

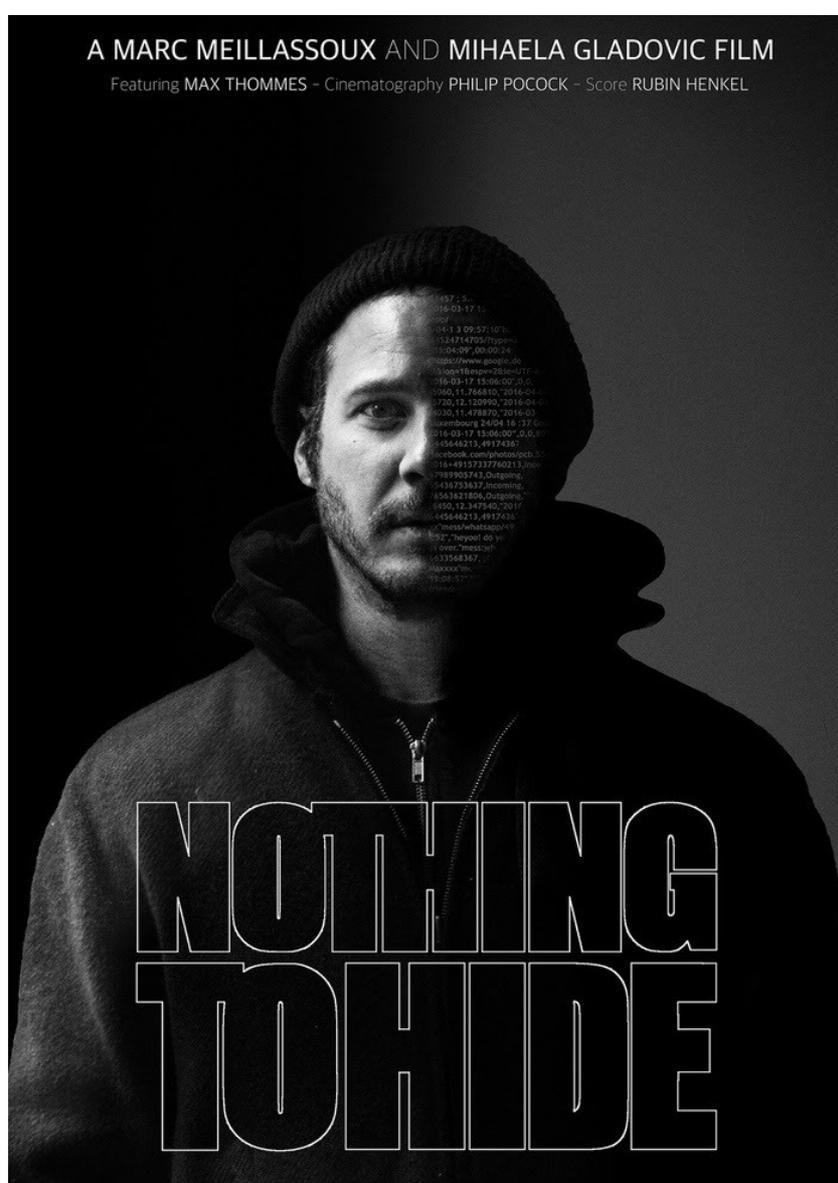
NOTHING TO HIDE

le film

Production & réalisation : Mihaela GLADOVIC & Marc MEILLASSOUX

Sortie : Septembre 2017

Durée : 86 min



Visible en ligne (sous licence "Creative Commons") depuis le 30 septembre 2017 :

<https://nothingtoidoc.wordpress.com/nothing-to-hide-french-high-quality/>

"NOTHING TO HIDE"

UN DOCUMENTAIRE SUR LA SURVEILLANCE

<https://blogs.mediapart.fr/nothing-hide-documentaire/blog/021116/nothing-hide-un-documentaire-sur-la-surveillance>

Auteur : Marc MEILLASSOUX

Publication : MEDIAPART (02 novembre 2017)

Le documentaire "Nothing to hide", dédié à la surveillance, est en compétition ce jeudi 3 novembre au Festival International du Film (FIFF) Français de Stuttgart-Tübingen et au Festival des Cultures Numériques KIKK, à Namur. Un film qui parle de vous et de vos données personnelles.

[...] NOTHING TO HIDE interroge la vaste acceptation de la surveillance au sein de la population par l'argument "je n'ai rien à cacher". A travers cinq protagonistes et une vingtaine d'intervenants (lanceurs d'alerte, hackers, juges, sociologues, victimes de la surveillance) le documentaire explore les implications d'une telle rhétorique à l'époque du tout-numérique et interroge ce modèle de société que nous contribuons chaque jour à façonner.

