qui s'étonnent d'être surveillés, mais plutôt parmi ceux qui veulent surveiller tout le monde à tout prix.

Dans une démocratie, c'est à l'accusation d'apporter les preuves de la culpabilité des suspects, pas à ces derniers d'apporter les preuves de leur innocence. Le problème des atteintes à la vie privée est éminemment politique, voire idéologique.

Un tel traitement de surveillance généralisée affecte les relations entre les gens et les institutions d'un Etat moderne. Il ne se limite pas à frustrer l'individu en créant un sentiment d'impuissance, mais il affecte toute la structure sociale en altérant les relations que les gens ont avec les institutions qui prennent des décisions importantes sur leur existence.

Pour ceux qui avancent qu'ils n'ont « *rien à cacher* » puisqu'ils n'ont « *rien à se reprocher* », les contrôles ou la surveillance dont ils font l'objet ne les identifiera jamais comme suspects. Sauf que la suspicion, et ses erreurs d'interprétation, c'est un peu comme le Loto, ça n'arrive pas qu'aux autres.

Car comment peut-on être certain de n'avoir rien à se reprocher ? Et si les règles changeaient ? Et si plusieurs personnes qui disposent d'un pouvoir sur nous les interprétaient différemment, ou appliquaient des règles différentes ? Et si, surtout, on ne pouvait jamais être certain de savoir qui applique quelles règles, et de quelle manière ?

Sans compter que la fouille sociale de données n'est pas la panacée… (**http://www.internetactu.net/2011/09/14/les-limites-de-la-fouille-sociale-de-donnees/**). Bref, déjà ou à venir, des implications sociétales importantes de l'usage de ces technologies intrusives !

Si les naïfs découvrent Prism, c'est qu'un autre projet est en cours

Sept pays sont impliqués dans la surveillance de masse du réseau Prism et sont plus ou moins directement liés au programme global des autorités américaines. Ils auraient signé des accords secrets avec les USA sur des questions de SIGINT (le renseignement de source électromagnétique) :

- Le Royaume-Unis
- L'Allemagne (revoyez donc la vidéo de Merkel demander énergiquement des explications aux USA)
- Les Pays-Bas
- La France (Holland va encore en tomber des nues !?…)
- Le Danemark
- L'Italie
- L'Espagne

De quoi jouer les vierges effarouchées !?

Des documents déclassifiés révèlent que les USA classent les Etats par degré de de la confiance qu'ils leur accordent. Une confiance de niveau 1 est accordée au Royaume-Unis, au

Canada, à l'Australie et la Nouvelle-Zélande. Une confiance de niveau 2 est accordée à l'Allemagne et à la France.

C'est pourtant un degré bien plus embêtant que de constater que ces 7 pays donnent leur consentement pour que les USA interceptent une masse de données énorme, portant sur des appels téléphoniques, des emails, et les simples visites sur des sites web (bref, tout le trafic), via les câbles sous-marins.

Nous le savons depuis le tout début de l'affaire Prism, le scandale est loin de se limiter à l'opérateur Verizon et aux 9 géants du Net collaborant directement avec ce programme. Le projet UPSTREAM, programme qui désigne l'écoute des câbles sous-marins, commence à fuiter. Et oui, Prism est un tout petit machin !… Il s'agirait là d'une écoute massive des populations via les câbles et les backbones qui véhiculent les flux Internet (scoop reflets.info).

En France, un projet Eagle n'est en sus pas à exclure (projet de même acabit que celui fourni à la Libye de Kadhafi, la Syrie… par Bull via Amesys). Il parait même à portée puisqu'il est déjà nommé en interne, chez Amesys, du petit nom suivant : EAGDLP1101 (nouveau scoop reflets.info).

Un projet installé à Toulon depuis début 2012. Voire Lorient, qui est également une base militaire importante.

De quoi s'agit-il ? Le contrôle de ce qui sort d'un réseau privé, afin d'éviter des fuites d'informations. Il ne s'agirait donc pas d'un système d'écoute globale des flux Internet français. L'écoute globale du pays serait d'ailleurs complexe à mettre en place** (car l'Internet en France n'est pas centralisé comme aux USA mais passe par près de 16000 répartiteurs téléphoniques et 40000 points d'interconnexion DSLAM ; trop de fournisseurs d'accès, trop de points d'entrée). Toutefois, des écoutes ciblées sont possibles.

