Snowden et l'avenir, partie IV :

L'avenir de la liberté

Eben Moglen

Professeur de droit à l'Université de droit de Columbia à New York, Fondateur, directeur du Software Freedom Law Center

Traduit de l'anglais par :
José Fournier, Caroline Laurent, Geoffray Levasseur et Yanick Roger
Relecture et corrections de :
Geoffray Levasseur, Caroline Laurent, Éric Guirbal et Clara Janin

Université de droit de Columbia

4 décembre 2013

Bon après-midi.

Nous devons maintenant porter notre attention sur ce que M. Snowden nous a appris en ce qui concerne la portée de notre problème, considérer avec son aide ce que nous pouvons faire pour concevoir nos réponses.

Nous avons observé cela avec l'acharnement des opérations militaires. Ceux qui écoutent aux États-Unis, se sont embarqués dans une campagne contre la vie privée de l'humanité. Ils ont, à travers de larges couches de l'humanité mis en péril la confidentialité, détruit l'anonymat et ont porté atteinte à l'autonomie de milliards de gens.

Ils firent cela parce qu'ils s'étaient vus confier une mission par un gouvernement national imprudent aux États-Unis ; celui-ci ayant échoué à éviter une très sérieuse attaque sur les civils états-uniens chez eux, en ignorant largement les avertissements, décréta qu'il ne serait plus jamais mis dans une situation où il aurait dû savoir.

Cela eut pour conséquence une réponse militaire, qui est de se rapprocher du toute chose autant que faire se peut. Parce que si vous ne vous tenez pas aussi proche que possible de toute chose, comment auriez-vous pu dire que vous connaissiez chacune des choses que vous auriez dû connaître ?

Le problème fondamental était le problème politique, pas le problème militaire, si on se met à réfléchir. Quand les chefs militaires reçoivent des objectifs, ils les atteignent quel qu'en soit le coût collatéral qui ne leur a pas été interdit. C'est leur travail. Et si vous employez le général Curtis Le May[1] pour résoudre un problème et que vous obtenez une destruction à grande échelle, eh bien, c'est pour cela que vous avez fait appel au général Curtis Le May. Le général Le May avait raison de dire, que si les États-Unis avaient perdu la Seconde Guerre mondiale, lui et son état-major auraient été jugés pour crimes de guerre. Du point de vue du général Le May cela voulait dire qu'il avait fait son travail.

Ce n'est pas à eux, les soldats et les espions, de déterminer par eux-mêmes si leurs comportements est incompatible avec la morale de la liberté. C'est la raison pour laquelle nous considérons que la démocratie requiert, parmi d'autres choses *sine qua non*, le contrôle civil des activités militaires. Lorsqu'une administration des

1 Curtis Emerson LeMay, né le 15 novembre 1906 à Columbus (Ohio) et mort le 1er octobre 1990, est un général des forces aériennes des États-Unis. Il est connu pour ses positions bellicistes qui tendaient à aggraver les tensions lors de graves crises internationales.

États-Unis particulièrement imprudente abandonna l'État de droit en ce qui concerne ceux qui écoutent, se réfugiant derrière le simulacre d'une Cour désignée et opérant en secret, les conséquences ne furent pas que les oreilles des militaires aient à juger par eux-mêmes. Comme nous l'avons vu, M. Snowden a insisté pour que ce soit à la démocratie de fixer les limites de ce comportement. La démocratie — M. Snowden est d'accord avec M. Jefferson[2] sur ce point, et avec presque n'importe qui d'autre qui a un jour pensé sérieusement à cela — la démocratie exige une citoyenneté informée.

Pour cette raison, M. Snowden a sacrifié son droit à toute chose que nous chérissons, notre vie privée, notre sécurité, notre futur, afin d'informer les citoyens des États-Unis et du monde.

Ce que nous affrontons, comme nous l'avons vu, est une calamité environnementale[3]. Elle résulte des dommages collatéraux de cette écoute militaire : cela a été entrepris avec une efficacité acharnée, par des gens qui disposent de plus de moyens que toutes les autres oreilles réunies du reste du monde[4] ; ils pouvaient légitimement considérer que la mission première que leur avait confiée un gouvernement imprudent, leur conférait le pouvoir, et en réalité leur donnait l'ordre, de se rapprocher sans autre limite que le possible, de toute chose, en la pillant.

En conséquence, ils ont corrompu le monde de la science, ils ont mis en péril la sécurité du commerce et ils ont détruit la vie privée et l'anonymat de personnes qui vivent sous le contrôle de gouvernements despotiques et qui sont en danger à cause de ce qu'ils croient et à cause de ce comportement destructif. Et, aussi longtemps que cela sera encore appelé une guerre, pour autant que cela les concerne, ils seront encore en train d'accomplir leur mission.

Nous n'avons pas de réponse simple à chacune des questions qui sont posées, comme avec les autres calamités environnementales que la race humaine doit affronter. Une chose seule ne fonctionne pas. Elle ne fonctionne même pas en un endroit précis, en oubliant le reste. Au contraire, nous sommes confrontés à un problème qui, parce qu'il s'agit d'une calamité environnementale, nous appelle à agir, comme nous le faisons, de notre mieux, en pensant globalement et en agissant localement. C'est à dire, en identifiant les principes qui doivent être appliqués en ce qui concerne ce cataclysme environnemental qui touche la vie privée et que nous connaissons actuellement, et en agissant là où nous vivons. Chacun d'entre nous doit agir de la manière qui convient au rôle qui est le sien et au lieu dans lequel il

2 Thomas Jefferson, né le 13 avril 1743, mort le 4 juillet 1826, fut le troisième Président des États-Unis d'Amérique. Il est connu pour avoir été un fervent droit-de-l'hommiste.

3 Voir *Snowden et l'avenir, partie III : L'Union, puisse-t-elle être préservé*, page 3.

4 Voir *Snowden et l'avenir, partie I : Vers l'ouest, le parcours de l'Empire*, page 3.

vit, conscient du fait que collectivement nous essayons de sauver la liberté de pensée et la démocratie pour l'humanité ; c'est impossible de les sauver autrement. Parce que nous avons été les témoins de la destruction de la liberté de pensée par la surveillance invasive et acharnée. Et sans liberté de penser, toutes les autres libertés ne sont que des privilèges concédés par le gouvernement.

Dans une telle situation, partout où nous travaillons, nous aurons à appliquer des mesures politiques aussi bien que techniques. Dans un sens, simplement pour empêcher le problème de s'aggraver, et dans un autre sens, pour commencer le processus d'inversion politique. Ce que tous les gens partout dans le monde réclament, partout où ils ont le droit à l'auto-détermination ou à la prise en compte de leur opinion, c'est de ne pas être espionnés.