Le principal protagoniste du film est un jeune artiste qui pense, comme la plupart d'entre nous, "ne pas avoir grand-chose à cacher". Avec son accord, les données de son MacBook, de son iPhone et de l'ensemble de ses applications (Whatsapp, Facebook Messenger, Skype...) sont récoltées durant un mois à l'aide d'un logiciel espion. L'expérience 'Mister X' se concentre sur les "métadonnées" (*metadata* en anglais), les "données sur les données" : les heures de connexion de Mister X sur Facebook, sa géolocalisation sur son iPhone, l'objet de ses mails ou la fréquence de ses communications dans sa liste de contacts. Ces informations collectées par la plupart de nos applications constituent la matière première du profilage numérique dont nous faisons l'objet au quotidien.

Ce que nos métadonnées disent de nous : l'expérience "Mister X"

Les métadonnées sont par ailleurs de plus en plus scrutées par les agences de renseignement. Leur collecte est présentée comme plus protectrice de la vie privée par nos dirigeants politiques, car elle n'implique pas les contenus de nos messages, sms, mails... L'objectif est de comprendre ce qu'une entité privée ou une agence de renseignement peut savoir de nous et ce que l'agrégation de métadonnées peut générer comme contenu.



**Alison Macrina, the Tor Project
(protocole et navigateur anonyme)**

Nos métadonnées permettent-elles de déterminer notre orientation sexuelle, politiques notre état de santé, les taux d'intérêt que nous payerons pour l'achat d'une maison? Quels dangers y a-t-il à ce que le gouvernement ait accès aux données personnelles de ses juges, médecins, chercheurs, militants, journalistes et citoyens?



Thomas Drake, lanceur d'alerte de la NSA

Le documentaire explore également une rhétorique de plus en plus associée en temps de "lutte contre le terrorisme": doit-on sacrifier notre vie privée pour plus de sécurité ainsi que les similitudes entre les régimes de surveillance d'hier (la Stasi allemande) et d'aujourd'hui. Les destins des plusieurs protagonistes du film, tous victimes de la surveillance, tend à montrer que chacun pourra un jour être concerné, même s'il n'a *a priori* "rien à cacher".

Le documentaire entame sa phase de distribution avec plusieurs festivals et projection-débat. Le film financé de manière 100% indépendante est également ouvert à d'autres canaux de diffusion avant de rendre le documentaire accessible à tous.

VOUS ÊTES SURVEILLÉS LA PREUVE AVEC LE DOCUMENTAIRE "NOTHING TO HIDE"

<http://www.up-inspirer.fr/37346-vous-etes-surveilles-la-preuve-avec-le-documentaire-nothing-to-hide>

Auteur : Mounir BELHIDAOU¹

Publication : UP le mag (29 septembre 2017)

On n'en sort pas indemne. Pendant plus d'une heure vingt minutes, "Nothing to Hide" ("Rien à cacher" en anglais) va poser la question de la trace que nous laissons sur Internet. Surtout, le film nous montre que la surveillance de masse ne date pas d'hier, qu'elle avait déjà eu lieu en Allemagne de l'Est avec la Stasie (police d'espionnage de la RDA) et qu'elle a trouvé son apogée avec les révélations fracassantes d'Edward Snowden, cet ancien salarié des services secrets américains qui a rendu publics des documents très compromettants, mettant en cause les États-Unis. "Nothing to hide" nous montre aussi l'expérience, appelée "Mister X", d'un jeune acteur berlinois qui a accepté de se prêter à l'expérience de l'espionnage à partir de ses données téléphoniques. Le résultat est saisissant. Après avoir vu ce documentaire, nous avons rencontré Marc Meillassoux, son réalisateur.

Comment avez-vous eu l'idée de ce documentaire ?

À l'époque des révélations d'Edward Snowden, j'avais acté, résigné, la fin de la vie privée en ligne et la confidentialité de mes communications, me sentant démuni en raison de mon inculture en informatique. Un jour, un ami m'a parlé des CryptoParties – ces workshops gratuits où tout le monde peut apprendre à protéger ses données – et ça m'a vite passionné de découvrir des moyens de surfer anonymement sur le net, de chiffrer les mails ou de découvrir les logiciels "libres". Pour la première fois, j'avais l'impression de reprendre un peu de contrôle.

Quand j'essayais d'en discuter autour de moi, j'entendais systématiquement : "En quoi cela me concerne-t-il ? Je ne fais rien de mal..." et *in fine* : "De toute façon ils peuvent bien regarder, je n'ai rien à cacher." J'ai rencontré ma collègue Mihaela Gladovic à ce moment-là et on s'est dit qu'il fallait creuser ce mythe du "rien à cacher". Cette formule semble indolore et *a priori* de bon sens. Elle est aussi pratique pour se rassurer et continuer de consommer nos applications préférées. Quand on creuse un peu plus, on se rend pourtant qu'elle implique un vrai choix de société.