La fuite en avant est engagée d'aussi loin que le progrès technologique se met au service de l'espionnage et du contre-espionnage. Aussi, si l'on veut faire de la collecte massive, développer la vidéosurveillance, enregistrer tous les déplacements de chacun, développer le fichage, il serait indispensable qu'en contrepartie nous ayons un meilleur accès à la collecte de données, de meilleures garanties quant aux règles qui régissent les processus afin qu'elles ne puissent être changées unilatéralement, de meilleures assurances et protections quant à la dissémination ou l'invasion.

A suivre

Lurinas

* les Européens semblent avoir oublié l'existence du réseau américain Echelon qui scrute depuis les années 70 les conversations téléphoniques, les fax, les courriels du monde entier y compris donc de l'Union européenne. Des stations d'écoutes sont même installées dans les pays anglo-saxons considérés comme particulièrement sûrs par les États-Unis (Australie, Canada, Nouvelle-Zélande…), la principale étant située dans le Yorkshire, au Royaume-Uni.

C'est le Parlement européen qui a sonné la charge contre ce qui apparaît comme une gigantesque violation des droits civils en créant une commission d'enquête fin 2000. Son volumineux rapport, remis en juillet 2001, quelques semaines avant le 11 septembre, est tombé dans l'oubli, la lutte contre le terrorisme l'emportant sur la préservation des libertés publiques. Douze ans plus tard, le réseau Echelon est toujours en activité et s'est même considérablement perfectionné.

Rapport parlementaire européen ici : **http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//FR**

** Ce qui ne signifie pas que la DGSE n'espionne pas tout ou partie des télécommunications qui transitent par satellite. La loi de 1991 relative au secret des correspondances émises par la voie des communications électroniques (**http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000173519**), censée encadrer les interceptions de communications électroniques et désormais intégrée au Code de la sécurité intérieure, excluait le spectre hertzien de toute forme de contrôle : « Cette dérogation a été exigée par les plus hautes autorités de l'Etat, confie un ancien conseiller du ministre de la Défense de l'époque, Pierre Joxe. Pourquoi ? Souvenez-vous, à cette époque, la DGSE lançait un vaste plan de modernisation de ses « grandes oreilles ». Il était hors de question de le compromettre ».

Bref, laisser les coudées franches aux services secrets et ne pas les enfermer dans un quota d'écoutes autorisées.

Accessoirement, les ondes hertziennes servent aussi en matière de radio-identification (RFiD), de GPS, de GSM et de Wi-Fi… technologies qui, en 1991, n'étaient pas utilisées par le grand public, contrairement à aujourd'hui. Un écoute donc grandement étendue par la force du progrès technologique !

Reste donc aussi la question des câbles de fibres optiques sous-marins, qui ne relèvent pas du spectre hertzien, et qui ne sauraient donc être légalement espionnables par la DGSE. Question laissée en suspens.

« Tous les pays démocratiques qui se sont dotés de services d'écoute «satellitaire» ont mis en place des garde-fous, des lois et des instances de contrôle afin de protéger leurs citoyens contre la curiosité de ces «grandes oreilles». Tous, l'Allemagne et les Etats-Unis en tête. Pas la France.»

Sources

http://bugbrother.blog.lemonde.fr

http://www.bortzmeyer.org/

http://reflets.info/

http://www.slate.fr/

Les commentaires (1)

marcon 4 septembre 2013 à 20 h 30 min

Ah,que le manque,confortes§Car il ne fait que révéler,nos-doutes,nos faiblesses,nos « manque-de-substances »,en-bref',MANQUE'd'UNITé,salut'frére,prépares-moi !

À la une

Municipales : Un Chinois à Paris

[Appel à Financement] Un Studio pour LaTéléLibre !

[RUSHS LTL News] Qui a Peur des Bonnets Rouges Bretons?

[LE FOSSOYEUR #7] L'Échelle De Jacob

NKM : Un Autre Dissident Dans le 10ème

Le meilleur

SAUVER KOKOPELLI ? MAMÈRE A UNE IDÉE…

SOUS LES PAVÉS… DENIS ROBERT – 1/3

SOUS LES PAVÉS… DENIS ROBERT – 2/3

B.A. DANY "L'ESPRIT DE MAI 68, C'EST MOI"

Un Toit Pour Moi

Journal

[L'ÉDITO DE JO] Minute : l'Éjaculateur Précoce de l'Extrême-Droite ?

[Hollandie] Un Accord Transatlantique encore Transcendant

[Hollandie] Panoptique, nous voilà !

[Appel à Financement] Un Studio pour LaTéléLibre !

Les 343 Connards

À propos

Qui sommes-nous ?

L'association

Ils nous soutiennent

Charte éditoriale

Mentions légales

Nous contacter

Culture Économie Médias Monde Politique Société Sport