M. Snowden nous a montré la complicité immense de tous les gouvernements, y compris ceux considérés comme adversaires des États-Unis sur bien des problèmes, vis à vis des écoutes venant des États-Unis. Ils bénéficient des fruits de la recherche conduite, dans la limite de ce que le gouvernement des États-Unis, par accord ou par générosité, est décidé à partager avec eux. Ils ont fermé les yeux sur la corruption de leurs opérateurs de communication, parfois dans le cadre de partenariats. Tous ces liens, dans bien des cas, remontent, comme M. Snowden l'a montré, jusqu'à la période qui a immédiatement suivi la fin de la Seconde Guerre mondiale. Ils se sont simplement renforcés avec le temps. Les moyens techniques que recouvraient les accords sont passés du télégraphe au téléphone, à travers la reconstruction du réseau de communication — en Europe, celui-ci avait été détruit par la Seconde Guerre mondiale. Maintenant, ils couvrent le réseau instantané à l'échelle planétaire dans lequel nous évoluons couramment aujourd'hui ; si nous ne faisons rien pour l'arrêter, il s'étendra plus loin, au cours de ce vingt-et-unième siècle, dans ce système neuronal unique connectant tous les humains dans un énorme réseau[5].

En d'autres termes, M. Snowden a montré que partout où les citoyens ont droit à la parole dans l'élaboration des politiques, ils ont été privés des politiques qu'ils souhaitaient pour leur gouvernement. En premier lieu, ils veulent un gouvernement qui les protège contre l'espionnage extérieur. C'est l'objectif fondamental des gouvernements de protéger les gens au nom desquels ils agissent, et en conséquence, il apparaît évident que les gouvernements doivent protéger leurs citoyens contre l'espionnage extérieur, où que ce soit. Et partout où les citoyens ont le droit d'exprimer leurs souhaits en ce qui concerne le gouvernement qui conduit la politique et la surveillance intérieure à des fins sécuritaires, ces citoyens ont la volonté qu'une telle surveillance intérieure à des fins sécuritaires et une telle conduite de la politique, soient assujetties à l'état de droit, sous le contrôle de n'importe quelle institu-

5 Voir *Snowden et l'avenir, partie I : Vers l'ouest, le parcours de l'Empire*, page 7.

tion locale, pour une protection solide contre tout gouvernement outrepassant ses prérogatives.

Aux États-Unis, nous devrons rajouter une troisième exigence politique à notre action. Les États-Unis, je veux dire le peuple des États-Unis, ne sont pas prêt à abandonner leur rôle de porte-drapeau de la liberté dans le monde. Nous ne sommes pas prêts à échanger notre rôle de diffuseur de la liberté dans le monde contre le rôle de diffuseur des processus du totalitarisme. Nous n'avons jamais voté pour cela. Le peuple des États-Unis ne veut pas devenir la police secrète du monde. Nous avons dérivé vers cela parce qu'une administration imprudente à donné aux militaires le pouvoir de faire ce que tout militaire fait, qui est de foncer en dépit des torpilles. Il est donc temps, pour le peuple des États-Unis, de faire part de leur décision sur le sujet.

En même temps, le président des États-Unis possède la seule voix nécessaire pour arrêter la guerre. Tout cela est possible parce que nous sommes en temps de guerre, ou plutôt à cause du mythe qui nous le fait penser.

Ignorer les libertés civiles du peuple des États-Unis pour des raisons de sécurité est possible en temps de guerre. Déclarer que toute personne sans passeport états-unien utilisant le réseau de télécommunication n'est pas sujette à la protection de ses libertés civiles, n'est possible qu'en temps de guerre. Et l'idée que nous pouvons abandonner la moralité de la liberté et diffuser les processus du totalitarisme à travers le monde à des fins de sécurité ne pourrait être possible qu'en temps de guerre. Cela ne peut pas être notre vision d'une société en paix. L'imprudence fondamentale a été l'utilisation, ouverte à la controverse, du privilège constitutionnel de partir en guerre sans une déclaration du Congrès, pour créer un état de guerre sans fin aux États-Unis.

Ceux qui ont fait ça seront jugés sévèrement par l'Histoire.

Et cela vaudra pour les gens qui ont refusé d'y mettre un terme.

Le président des États-Unis possède un vote et ce vote peut mettre fin à la guerre. Nos distingués et honorables collègues à la Cour Suprême de Justice des États-Unis, possèdent neufs votes susceptibles de restaurer l'État de droit. Pas de doute qu'ils n'ont pas envie de s'en servir, pour une multitude de raisons, dont certaines — avec lesquelles je pense que nous tous, les gens qui réfléchissons à la constitution, sommes d'accord — sont sérieuses. Mais le temps vient, pour eux, d'agir.

Tous ceux d'entre nous qui ont déjà servi le gouvernement fédéral, et je suis l'un d'entre eux, ont prêté le serment de préserver, protéger et défendre la constitution des États-Unis[6].

Certains vont devoir se souvenir qu'ils ont prêté ce serment.

Il arrive un moment dans l'histoire de la nation où les gens doivent se souvenir que le serment fonctionne ainsi, que c'est à la défense de l'ordre constitutionnel de l'Union que nous avons fait allégeance.

Une compréhension claire de ce fait nous a conduits aux moments les plus horribles de notre nation, et c'est ce qui a conduit M. Snowden à ce moment de rencontre avec la vérité.

Nous ne sommes pas le seul pays du monde à avoir des responsabilités politiques exigeantes. Le gouvernement du Royaume-Uni doit cesser d'attenter aux libertés civiles de son peuple, il doit cesser d'utiliser son territoire et ses moyens de transport comme des auxiliaires du comportement militaire des États-Unis. Il doit cesser de refuser la liberté de la presse, et d'oppresser les éditeurs qui cherchent à informer le monde sur les menaces pour la démocratie, alors qu'il est relativement compréhensif avec la presse qui enquête sur des filles assassinées.

La chancelière allemande doit cesser de parler de son téléphone mobile et doit commencer à se demander s'il est normal que tous les appels téléphoniques passés et que tous les SMS envoyés en Allemagne soient délivrés aux états-uniens — un sujet qui devrait faire l'objet d'une discussion nationale en Allemagne, mais que la chancelière cherche à éviter en parlant plutôt de son téléphone. Cette mascarade ressemble à l'une de ces conversations téléphoniques que vous entendez tout le temps en public, dans laquelle les gens sont occupés à se dire où ils se trouvent, mais n'en viennent jamais à dire à chacun ce qu'ils devraient réellement faire.

Les gouvernements qui opèrent dans le cadre d'une constitution qui protège la liberté d'expression doivent, en tant que sujet de moralité de la liberté dans leurs

6 Serment que doit prêter tout fonctionnaire titulaire de l'administration fédérale des États-Unis stipulé dans l'article « US Code, titre 5, partie III, sous-partie B, chapitre 33, paragraphe 3331 *Oath of office* (*Serment de service*) ». Il se traduit ainsi : « *Moi, [Nom], jure solennellement (ou affirme) que je maintiendrai et défendrai la Constitution des États-Unis contre tous ses ennemis, intérieur ou extérieur ; que j'y porterai une véritable foi et une entière allégeance ; que je prendrai cette obligation librement, sans aucune réserve intellectuelle ou possibilité d'échappement ; et que je vais correctement et fidèlement remplir les devoirs de la charge que je m'apprête à occuper. Que Dieu me vienne en aide.* ». Selon la fonction, des serments supplémentaires peuvent être nécessaires.

sociétés, se poser urgemment la question de savoir si la liberté d'expression existe quand toute chose est espionnée, surveillée et écoutée.