Vous souvenez-vous de ce mois de déprime hivernale il y a deux ans quand vous avez manqué deux jours de travail ou du nombre de soirées où vous êtes rentrés tard (donc éméchés ?) en 2015 ? Non. Les algorithmes de Facebook, eux, le savent.

1. <http://www.up-inspirer.fr/author/mounir-belhidaoui>



Mister X, qui a accepté une expérience de surveillance pour le compte du film. Crédits : DR

On peut voir que la consultation de sites web de santé peut mener à de la revente de données à des laboratoires pharmaceutiques. Est-ce légal ?

La question légale est compliquée. Certaines choses peuvent être légales aux États-Unis et illégales en Europe. Et vice et versa. La commercialisation de données dites "sensibles" (données médicales, orientations sexuelles, ethniques etc.) est interdite en Europe. Beaucoup d'entreprises revendent par contre des données dites "anonymisées", qui sont d'après de nombreux spécialistes en sécurité informatique facilement "ré-identifiables". Être journaliste, trentenaire, travailler entre la France et l'Allemagne, et, imaginons, faire de l'hypertension, ce sont quatre données "anonymes" très facilement accessibles. Pourtant, en les croisant, je pourrais bien être le seul dans ce cas. On voit aussi que la tendance est toujours plus favorable aux entreprises, en raison notamment de la mauvaise santé de l'économie. Donald Trump vient ainsi d'autoriser aux fournisseurs d'accès à internet américains de vendre les données de navigation de leurs clients.

Facebook pourra bientôt vérifier notre solvabilité, histoire de voir si on peut rembourser ses crédits... C'est un peu préoccupant, non ?

Facebook a fait breveter une technologie qui permet d'associer une note de solvabilité à un potentiel emprunteur basé sur ses données de connexions. Facebook nous connaît parfois mieux que nous nous connaissons nous-même. Vous souvenez-vous de ce mois de déprime hivernale il y a deux ans quand vous avez manqué deux jours de travail ou du nombre de soirées où vous êtes rentrés tard (donc éméchés ?) en 2015 ? Non. Les algorithmes de Facebook, eux, le savent. Si vous avez Facebook Messenger sur votre smartphone, ils savent même très exactement quand vous vous couchez (votre téléphone s'immobilise) et quand vous vous levez (votre téléphone reprend son activité). Certains imaginent même que Facebook (ou d'autres GAFAs) se lance un jour lui-même dans l'assurance ou dans la banque, avec un avantage compétitif déterminant.

La question de l'intimité revient beaucoup dans ce documentaire. Comment la définiriez-vous ? Est-elle "violée" dès lors qu'on se connecte, par exemple, à un réseau social ?

L'intimité, ce sont tous ces moments durant lesquels vous êtes seuls face à vous-même et vous explorez des choses nouvelles à *l'abri du regard des autres et sans jugement d'autrui*. Ces moments où vous chantez sous la douche, vous apprenez un instrument en massacrant les notes, vous faites des recherches sur Internet pour développer vos connaissances et votre esprit critique. Dans la théorie de Bentham sur le *Panoptique*, un seul surveillant peut – du haut d'une tour placée au centre d'une prison circulaire aux cellules ouvertes – tenir en respect des centaines de prisonniers. Il ne peut bien sûr pas tous les surveiller en même temps, mais la conscience des prisonniers qu'ils *pourraient être surveillés* entraîne une modification de leur comportement.



Jérémie Zimmermann, fondateur de La Quadrature du Net, alerte sur les dangers de la surveillance de masse. Crédits : DR

Le danger serait une normalisation, au sens d'uniformisation, des comportements. Le philosophe Gilles Deleuze, qui a notamment travaillé sur les sociétés de contrôle, conclut ainsi sur le *Panoptique*: "La formule abstraite du Panoptique n'est plus "voir sans être vu", mais "imposer une conduite quelconque à une multiplicité humaine quelconque"..."

En ligne, il faut être conscient de la puissance des "métadonnées", au delà des seuls contenus des communications. Des métadonnées courantes seront, par exemple, un appel passé par Monsieur X à Madame Y, à telle géolocalisation, à telle heure, à telle fréquence, pendant tant de temps. Nous laissons des centaines de métadonnées par jour, qui indique quand nous travaillons, si nous sommes actifs ou sédentaires, combien nous dormons, avec quel type de personnes nous interagissons, etc. Facebook a déjà ouvertement fait deux expériences psycho-sociologiques en manipulant l'algorithme, se félicitant de pouvoir influencer sur l'humeur des gens. On revient ici très directement aux travaux de Michel Foucault (*Surveiller et Punir*) et de Gilles Deleuze.

Edward Snowden apparaît dans le film. Les lanceurs d'alerte sont-ils toujours pourchassés ? Quel est son crime *in fine* ?

Les lanceurs d'alerte comme Edward Snowden ont contribué à relancer un grand débat démocratique à travers le monde. Ils ont aussi porté atteinte à l'image des agences de renseignement et ont remis en question l'autorité de l'État. Un seul homme qui déjoue la

surveillance de la NSA, du FBI, de la CIA et de treize autres agences ça fait jaser et ça peut donner des idées à d'autres. D'où cette chasse aux lanceurs d'alerte.

Dans le documentaire, Thomas Drake explique comment, tout en ayant épuisé les ressources légales au sein de la NSA puis au congrès américain des dérives internes, il est devenu un ennemi public des États-Unis. En France, le sort réservé à des lanceurs d'alerte comme Stéphanie Gibaud (UBS), Antoine Deltour et Raphaël Halet (Luxleaks) n'est pas plus glorieux. Ils ont pourtant permis à la France et aux contribuables français de récupérer plusieurs milliards d'euros évadés dans des paradis fiscaux.

Tous les auteurs des attentats en France étaient déjà fichés, mais les services manquaient de moyens... ceux-ci étant progressivement alloués à la surveillance de masse

Les lois de surveillance post-attentats ont-elles signé l'arrêt de mort de nos libertés ?

En France, le recul sur les libertés individuelles, c'est-à-dire garante du fonctionnement démocratique du pays, ont factuellement nettement reculé en deux ans. D'après Montesquieu et les grands penseurs de la démocratie, cette dernière se fonde sur une série de libertés individuelles et sur la séparation des pouvoirs. En France, on tend vers un État d'exception permanent avec un pouvoir exécutif omniprésent. L'État d'urgence a retiré aux juges leur pouvoir de contrôle, les recours à l'article 49-3 puis aujourd'hui les ordonnances permettent de passer des lois sans les débattre à l'Assemblée.

Il faut une mobilisation dans la population pour revenir sur ces mesures d'exception et réintroduire des contre-pouvoirs. Concernant la vie privée en ligne, il y a en ce moment des débats cruciaux au parlement européen, notamment le règlement ePrivacy. **La Quadrature du Net**, une association qui fait beaucoup pour les libertés individuelles notamment en ligne, vient de lancer une campagne de mobilisation en France². Chacun peut y prendre part, contacter son député. Il y a eu ces dernières années plusieurs décisions intéressantes des juges (d'où l'importance des juges) de la Cour de justice européenne (Arrêts "Google Spain" et "Max Schrems") et le dernier règlement européen RGPD est intéressant, même si imparfait.

Toujours dans ce contexte, un récent projet de loi antiterroriste prévoit une "surveillance étendue". Qu'en pensez-vous ?

Le terrorisme est un vrai problème et qui a frappé tragiquement de nombreux innocents en France en Europe, mais aussi (et surtout) au Moyen-Orient. Il faudra un jour s'intéresser aux causes du problème. Ils ont notamment à voir avec la déstabilisation du Moyen-Orient (opérations en Irak, Libye, etc.) plutôt que de sacrifier tous les principes fondateurs de la démocratie. William Binney, ancien directeur technique de la NSA, explique dans *Nothing to Hide* comment la surveillance de masse est incapable de prévenir le terrorisme. Tous les auteurs des attentats en France étaient déjà fichés, mais les services manquaient de moyens... ceux-ci étant progressivement alloués à la surveillance de masse.

2. https://www.laquadrature.net/fr/campagne_eprivacy

Le constat est assez sombre aujourd'hui, mais il y a de nombreuses initiatives qui vont dans le bon sens. Il y a des fournisseurs d'accès à internet associatifs³ qui permettent de s'émanciper des grands opérateurs, il y a des "logiciels libres" et des alternatives à la quasi-totalité des services Google⁴ et autres. À ce sujet, on n'est pas obligé de quitter complètement Google. Ce dernier offre objectivement des services de qualité, mais il faut éviter de cumuler Google Search, Google Map, Google Mail, Google Doc...

On peut aussi aller à des CryptoParties⁵, aider financièrement les associations comme la Quadrature du Net. On peut installer le navigateur Firefox pour se connecter à ses mails et en parallèle le navigateur anonyme Tor pour ses recherches quotidiennes.