Au vingtième siècle, cela n'aurait pas été une question difficile, comme je l'ai mentionné au début de nos rencontres. Cela aurait été considéré comme simple et évident ; c'est la raison pour laquelle nous avons décidé de sacrifier des millions de vies pour détruire ce que nous appelions fascisme et totalitarisme.

Ce week-end, j'ai perdu un ami cher qui fût emprisonné par la Gestapo à Amsterdam en 1944. Cela me trouble de penser que, avec le départ de nos amis chers qui ont vécu à cette époque, nous puissions oublier ce qui arrive lorsque l'on n'attache pas assez d'importance à la moralité de la liberté.

Nous produisons et diffusons à travers le monde, aux dépends des contribuables des États-Unis, une technologie qui est en permanence l'objet d'une utilisation détournée pour soutenir le totalitarisme. Que les gens qui font cela veuillent nous faire croire qu'en tant que responsables états-uniens ils sont dignes de confiance, me paraît totalement dénué de tout rapport, ces derniers n'ayant rien à faire du problème éthique d'équiper de satanés despotes du vingt-et-unième siècle, avec la possibilité d'assurer l'immortalité de l'immoralité de leur pouvoir.

En plus de la politique, nous avons à légiférer. Dans un sens, j'ai déjà défini ce que ce travail sur la loi doit être : assujettir les choses à la Force de la loi dans les juridictions locales est le travail des juristes[7]. Et il est évident que, si notre politique locale à effet global est de chercher à assujettir les écoutes locales à la Force de la loi, alors les juristes devront s'en charger. Dans certains endroits, il leur faudra être très courageux ; partout dans le monde, ils devront être bien entraînés, partout dans le monde ils auront besoin de notre appui et de notre attention.

Mais, il est aussi clair que d'assujettir les écoutes du gouvernement à la Force de la loi n'est pas du seul ressort des juristes. Comme nous l'avons vu, les relations entre les oreilles militaires des États-Unis partout ailleurs dans le monde, et le grand marché de l'exploration de données qui a explosé au vingt-et-unième siècle est trop complexe pour être sans danger pour nous.

Les révélations continues de M. Snowden ont montré à quel point les géants de l'exploration de données aux États-Unis ont été intimidés, séduits et aussi trahis par ceux qui écoutent. Ce qui a tellement mis en colère *Google* et *Facebook*, c'est dans quelle mesure le contrat qu'ils avaient passé avec ceux qui écoutent, qui,

7 Voir *Snowden et l'avenir, partie II : Oh, liberté,* page 12.

pensaient-ils, leur apporterait une protection en retour de leur coopération, n'avait pas eu un tel effet du tout : ceux qui écoutes ont continué à attaquer leurs barrières de sécurité, à les espionner et à les piller de toutes les manières possibles. Cela n'aurait pas dû les surprendre, mais l'a cependant fait. Apparemment, ils ne pensaient pas qu'ils passaient un contrat avec une armée en temps de guerre. Je ne sais pas pourquoi.

Et nous ? Nous sommes conscients, qu'au début du vingt-et-unième siècle, le réseau était utilisé pour concentrer nos données dans les mains d'autres personnes. Comme nous le verrons, la conception technologique pour affronter la crise environnementale que nous traversons, suggère que nous devrions décentraliser les données, que nous ne devrions pas les stocker en de grands amas qui facilitent les recherches des gouvernements totalitaires et des autres.

Mais avant d'en arriver là, nous devrions comprendre qu'il y a beaucoup de gens de par le monde qui gèrent nos données, et qui n'en sont pas responsables. Il y a un travail de législation à faire dans ce domaine aussi.

Aux États-Unis par exemple, un de nos objectifs législatifs devrait être de supprimer l'immunité donnée aux opérateurs de télécommunication dans l'assistance apportée aux écoutes illégales aux États-Unis. L'immunité a été étendue par la loi de 2008[8]. Barack Obama, lors de sa course à la présidence disait qu'il allait faire obstruction pour retarder cette loi si constitutionnelle au Sénat des États-Unis... Bref, je ne vais pas parler à sa place. Puis en août 2008, quand il fut clair qu'il allait devenir président des États-Unis, il changea d'avis. Non seulement il laissa tomber sa menace d'obstruction à la loi, mais il pris l'avion pour revenir de sa campagne à Washington DC afin de voter pour elle au sénat des États-Unis : une des rares choses dont il pensait qu'elle méritait un peu de son temps fut de voter au sénat en tant que candidat à la présidence en 2008.

Nous ne devrions pas discuter sur le fait de savoir si l'immunité aurait dû être étendue aux opérateurs à l'intérieur des États-Unis ; ce n'est pas une question importante pour le moment. Nous devons fixer une date, certains disent le 1er janvier 2017[9], date après laquelle, peut-être, tous les opérateurs de réseaux de télécommunications opérant aux États-Unis et qui facilitent les écoutes illégales par le gouvernement états-unien seront assujettis à la responsabilité civile ordinaire sans immunité. Aucune loi particulière, pour rendre quiconque responsable de quoi que ce soit, n'est nécessaire, simplement annulons l'immunité. Une coalition intéressante entre les juristes des droits humains et cela aurait d'énormes conséquences

8 *Fisa Amendment Act* (*FAA*), H. R. 6304, 110th Congress, 9 juillet 2008. Qui accorde l'immunité aux opérateurs des États-Unis sur toutes écoutes d'intérêts étrangers.

9 *A priori*, date approximative d'investiture du futur président des États-Unis (vers le 20 janvier).

positives sur les citoyens des autres pays également. C'est le cas partout où l'immunité est actuellement en place et peut être retirée en reconnaissant que, dans la majorité des endroits où l'immunité dans l'aide apportée aux écoutes illégales du gouvernement existe, les citoyens ne l'ont jamais observé dans des termes législatifs. Cela a simplement été fait par le gouvernement dans leur dos, derrière des portes closes, dans l'obscurité. Dans tous les endroits ou l'immunité peut être retirée par des moyens légaux, elle doit l'être. Aider les gens à vous espionner quand on a pas le droit de le faire est une conduite que la loi, presque partout, a parfaitement compris et vous fait porter une responsabilité depuis des centaines, si ce n'est pas des milliers, d'années. Il n'y a aucune raison de réclamer de nouvelles lois à ce sujet ; nous avons simplement besoin de juristes qui la font appliquer.

De la même façon, nous devons reconnaître que cette énorme masse de données nous concernant qui se retrouve entre les mains d'autres individus n'est pas un problème inconnu pour la loi. Bien au contraire, les principes légaux les plus élémentaires qui ont à voir avec sont les mêmes que ceux que vous rencontrez quotidiennement lorsque vous allez au pressing. Les juristes anglophones parlent de « contrat de dépôt ». Voici ce que cela signifie réellement : si vous faites confiance à quelqu'un au sujet de vos affaires personnelles, il doit en prendre soin comme si elles lui appartenaient, et s'il n'agit pas de la sorte, il est alors tenu pour responsable de son éventuelle négligence.

En tant qu'historien du droit, je peux vous assurer que la loi anglaise a eu besoin de plusieurs siècles de travail et de nombreuses hésitations et d'annulations de principes temporairement acquis pour en arriver à cette conclusion. Mais que vous soyez un juriste du monde anglophone ou non, ces grands principes ont, de fait, été déployés avec les lois commerciales romaines aux débuts de notre civilisation — je parlais d'ailleurs assez grossièrement il y a quelques semaines du moment où la République de Rome fût détruite de l'intérieur par un tyran rusé répondant au nom d'Auguste[10], qui avait assuré à tout le monde qu'ils possédaient toujours leurs anciennes libertés alors qu'il les leur subtilisait, construisant dans le même temps un réseau de renseignement qui fit de lui l'homme le mieux informé au monde.

Donc ce dont nous avons réellement besoin, c'est de voir ce principe de confiance par contrat de dépôt, ou quelque soit le vocabulaire législatif local, appliqué à toutes les données que nous avons confiées à d'autres individus et qui ont la responsabilité d'y faire attention au moins autant qu'aux leurs.

A partir de là, je partage par sympathie l'embarras des ingénieurs de *Google* qui ont réalisé qu'en levant tous les encodages des données de tierces personnes qui sont

10 Voir *Snowden et l'avenir, partie I : Vers l'ouest, le parcours de l'Empire*, page 1.

parvenues aux frontières de *Google*, et qu'en les faisant passer d'un data-center à un autre via des fibres optiques sans les ré-encoder, ils ont pour ainsi dire invité ceux qui écoutent à venir se servir. Les loups sont entrés par la porte de derrière, après avoir rondement mené leur affaire à la porte principale. Mais à vrai dire, évidemment qu'ils auraient dû savoir que leurs ordinateurs auraient dû n'être liés que par des connections chiffrées. Même dans le petit bureau où je travaille c'est ce que nous faisons.

Le véritable problème réside en ce que les militaires qui écoutent ont corrompu il y a une vingtaine d'années notre désir de faire en sorte qu'Internet soit dans son intégralité un réseau qui fonctionne ainsi — c'est-à-dire chiffré d'un bout à l'autre —, avec leurs objections obscurantistes, les efforts menés pour remettre ces questions à plus tard, et en niant la nécessité de chiffrer le Net d'un bout à l'autre. Pourquoi ? Parce-que si nous avions construit cette technologie de la bonne manière, tout ce qui aurait transité leur aurait été plus difficile à dérober. Nous devons en revenir là. Évidemment, nous devons le faire par nous-mêmes, qui que nous soyons : *Google*, les banques, les hôpitaux, ou tout simplement nos familles.

Mais du point de vue du travail des juristes autour du monde, il y aurait un énorme avantage à traiter les données personnelles selon les règles du contrat de dépôt, dans le sens où nous appliquerions alors des principes familiers à nos affaires personnelles placées entre les mains d'autrui.

Les règles concernant nos affaires qui son gardées par d'autres personnes, sont qu'elles possèdent leur existence morale, qu'elles se réfèrent au lieu où nous les avons invoquées, là où le contrat de confiance a été établi. Si le blanchisseur choisi de déplacer vos vêtements à un autre endroit et qu'alors surviens un incendie, ce n'est pas l'endroit ou le feu est intervenu et où ils ont déplacé vos affaires qui détermine la responsabilité, c'est l'endroit ou ils vous ont pris vos affaires.

Les grands géants de l'exploration de données tout autour du monde jouent au jeu du *lex loci server*[11] tout le temps : « *Oh nous ne sommes pas vraiment à X, nous sommes en Californie, c'est là que se trouvent nos ordinateurs.* »

C'est une mauvaise habitude juridique. C'est comme si manger de la mauvaise nourriture conduisait à cette chicane juridique qui supposerai que cela vous garderait en bonne santé pour toujours. Ça fonctionne jusqu'à ce que ce soit fait, et alors ça ne fonctionne plus et alors quoi ? Nous ne leur rendrions réellement pas un mauvais service en les aidant à sortir de cette mauvaise habitude, en leur démontrant que ce dont ils ont vraiment besoin est une stratégie légale pour gérer la rela-

11 Loi de localisation des serveurs.

tion de confiance avec les gens qu'ils possèdent, où que ces personnes se trouvent. À long terme, cela ne leur fera aucun bien de nier qu'ils se trouvent à tel endroit. Et si nous en étions à appliquer les bons principes de responsabilité légale pour leur attention, soit appropriée, soit négligente, des affaires sous leur contrôle, nous aurions fait un travail suffisant. Ce n'est pas une solution à tous les problèmes, pas plus que les principes de responsabilité sur la détérioration de l'environnement ne règlent le problème de la pollution. Mais cela produit la possibilité de décisions productives que nous appelons « négociations sous le couvert de la loi ».

Si vous voulez, nous allons avoir besoin d'une loi privée internationale pour la vie privée. C'est à dire, de principes de choix des lois dans le monde qui relient les diverses formes de contrat de confiance et de contrat de dépôt — ainsi que des choses comme « mes affaires entre vos mains » et « les choses que je vous ai confiées pour que vous en preniez soin » —, dans les divers systèmes légaux. Ce n'est pas un travail de traités internationaux produit par les gouvernements. Les gouvernements ne sont pas intéressés : au contraire, les gouvernements sont tous complètement à l'opposé de ceci.

Alors, il y a du travail à faire dans les lois publiques internationales. C'est-à-dire, la question de savoir comment les gouvernements devraient être concernés par la dévastation de l'environnement.

Les deux gouvernements les plus puissants du monde, les États-Unis d'Amérique et la République Populaire de Chine, sont maintenant fondamentalement d'accord à propos de leur politique sur le traitement des menaces sur le réseau. Le principe de base est : « Quel que soit l'endroit sur Internet où existe une menace à notre sécurité nationale, nous la pourchasserons. »

L'un des premiers stratèges (je me retiens de dire apologistes) pour la surveillance aux États-Unis, M. Stewart Baker[12] — avec qui mes relations remontent maintenant à bien trop de décennies — M. Baker a déclaré la semaine dernière qu'aux États-Unis il est bon pour le gouvernement de conserver des traces des habitudes à regarder du porno de personnes à l'étranger qu'il considère comme étant les djihadistes ayant encouragés les attaques sur les intérêts états-uniens hors des État-Unis.

M. Baker a dit que mieux encore que les tuer, il fallait « *leur balancer la vérité à la gueule.* » J'ai ressenti que c'était l'équivalent pour Internet de cette vieille idée de la

12 Stewart Abercrombie Baker, né le 17 juillet 1947 fut le premier Secrétaire Assistant (équivalent en France des ministres délégués) à la politique du Département de la Sécurité Intérieure des États-Unis (*United States Department of Homeland Security*) sous la présidence de George W. Bush. Il a également été, de 1992 à 1996, conseillé général de la NSA.