Enfin, et c'est le plus important, il faut relancer le débat public. Montrer à ceux qui sont pour la surveillance de masse les dangers qu'elle implique et à ceux qui doutent que ce n'est pas une bataille perdue. La liberté n'a jamais été donnée, il a toujours fallu la conquérir puis la défendre. On dit parfois que la vie privée est la mère des autres libertés, et que, sans elle, il n'y a pas de liberté d'expression, de réunion, d'aller et de venir, de manifestation, etc.

3. <https://www.ffdn.org/>

4. <https://degooglisons-internet.org/>

5. <https://www.cryptoparty.in/location#france>

"NOTHING TO HIDE" : POURQUOI CE DOCU SUR LA SURVEILLANCE DE MASSE NOUS CONCERNE-T-IL TOUS ?

<http://www.lesinrocks.com/2017/09/09/cinema/nothing-hide-pourquoi-ce-docu-sur-la-surveillance-de-masse-nous-concerne-t-il-tous-11983255/>

Auteur : Bruno DERUISSEAU⁶

Publication : INROCKS (09 octobre 2017)

Grâce à la collecte de nos données numériques, les agences de renseignement disposent aujourd'hui d'un accès quasi-total à notre intimité. Sorti cette semaine, "Nothing to Hide" propose, en évitant l'écueil de la paranoïa, une prise de conscience des enjeux de la surveillance de masse et des moyens dont chacun dispose pour s'y soustraire.



Il était une fois internet. Le capitalisme pensa en tirer profit en proposant des contenus payants mais il s'avéra bien vite que les utilisateurs voyaient d'abord internet comme un espace de gratuité. Alors le capitalisme eut l'idée d'une surveillance invisible qui collecterait les données générées par les utilisateurs pour ensuite les vendre à des entreprises et des gouvernements. La surveillance de masse est née. L'observation de ce péché originel d'internet débouche sur une question avec laquelle ce passionnant documentaire ne cesse de tisser son propos : pourquoi m'inquièterais-je de la surveillance de masse puisque je n'ai rien à cacher?

6. <http://www.lesinrocks.com/auteur/bruno-deruisseau>

Alternant entretiens avec des spécialistes de la surveillance, des exemples concrets et une étude de cas, Nothing to Hide de Marc Meillassoux illustre le trajet d'une prise de conscience des dangers de la surveillance et pose avec intelligence et tempérance la question de l'intimité et de la capacité à se rebeller à l'intérieur d'une société qui dispose d'outils dignes d'un régime totalitaire.

Au fil de nos recherches, de nos conversations et de nos déplacements, le documentaire montre que nos téléphones portables et nos ordinateurs sont devenus les réceptacles d'informations qui permettent de connaître notre mode de vie, nos idées politiques, nos croyances, nos intérêts, notre vie social et nos pratiques sexuelles.

La possession de telles données recueillies massivement et revendues par notamment Facebook et Google permet déjà à des entreprises de nous proposer un contenu publicitaire ciblé et à l'Etat de contrôler la population. Mais d'autres pratiques pourraient voir le jour dans les prochaines années ; les compagnies d'assurance devraient nous proposer des prestations en rapport avec notre hygiène de vie, les banques, des prêts en fonction de la notation financière que nous aura octroyée Facebook et notre potentiel employeur pourrait même nous évaluer à partir de l'analyse des données qu'il aura en sa possession. Toutefois et sans tomber dans la paranoïa, il existe des outils qui permettent de réduire nos traces sur internet, comme l'évoque Marc Meillassoux dans l'entretien qu'il nous a accordé.

Comment est né le désir de faire un documentaire sur la surveillance de masse?

Marc Meillassoux – A la base, je suis plutôt journaliste spécialisé en économie, et j'écrivais sur l'économie du digital. J'ai rencontré Mihaela Gladovic, avec qui j'ai lancé le projet du film, et nous avons tous deux commencé à aller à des conférences sur la gestion des données privées et à des Cryptoparties. Les Cryptoparties sont des réunions libres et gratuites où les gens viennent avec leur téléphone portable et leur ordinateur et apprennent à protéger leurs données eux-mêmes. Et puis cela faisait longtemps que je m'intéressais aux théoriciens du panoptique (*procédé à la base utilisé dans l'architecture carcérale qui consiste à construire un point de vue où il est possible de tout voir de l'intérieur – ndlr*) comme Bentham et Foucault et aux écrits de Deleuze sur les sociétés de contrôle. Au moment des révélations Snowden, je me sentais incapable de réagir en raison de mon niveau en informatique. Mais après avoir comblé notre retard en fréquentant les Cryptoparties et la scène hacktiviste de Berlin, nous avons décidé de nous lancer dans ce documentaire.