CIA d'envoyer des agents à Cuba avec quelque chose à mettre dans les chaussures de Fidel Castro qui lui aurait fait tomber la barbe[13]. C'est un exemple supplémentaire de l'absurdité qui survient en temps de guerre, mais c'est aussi un rappel que la liberté de pensée est actuellement en danger pour les plus banales, de même que pour les plus importantes, des raisons une fois que les technologies du totalitarisme ont été propagées par nous, partout.

Par conséquent, il est raisonnable de se poser des questions sur les efforts que font ensemble les gouvernements pour réduire l'intensité de cette catastrophe environnementale.

Les États-Unis et l'Union Soviétique ont mis le monde en danger d'empoisonnement dans les années cinquante en testant des armes nucléaires, et on peut les créditer d'avoir, parallèlement à d'autre mesure empêchant la destruction du monde, été capables de passer des accords bilatéraux interdisant les tests atmosphériques d'armes nucléaires.

Ce qui — malgré les efforts toxiques occasionnels des français pour rappeler à tout le monde qu'ils n'avaient pas donné leur accord — a plutôt bien permis aux gens de se garder de faire péter des bombes atomiques[14] dans l'atmosphère et de détruire des civilisations humaines par accident.

Il est tout à fait raisonnable d'imaginer — en dépit du fait que les gouvernements n'ont pas l'intention de le faire — un accord entre le gouvernement des États-Unis et le gouvernement de la République Populaire de Chine pour cesser de transformer la race humaine en zone de tir libre pour les écoutes et les interférences. Mais ceci n'arrivera pas cette fois, comme si le Traité d'Interdiction des Essais[15] n'existait pas.

13 Allusion claire à l'épisode de la Baie des Cochons. Le débarquement de la Baie des Cochons est une tentative d'invasion militaire de Cuba par des exilés cubains soutenus par les États-Unis en avril 1961. Planifiée sous l'administration de Dwight Eisenhower, l'opération était lancée au début du mandat de John F. Kennedy. Elle visait à faire débarquer à Cuba, le 17 avril 1961, environ 1 400 exilés cubains recrutés et entraînés aux États-Unis par la CIA afin de renverser le nouveau gouvernement cubain établi par Fidel Castro, qui menait une politique économique défavorable aux intérêts états-uniens et se rapprochait de l'URSS. L'opération fut un échec complet.

14 Moglen utilise le mot familier « nukes ». Globalement sa phrase est volontairement familière et pleine de mépris, dans le but d'afficher son dégoût pour les armes nucléaires.

15 Le Traité d'interdiction complète des essais nucléaires ou TICEN ou encore TICE (en anglais *Comprehensive Test Ban Treaty*) est un traité international interdisant tout essai nucléaire ou tout autre type d'explosion nucléaire, que ce soit à des fins pacifiques ou militaires, dans quelque environnement que ce soit. Le TICEN a été ouvert à la signature le 24 septembre 1996 à New York, aux États-Unis. Il n'est toujours pas entré en vigueur. Pour ce faire, il faut que les 44 États repris dans l'annexe 2 du Traité ratifient le texte ; or, à la date du 29 septembre 2008, seuls 35 d'entre eux l'ont fait.

Maintenant, tout cela — toute ces politiques et lois — sont malheureusement lentes et incertaines, et dans leur meilleur achèvement, elles ne sauraient suffisamment arrêter la dégradation de notre intimité dans cet espionnage omniprésent sur le Net, ceci même si elles se mettaient en place avec une rapidité suffisante. Sans solutions techniques appropriées on ne pourra pas tout à fait réussir, tout comme il n'y a pas de moyens de nettoyer l'air et l'eau ou d'effectuer des changements positifs sur le climat sans changements technologiques.

Partout dans le monde les entreprises utilisent des logiciels qui sécurisent leurs communications et la plupart de ces logiciels sont créés par nous. Le « nous » dont je parle ici sont les rassemblement de gens partageant les progrès techniques appelés logiciels libres[16], logiciels open-source, avec lesquels j'ai travaillé pendant des dizaines d'années.

Les protocoles qui réalisent des communications sécurisées, utilisées par les entreprises entre elles et avec leurs clients — HTTPS[17], SSL[18], TLS[19], OpenVPN[20], toutes ces techniques de sécurisation des communications sur Internet — ont été la cible de ceux qui écoutent et de leurs interférences. M. Snowden nous a montré avec beaucoup de détails le niveau d'efforts intenses déployé pour casser ces formes fondamentales de communication sécurisée.

Je dois de nouveau faire remarquer qu'en exerçant une telle pression sur cette technologie, ils courent le risque d'un désastre financier international. S'ils avaient réussi dans leur atteinte aux protocoles par lequel les entreprises font des échanges sécurisés au niveau mondial nous aurions été à deux doigts du chaos global.

Les armées sur le champ de bataille, combattant avec ordre de faire quoi que cela puisse coûter, feront de telles choses. Mais, lorsque l'histoire sera écrite, l'imprudence du gouvernement des États-Unis à avoir libéré ses oreilles militaires à ce tel

16 Logiciel dont le code, la recette en quelque sorte, est public. Toute personne est libre d'utiliser sans aucune restrictions d'usages ces logiciels. Il est aussi possible à toute personne compétente de l'étudier, le modifier et d'en publier les modifications.

17 HTTP est l'acronyme de « *Hyper Text Transfer Protocol* » pour « *protocole de transfert hypertexte* ». Ce protocole de transfert de données permet d'afficher des pages Internet dans un navigateur. Le S à la fin de HTTPS signifie « *Secure* » ou « *Safe* » pour dire « *sécurisé* » : il s'agit en fait de la version chiffré de ce protocole.

18 Acronyme de « *Secure Socket Layer* » pour « *couche de branchement sécurisé* », un système d'établissement de connexions sécurisées (c'est-à-dire chiffrées) entre deux appareils dans un réseau.

19 Acronyme de « *Transport Socket Layer* » pour « *couche de branchement de transfert* », système proche de SSL et dont le rôle est similaire.

20 Permet de créer des réseaux privés virtuels, ou « *Virtual Private Network* » en anglais, c'est-à-dire un système abstrait permettant de considérer plusieurs ordinateurs distants comme étant sur le même réseau local. L'ensemble des transfert entre les machines d'un VPN sont chiffrés.

point, sera le premier titre. Cette conduite apparaîtra dans le futur comme représentant le même degré d'acharnement économique que la dévaluation de la monnaie romaine hier et aujourd'hui : c'est une menace fondamentale à la sécurité de l'économie dans le monde.

Les mauvaises nouvelles sont les différentes sortes de progrès qu'ils ont fait : tout d'abord, ils ont corrompu la science. Ils ont affecté dans l'ombre la production de normes techniques de manière fondamentale, affaiblissant la sécurité de chacun, partout, pour rendre leur travail plus facile... Dans les prochaines semaines, j'aurai des discussions techniques plus détaillées sur ce point, avec des chercheurs qui peuvent parler avec autorité, à la fois de ce que les documents disent et de ce qu'ils signifient.

En second lieu, ils se sont engagés dans le vol de clé de chiffrage à un niveau que vous ne pouvez réaliser que si vous êtes le voleur le mieux financé au monde. Partout où les clés de chiffrage sont incorporées dans le matériel, ils sont allés là où les composants sont fabriqués. Ils ont collecté d'immenses piles de clé, qu'ils conserve à portée, avec les équipes superbement talentueuses pour les voler, qu'ils ont spécialement entraînes.

Début septembre, lorsque les documents de Mr. Snowden sur ce sujet ont été rendus publics dans le *New York Times*, l'onde de choc de cette découverte s'est réverbérée tout autour du monde industriel. Ils faisaient référence à une version précoce de leur effort de « key recovery »[21] pour voler systématiquement les clés utilisées pour des communications mondiales sécurisées dans les affaires sous le nom de code de « *Manassas* ». Par la suite, ils l'améliorèrent beaucoup. C'est la documentation de la version améliorée numéro 2 qu'ils baptisèrent « *Bull Run* »[22], que Mr. Snowden a publié début septembre.

Nous pouvons bien sûr faire des conjectures sur le fait — peut-être devrions-nous assumer — qu'en s'adressant à ses propres responsables, la National Security Agency ne dit pas l'entière vérité dans ces documents.

Mais la très grande satisfaction qu'ils expriment dans l'extension de la « key recovery » — qui est une activité de vol de clés — et la documentation qui en découle, constatant jusqu'où ils ont pénétré par effraction dans les infrastructures de *Google*, de *Facebook*, et d'autres lieux, en ne cassant pas le chiffrage SSL entre le

21 Récupération de clés.

22 Bull Run (littéralement « Course de taureaux ») est un programme états-unien secret, utilisé par la NSA, ayant pour but de casser les systèmes de chiffrement (SSL, TLS, VPN...). L'équivalent britannique s'appelle *Edgehill*. L'existence du programme a été révélée en septembre 2013.

monde extérieur et le monde des affaires, tend à confirmer le fait le plus important que M. Snowden a essayé de nous faire saisir en utilisant les documents de l'agence même : Ils préfèrent — ou ont choisi par nécessité, comme c'est certainement le cas — voler des clés, plutôt que de casser la cryptographie fondamentale qui sécurise l'économie mondiale, qui est essentiellement élaborée, selon des principes coopératifs, par mes clients[23].

C'est le premier facteur incendiaire concernant les révélations de M. Snowden, du point de vue de la NSA : dire aux gens ce qu'ils peuvent lire ou pas, c'est ce que ceux qui écoutent devraient plutôt cesser que faire . Parce qu'aussi longtemps que personne ne sait ce que vous pouvez lire vous êtes réputé omniscient, et si quelqu'un sait ce que vous ne pouvez pas lire, alors tôt ou tard vous ne pourrez plus rien lire du tout. Donc ce que M. Snowden a fait, c'est nous révéler que leur avance sur notre chiffrement fondamental était bonne mais pas excellente. Il nous a montré qu'ils gagnent du terrain par la force brute, plutôt qu'en utilisant des fusées magiques construites en zone 51[24] contre lesquelles nous ne saurions rivaliser.

Mais M. Snowden nous montre aussi qu'il nous reste très peu de temps pour améliorer notre propre cryptographie, qu'il nous reste très peu de temps pour récupérer des dommages que nous avons subis à cause de la corruptions des normes techniques, et qu'à partir de maintenant tous les gens qui réalisent des logiciels libres de chiffrement pour les mettre à la disposition de tous doivent assumer qu'ils sont contre « les moyens nationaux du renseignement », qui essayent de casser leur technologie et d'organiser la subversion de leurs organisations. Dans cette affaire, c'est une mauvaise nouvelle pour les développeurs, parce que c'est jouer dans la cour des grands et si vous devez jouer avec eux à chaque instant alors une seule erreur est fatale.

Ce qui veut dire sur le plan technologique que nous devons faire deux choses dés maintenant. La première c'est que ceux qui le peuvent doivent se coaliser pour renforcer la commodité du chiffrement de base dans le monde libre et nous devons le faire tout de suite. Ceux qui écoutent savent qui ils sont, et ce sont des jeunes à travers le monde qui ont un grand destin devant eux, non pas en travaillant affranchis des barrières de sécurité à l'intérieur de la *National Security Agency*, mais pour la liberté.

23 Les clients de Moglen sont tous des acteurs du logiciel libre, à travers sa fondation, la *Software Freedom Law Center*.

24 Zone du Nevada aux États-Unis où se trouve une base militaire dite secrète, testant entre autres des appareils expérimentaux. Elle est mentionnée pour la première fois sur des documents officiels américains déclassifiés en août 2013.

Mais la seconde chose que nous devons faire, c'est de changer l'environnement pour les gens pour le rendre plus sûr. Cela constitue à diffuser largement les technologies que le monde des affaires utilise depuis quinze ans maintenant dans les vies des gens ordinaires. Ce qui ne s'est pas passé, vous comprenez.

La cybersécurité est une activité professionnelle très développée de nos jours. Les responsables de la sécurité de l'information sont des gens compétents qui effectuent un travail compliqué, mais à la fin de la journée, ils mettent en place des réseaux qui sont plus sûrs pour les entreprises qui les emploient. Nous pouvons le faire aussi. C'est comme si chaque usine aux États-Unis possédait un système de sprinkler[25] avancé — des détecteurs de fumée, des détecteurs de mono-oxyde, des sprinklers, des conduites haute pression, des extincteurs perfectionnés — alors que la maison de tout un chacun n'aurait ni détecteur de fumée, ni extincteur, ni retardateur de flamme, rien.

Donc, ce que nous devons faire, c'est de rendre pratique l'utilisation personnelle des technologies que les entreprises ont déjà complètement adoptées, et nous devons les mettre à la disposition des gens dans des modalités qui ne réclament pas plus de savoir faire que pour installer un détecteur de fumée, accrocher un extincteur au mur, apprendre à leur enfant par quelle porte s'échapper si les escaliers sont en feu — peut-être installer une échelle de corde à la fenêtre du deuxième étage. Rien de tout cela ne règle le problème de l'incendie. Rien de tout cela ne rend la distribution d'électricité plus sure. Ça n'empêche pas les coups de foudre. Ça ne règle rien à propos du manque de moyens alloués au département incendie. Rien de tout cela. Mais si un incendie se déclare dans votre maison, ça sauvera la vie de votre enfant.

Donc nous devons faire cela aussi. Il y a maintenant des projets autour du monde qui travaillent là-dessus. Mon projet de *FreedomBox*[26] en est un ; il y en a des tas d'autres. Mais je suis particulièrement heureux de voir que nous commençons à rencontrer des compétiteurs commerciaux. Je lisais une publicité sur routeur *Tor*[27] basé sur une prise-serveur à 49 $ la semaine dernière. Les entreprises sont aujourd'hui conscientes : les peuples du monde ne sont pas d'accord pour le fait que l'étau de la technologie du totalitarisme devrait être resserré sur chacune des mai-

25 Extincteur automatique à eau utilisé dans certains bâtiments publiques ou dans des bâtiments pour lesquels l'accès aux pompiers est difficile, notamment les gratte-ciels.