Le film montre que l'état d'urgence et la surveillance de masse sont aussi bien utilisés pour lutter contre le terrorisme que contre le militantisme écologique et politique. Penses-tu qu'un tel climat de contrôle de la population arrange les gouvernements ?

C'est une question compliquée car il y a toujours le risque de verser dans la paranoïa et le complotisme. Cela fait six fois que l'état d'urgence est prolongé et ça pourrait durer car le gouvernement le renouvelle aussi pour se couvrir devant l'opinion en cas de nouvel attentat. Ce qui est sûr, c'est que l'état d'urgence donne des outils sans précédent pour contrôler et neutraliser toutes sortes d'activistes. Durant la COP 21, on a ainsi vu que les services de renseignements français utilisaient ces outils pour dresser des profils de militants qui n'avaient jamais rien fait d'illégal mais qui, pour reprendre le terme de leur "*note blanche*" : "*représentent une menace pour les institutions de l'Etat*". C'est le cas montré dans le film où Joël Domenjoud a fait l'objet d'une

surveillance physique et numérique et a été assigné à résidence simplement pour avoir participé à des manifestations de militants écolo.

Penses-tu désormais être l'objet d'une surveillance particulière du fait de ce documentaire ?

Nous sommes potentiellement tous surveillés. Snowden a dévoilé que la NSA fonctionnait selon un système à deux cercles. Si un individu se retrouve en contact avec un individu déjà surveillé, il se retrouvera automatiquement surveillé, tout comme tous ses propres contacts. Ce qui veut dire que, si je suis surveillé, tu l'es automatiquement ainsi que toutes les personnes avec qui tu communique. C'est inquiétant, surtout quand on sait qu'avec les réseaux sociaux, nous ne sommes plus qu'à cinq poignées de main de n'importe qui dans le monde.

Y a-t-il un pays où la surveillance de masse est moins pratiquée ?

Pas vraiment, à part l'Islande et deux ou trois autres pays, tous pratiquent la surveillance de masse. Les Etats-Unis allouent un budget énorme à la surveillance mais les services secrets français sont aussi très réputés en la matière, tout comme les services secrets allemands, russes ou turcs. Il y a des scandales dans pratiquement tous les pays, qu'ils viennent d'agences de renseignement privées ou publics. Au moment du Printemps arabe, une société française avait par exemple été mise en cause pour avoir vendu des informations au régime syrien. Comme le dit William Binney, ex-directeur technique de la NSA, "nous avons propagé un cancer à travers le monde".

On pourrait déjouer cette surveillance en n'ayant pas de téléphone portable et en refusant de s'identifier devant un ordinateur mais le documentaire montre qu'il existe d'autres moyens moins radicaux.

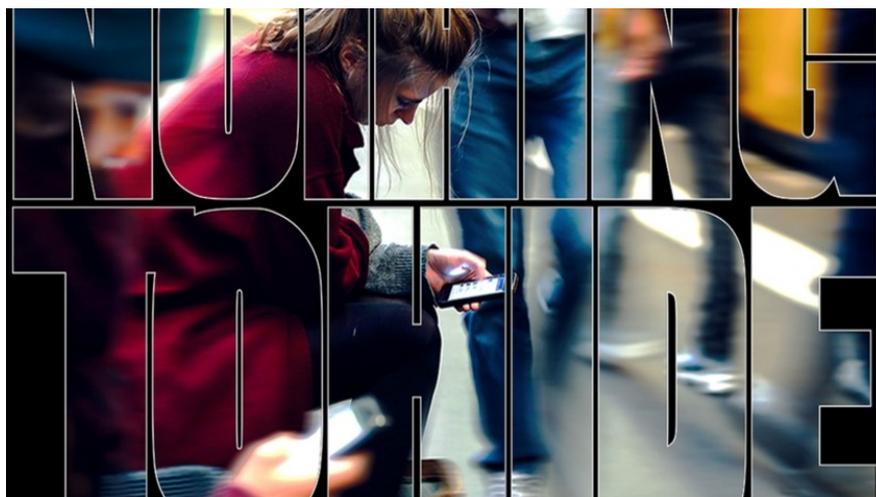
Oui, je travaille d'ailleurs actuellement sur un second documentaire qui s'intéresse aux différentes formes de disparitions numériques. Même s'il est très difficile de se protéger contre la NSA, on peut assez facilement effacer certaines traces vis-à-vis de la surveillance privée, comme celle exercée par Google, en utilisant des moteurs de recherche comme DuckDuckGo ou le navigateur anonyme Tor, en utilisant des logiciels libres comme Linux ou en utilisant une messagerie instantanée comme Signal. Il y a différents niveaux de protection et il n'est pas nécessaire d'aller au stade le plus extrême pour avoir une utilisation d'internet qui soit satisfaisante. Pour estimer les traces que chacun laisse derrière soi sur internet, il existe par ailleurs un site qui s'appelle Myshadow.org. J'essaie personnellement de ne pas prendre ça comme une paranoïa mais plutôt comme une forme de jeu, de challenge : comment laisser le moins de trace possible. [...]

"NOTHING TO HIDE" N'AVOIR "RIEN À CACHER" N'EST PAS UN ARGUMENT

<https://usbeketrica.com/article/pourquoi-n-avoir-rien-a-cacher-n-est-pas-une-raison-pour-accepter-la-surveillance-de-masse>

Auteur : Annabelle LAURENT

Publication Usbek & Rica: (20 octobre 2017)



“Je n’ai rien à cacher”, “je n’ai rien de fait de mal ni d’illégal donc peu importe si on m’espionne”. C’est l’argument auquel se heurtent systématiquement les défenseurs de nos libertés numériques. Mais n’avoir “rien à cacher”, et accepter de livrer toutes ses données à Facebook, Google et à une multitude de services “gratuits” tout en sachant, de façon plus précise depuis les révélations d’Edward Snowden, que ces données alimentent directement la surveillance de masse : est-ce vraiment un raisonnement tenable sur le long terme ? Est-ce la société que nous voulons ? Diffusé en salles depuis quelques mois, avant une mise en ligne sous licence Creative Commons prévue pour le 30 septembre, le documentaire “Nothing to Hide” de Marc Meillassoux est une réponse passionnante à cette question cruciale pour notre avenir.

Juin 2013. De la chambre d’hôtel de Hong-Kong où il est reclus, Edward Snowden observe le scandale des écoutes de la NSA éclater en direct à la télévision, à l’issue des huit jours pendant lesquels il vient de tout révéler aux journalistes devant la caméra de Laura Poitras (Citizenfour). Depuis, quatre ans ont passé. Et si Prism - du nom du programme de la NSA conçu pour scanner les communications numériques échangées sur AOL, Apple, Facebook, Google, YouTube, Microsoft, Skype, Paltalk et Yahoo! - et plusieurs affaires qui ont suivi ont largement contribué à éveiller la conscience des citoyens sur les données et la surveillance de masse, la plupart d’entre eux ont fini par se désintéresser de la question, sous prétexte qu’ils n’ont “rien à cacher”.

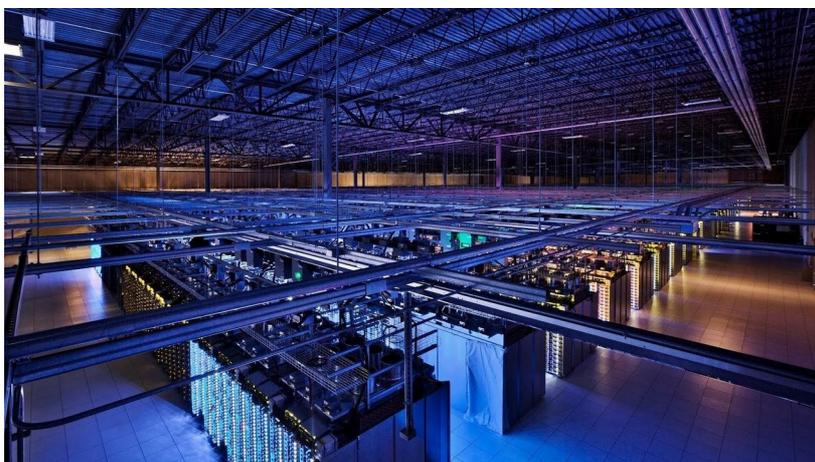
La société et ses données d'abord

"Dire que votre droit à la vie privée importe peu car vous n'avez rien à cacher revient à dire que votre liberté d'expression importe peu, car vous n'avez rien à dire. Car même si vous n'utilisez pas vos droits aujourd'hui, d'autres en ont besoin. Cela revient à dire : les autres ne m'intéressent pas" : Edward Snowden, qui témoigne dans Nothing to hide parmi une vingtaine d'autres intervenants, est toujours sur la même ligne, celle qui consiste à faire passer l'intérêt de la société devant les considérations individuelles. C'est aussi ce à quoi invite ce documentaire réalisé par deux journalistes, le Français Marc Meillassoux et l'Allemande Mihaela Gladovic.