26 *FreedomBox* est un projet communautaire visant à développer, concevoir et promouvoir l'utilisation de serveurs personnels fonctionnant à base de logiciels libres pour fournir des services de réseaux sociaux distribués, courrier électronique et communications audio/vidéo. Le projet a été annoncé par Eben Moglen à New York le 2 février 2010. Sa première version est sortie le 27 août 2012.

27 *ToR* (acronyme de « *The Onion Router* », littéralement le routeur oignon) est un réseau informatique superposé mondial et décentralisé, implémentation du principe de réseau mélangé « *mix network* ». Il est composé de routeurs organisés en couches, appelés nœuds de l'oignon, qui transmettent de manière anonyme des flux sur Internet.

sons par les États-Unis et des gouvernement sympathisants dans leur pays. Non seulement les peuples du monde ne sont pas d'accord sur cela d'un point de vue politique, mais ils ne sont pas d'accord sur cela d'un point de vue commercial non plus.

Ainsi, si nous préservons un solide chiffrement à portée de tous et continuons à fabriquer des prototypes de choses conçues pour aider les gens à avoir une meilleure vie privée et la sécurité dans leurs communications, le marché le gérera. Les fabricants tout autour du monde qui font des tas de choses avec le gouvernement, feront aussi quelques choses sans ce gouvernement parce qu'il y a de l'argent à gagner.

Donc, nous devons assumer nos deux principales responsabilités fondamentales, celles que les communautés de l'élaboration de logiciel ont poursuivies avec sans relâche elles-mêmes, si ce n'est sous une forme militaire, depuis de décennies maintenant : imaginer ce qui est bon pour la liberté, le faire, le partager avec les gens, laisser d'autres personnes l'utiliser pour leurs affaires, ne pas entraver l'amélioration. Tout ira bien pour nous, mais seulement parce que M. Snowden nous a dit ce que nous pouvons faire, et ce que nous ne pouvons pas faire, ce qui est déjà perdu, et quelles défenses marchent encore — nous serons sauvés parce qu'il a fait ça pour nous.

Autrement, les types de *Manassas* et de *Bull Run* vont continuer, et s'ils continuent, ils vont atteindre un point où nous aurons beaucoup de mal à inverser ce qu'ils auront fait. Parce que c'est comme ça que ça se passe dans les catastrophes environnementales. Vous ne pouvez tout simplement plus revenir en arrière.

M. Snowden est un homme conscient du temps aussi bien que de l'espace et de la force. Il a dit à Hong Kong : « *J'ai été un espion toute ma vie.* » Il a espionné pour nous, rassemblant pour nous avec précaution — en réfléchissant — avec comme objectif de nous rendre capable de comprendre et de répondre pour sauver la liberté humaine et la démocratie. Précautionneusement, en réfléchissant, lentement il a amassé. À partir du moment où il a eu le premier document en sa possession, il s'est trouvé en danger mortel. Chaque jour il est allé au travail. Chaque jour il a fait plus que ce dont nous aurions eu besoin si nous avions été prêts à nous défendre nous-mêmes contre ces attaques militaires contre la vie privée de l'humanité.

Son courage est exemplaire. Mais il a mis fin à ses efforts parce que nous avions besoin de savoir maintenant. Nous avions à hériter de sa compréhension de cette urgence impérieuse.

Sur le plan politique, nous devons nous assurer que les responsables des démocraties, tous, savent que nous n'avons pas voté pour cela. Nous n'avons pas voté ailleurs dans le monde pour être espionné par les États-Unis sans autorisation.

Nous autres, aux États-Unis n'avons pas voté pour que nous cessions d'être le porte étendard de la liberté dans le monde. Nous n'avons pas voté pour, au lieu de cela, devenir la police secrète de partout. Nous n'avons pas donné notre accord pour que l'État de droit disparaisse aux États-Unis ; pas seulement en ce qui concerne ceux d'entre nous qui ont le passeport mais en ce qui concerne toutes les personnes qui vivent ici.

C'est un engagement fondamental ; nous ne pouvons pas nous écarter de cela. Quand nous nous écartons de l'idée que toute personne qui vit ici possède des droits constitutionnels sans tenir compte du fait qu'elle a ou pas le passeport, nous ne faisons que remettre Dred Scott[28] d'actualité.

Peut-être pouvons-nous faire cela en temps de guerre. Mais, nous sommes partis en guerre dans le passé pour empêcher que cela ne fût la règle en temps de paix. Notre politique ne peut pas attendre sur ce point. Pas aux États-Unis où la guerre doit prendre fin. Pas à travers le monde où les peuples doivent demander que les gouvernements remplissent les obligations de base pour protéger la sécurité de leur peuple. Si la chancelière allemande pense que son téléphone mobile ne doit pas être écouté, je suis avec elle. Je ne suis pas avec elle quand elle oublie toutes ces autres personnes dont elle est la première responsable du bien-être.

Sur le plan législatif, nous avons des endroits à visiter et des choses à faire. De merveilleux juristes de par le monde, jeunes et vieux, ont du travail à faire et ils vont le faire. Mais ils vont avoir besoin de soutien. Ils vont avoir besoin d'infusions de courage et de bien-être matériel, et dans quelques endroits en lutte dans le monde, ils vont avoir besoin de notre volonté à nous tenir à coté d'eux contre l'intimidation physique et la destruction.

Nous avons des camarades au Bahreïn qui sont torturés parce qu'ils ont apporté un *iPhone* lors d'une manifestation, et qu'ils ont été dénoncés. Nous devons faire quelque chose à ce sujet. En tant que juristes, nous devons reconnaître que la vie dans une société de surveillance invasive n'est pas une vie dans un état de droit. Cela ne devrait même pas être discuté et pourtant ça l'est. Sur le plan technologique, nous devons soutenir les quelques milliers de nous-autres à travers le monde

28 Dred Scott est un esclave états-unien d'origine africaine né en 1795 en Virginie et mort le 17 septembre 1858. C'est une figure important de l'anti-esclavagisme aux États-Unis.

qui fabriquent les technologies de base dont des entreprises qui engrangent des centaines de milliards de dollars par an dépendent.

Nous devons soutenir ces technologies contre les attaques les plus expertes dont nous avons entendu parler. Nous devons assumer que chacune de celles-ci ont été tentées, et que chacune des choses qui pouvaient être faites pour corrompre les mathématiques fondamentales l'ont été. C'est un effort immense — un projet ambitieux pour nous, mais nous devons le faire. Et alors, comme le fameux *US Moonshot*[29], nous devons distribuer des *Tang*[30] et des couvertures spatiales, et peut-être quelques ustensiles plus utiles à ces gens : les technologies de l'aérospatiale qui marchent à la maison.

La bonne nouvelle c'est que beaucoup de nos ordinateurs portables font chacune des choses dont nous parlons. Je regarde autour de moi dans cette salle et je vois bon nombre de personnes dont les mécanismes technologiques pour protéger leur vie privée seraient suffisants si nous les multiplions par un milliard de personnes. Nous devons décentraliser les données, vous comprenez. Si nous les maintenons en une grande pile unique — s'il y a un gars qui conserve tous les courrier électroniques et un autre gars qui s'occupe du partage social à propos du licenciement — alors il n'y a aucun moyen d'être plus protégé que le lien le plus faible autour de cette pile.