Deux approches permettent de contrer l'argument "je n'ai rien à cacher" : prendre conscience, d'une part, que tout le monde a quelque chose à cacher - et que ce quelque chose s'appelle l'intimité - ou pourrait avoir quelque chose à cacher : *"Imaginons que vous n'êtes pas engagé politiquement, ou que votre vie n'est actuellement pas très excitante. Vous vivez à la campagne et une compagnie pétrolière vient construire un gazoduc sur vos terres. Tout à coup, vous avez quelque chose à cacher, et vous avez un adversaire"*, suggère par exemple Alison Macrina, du projet Tor.

"Il faut se demander ce que c'est de vivre dans une société où nos juges, avocats, chercheurs et journalistes sont potentiellement surveillés et sous contrôle"

L'autre réponse est celle qui consiste à vouloir refuser les prémisses d'un Etat policier. "Il n'y a pas un argument valable pour tout le monde, nous détaille l'auteur du documentaire, Marc Meillassoux. Certains réagissent sur les notations financières en craignant d'avoir à payer plus cher leur emprunt ou leur assurance maladie selon ce que leurs données auront révélé de leur mode de vie. D'autres sont sensibilisés à la notion du tabou et à ce qui doit rester dans la sphère privée, par exemple si une personne de leur famille est touchée par une maladie mentale. D'autres peuvent avoir peur que le fisc ait accès à leurs données personnelles. Notre documentaire veut davantage insister sur le second aspect, sociétal : une tyrannie, qu'elle passe par une agression physique extérieure ou par la scrutation permanente de la population, reste une tyrannie. La surveillance policière est le fondement d'un État policier. Il faut se demander ce que c'est que de vivre dans une société où nos juges, avocats, chercheurs et journalistes sont potentiellement surveillés et sous contrôle."



Un Mister X pour cobaye

Nothing to Hide est riche de ses intervenants, nombreux et pertinents (lanceurs d'alerte, chercheurs, militants, hackers, etc.), qu'il fait dialoguer avec les témoignages de victimes des politiques de surveillance, parmi lesquelles une chercheuse en droits fondamentaux surveillée aux Etats-Unis (parce qu'elle a rencontré des femmes somaliennes, égyptiennes, irakiennes, afghanes et yéménites) ou un militant écolo surveillé en France. Le récit d'une ancienne activiste allemande surveillée dans les années 1980 par la Stasi introduit le parallèle avec le service d'espionnage de la RDA et les outils de surveillance actuels.

"Ils partagent la même obsession de tout récolter, ce même appétit sans fin pour les données, commente Marc Meillassoux. Avec l'idée que le moindre détail qui serait passé au travers sera considéré comme une faille dans le système de surveillance". Ainsi, considérer qu'on n'a "rien à cacher" est une chose, mais comment ne pas s'inquiéter que "tous les mécanismes de surveillance soient déjà en place", comme l'explique le lanceur d'alerte et ancien cadre de la NSA Thomas Drake, même s'ils sont encore, la plupart du temps, dans les mains de démocraties ? Est-il alors excessif de parler de cyberdictature ?

L'autre fil rouge du documentaire est l'expérience de surveillance à laquelle se livre Mr. X, un ami du réalisateur qui pensait n'avoir "rien à cacher", en acceptant d'être surveillé pendant un mois sur son téléphone, sur lequel est installé un logiciel espion (qui n'a pas accès au contenu des messages), et sur son ordinateur, dont est récolté l'historique de navigation. Une analyste de données et un hacker se font ensuite un plaisir de lui présenter le fruit de leur travail : une cartographie complète de ses déplacements (dont ils déduisent ses heures de sommeil, travail, sorties, s'il fait une nuit blanche, dort au même endroit), des détails extrêmement précis sur son mode de vie ou ses fréquentations. Le tout en utilisant simplement les "métadonnées" (données de connexions, heures et fréquences d'appels, positions GPS, etc.) auxquelles ils ont accès et sur lesquelles reposent les dispositifs de surveillance du Web de la "loi renseignement" adoptée en France en 2015, et des lois équivalentes adoptées ailleurs en Europe.

Alors que le Conseil national du numérique (CNNum) s'alarme des menaces que fait peser sur les libertés individuelles le projet de loi antiterroriste dont l'examen a démarré le 13 septembre à l'Assemblée, signe supplémentaire d'une trajectoire sécuritaire jugée "préoccupante", il n'est jamais superflu de revenir aux fondements de la société de surveillance, du "péché originel" d'Internet (c'est-à-dire l'acceptation de la gratuité des services en échange du tracking publicitaire) à sa transformation en un espace de contrôle qui nous fait ressembler chaque jour un peu plus au personnage de Winston dans 1984, le roman de George Orwell. Il est sans doute encore moins vain de s'intéresser, trois ans après Citizenfour et sa figure de héros incarnée par Snowden, à la façon dont chacun de nous participe, activement ou par défaut, à la validation de ce système de surveillance. [...]