Mais si chacune des personnes garde ses propres courriels, alors les liens faibles ouverts au monde extérieur ne laissent à l'assaillant que les affaires d'une seule personne. Ce qui dans un monde qui est gouverné par la force de la loi, peut être précisément optimal : une personne est la personne que vous pouvez espionnée parce que vous avez une raison probablement.

Les courriers électroniques fonctionnent bien sans quelqu'un en position centrale qui les conserve tous. Nous devons réaliser un serveur de courrier électronique pour les gens qui ne coûte que cinq dollars et se place dans la cuisine tout comme on avait l'habitude de mettre le répondeur téléphonique, un point c'est tout. S'il tombe en panne on le jette.

Le partage social décentralisé est plus difficile, mais difficile au point que nous ne saurions le mettre en place. Il y a trois ans, j'en ai appelé à cela. Un travail merveilleux a été fait qui n'a pas produit des choses que tout un chacun utilise, mais elles sont encore là : elles ne peuvent pas s'en aller, il s'agit du logiciel libre, il atteindra sa pleine signification bientôt.

29 Surnom donné au programme spatial états-unien *Apollo* de la NASA.
30 *Tang* est une boisson sucrée non gazeuse, au goût de fruit et non gazeux.

Pour les as de la technologie qui sont engagés à travers le monde, c'est le grand moment, parce que si nous faisons notre travail correctement la liberté survivra et nos petits-enfants diront : « *Alors, qu'est-ce que tu as fait ? — J'ai amélioré le SSL…* »

Et si nous ne le faisons pas…

La semaine dernière, aux États-Unis, nous étions en train de célébrer nos vacances annuelles du « *Thanks Giving* ». Chaque année, quand nous le faisons, nous évoquons les « P*ilgrim Fathers* »[31]. Les émigrants religieux venus d'Angleterre à Plymouth, Massachusetts, par les Pays-Bas en 1620 pour vénérer Dieu et penser comme il l'entendaient. Les deux premières années ils furent envoyés dans ce qui était considéré comme une terre inhabitée — pleine de gens qui savaient comment en vivre alors qu'eux ne savaient pas — furent extrêmement difficiles. Pendant deux hivers consécutifs, il y eut la famine et beaucoup d'enfants moururent.

Au cours du deuxième hiver, en 1621, certains de leurs confrères — des chrétiens congrégationaliste d'Angleterre qui pensaient à finalement émigrer pour aller avec la colonie de Plymouth — leur écrivirent pour les encourager à tenir bon contre l'hiver horrible qu'ils connaissaient. La lettre qu'ils écrivirent ne put même pas être délivrée au Massachusetts avant le printemps. L'océan Atlantique était infranchissable, mais ils avaient ouvert leurs cœurs à leurs collègues en lutte, envoyé leur message dans le vide, si loin dans une contrée si amèrement froide.

Les mots qu'ils écrivirent sont des mots que je dirais aujourd'hui à M. Snowden : « *Ne soyez pas tristes, écrivaient-ils, parce que vous avez été l'instrument qui a brisé la glace pour les autres. Vous serez honorés jusqu'à la fin des temps.* »

Nous ne rencontrons pas souvent, le temps d'une vie humaine, un moment de tel héroïsme, et nous oublions ce que nous devons faire quand nous l'avons rencontré. M. Snowden a fait avancer nos efforts pour sauver la démocratie avec noblesse et en le faisant il s'est tenu sur les épaules d'autres personnes : de M. Assange[32], Mlle

31 Les *Pilgrim Fathers* (ou *Pères Pèlerin* en français) sont l'un des premiers groupes de colons britanniques installés, après leur traversée à bord du *Mayflower*, sur le territoire des futurs États-Unis d'Amérique. Dissidents anglais, ils ont fui les persécutions religieuses et l'instabilité de l'Europe afin de trouver une terre vierge où créer une « *nouvelle Jérusalem* ». Les *Pères Pèlerins* n'étaient pas des puritains. Ils étaient des séparatistes qui voulaient se séparer de l'Église d'Angleterre contrairement aux puritains qui voulaient purifier et réformer l'Église d'Angleterre.

32 Julian Paul Assange, né le 3 juillet 1971, est un informaticien et cybermilitant australien. Il est surtout connu en tant que fondateur, rédacteur en chef et porte-parole de *WikiLeaks*. Sous le coup d'une extradition demandée par la Suède, il vit actuellement à l'ambassade d'Équateur à Londres depuis juin 2012.

Machon[33], M. Binney[34] et M. Drake[35]. L'honneur leur en reviendra, mais la responsabilité nous en incombe. Nous devons voir en cela que ces sacrifices n'ont pas été vains. Nous devons en tirer les enseignements.

Ils ont recherché le combat et une dure voie. Ils se sont mis en danger. Ils ne nous ont rien garanti, mais ils nous ont offert l'occasion d'assurer aux générations qui suivront que nous leur avons donné un monde aussi libre que celui que ceux qui nous ont précédé nous ont transmis.

Et donc, c'est à nous, les vivants, dont les vies n'ont pas été affaiblies pas la force de l'oppression, qui n'ont pas été soumis au fouet — c'est à nous de finir le travail qu'ils ont commencé. Nous devons y voir que leur sacrifice a un sens. Que cette nation, et toutes les nations, doivent connaître une renaissance de la liberté, et que le gouvernement du peuple, par le peuple, pour le peuple, ne disparaîtra pas de la terre.

Merci beaucoup.

33 Annie Machon, née en 1968, est une ancienne officier de renseignement du MI5 (pour *Military Intelligence section 5*, le service de renseignement britannique) qui a quitté le service en même temps que son partenaire, David Shayler, afin de l'aider à pointer du doigt les activités criminelles opérées au sein de l'agence. Ce faisant, elle du abandonner sa carrière, fuir à travers l'Europe, vivre cachée pendant des années, puis passer deux ans en exil à Paris. Elle, ainsi que nombre de ses amis, sa famille, ses soutiens et les journalistes qui l'ont publiée, déclarent avoir été intimidée, et certains d'entre eux ont été traduit en justice. Des menaces de mort lui ont été transmise via des radios à forte écoute.

34 William Edward Binney est un ancien employé haut gradé de la NSA connu pour avoir été un lanceur d'alerte en 2001, après avoir travaillé 30 ans au sein de l'agence. Il démissionne le 31 octobre 2001. Il a durement critiqué l'administration Bush. Il a été la cible d'une enquête du FBI et en particulier d'un raid sur son domicile en 2007. Lors d'une audition, il a témoigné sous serment que la NSA violait délibérément la constitution des États-Unis.

35 Thomas Andrews Drake, né le 22 avril 1957 en Louisiane aux États-Unis, est un ancien cadre supérieur de la NSA, vétéran de l'armée de l'air et de l'aéronavale. Il est principalement connu pour avoir été un lanceur d'alerte à propos de la mauvaise gestion du programme *Trailblazer* de modernisation de la NSA.

Œuvre originale disponible à l'adresse http://snowdenandthefuture.info/PartIV.html.