16 Avril, 2008

Dr. Alex Türk
Président, Groupe de travail Article 29 sur la protection des données
European Commission
Directorate General Justice, Freedom and Security
C 5 Data Protection Unit , secretariat WP art 29
46 Rue du Luxembourg
1000 Brussels Bruxelles

AMERICAN CIVIL LIBERTIES UNION

TECHNOLOGY AND LIBERTY PROGRAM

PLEASE RESPOND TO:
WASHINGTON, DC OFFICE
915 15th STREET, NW, 6TH FL.
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
F/212.549.2629

Cher Dr. Türk:

Nous voudrions prendre l'occasion de vous exprimer, à vous et à vos collègues, nos soucis concernant la nouvelle surveillance extra-judiciaire des activités d'européens et d'autres étrangers qui est en trâin d'être effectuée par le gouvernement des Etats-Unis sur la base de données relatives au trafic (*traffic data*) et de communications relatives aux matières (*content communications*) . Nous croyons que cette surveillance contravient aux exigences pour la protection de la vie privée sous l'article 8 de la "Convention européenne des Droits humains" et donc à la Directive 1995 de l'U.E. sur le traitement d'information de caractère personnel et la Directive 2002 sur la vie privée. Les fournisseurs de services de télécommunications à travers l'Europe et autour du monde qui offrent des services de communications aux européens sont susceptibles d'être dans la violation de ces lois. En plus, la sécurité des communications des citoyens de l'Europe et des personnes avec qui ils communiquent, y compris des américains, est en péril significatif.

L'Agence de Sécurité Nationale (la N.S.A.), l'agence du gouvernement des Etats-Unis qui est responsable pour la espionage électronique, a fortement augmenté son pouvoir ces dernières années. Son "programme de surveillance de terroristes" (T.S.P.) est le système ultime de surveillance de communications, comprenant des liens directs dans l'infrastructure de communications, permettant à la N.S.A. l'accès à des centaines de millions ou même à des billions de communicatons de voix ou de données.

Ce programme de surveillance a généré un degré significatif d'inquiétude et de controverse aux Etats-Unis. L'Administration du président George Bush et le Congrès sont entraînés en discussions sur les mesures à prendre pour sauvegarder les communications de citoyens des Etats-Unis en train de communiquer à l'intérieur du pays. D'ailleurs, ce programme a mené à des procès dans les cours américaines contre des compagnies importantes de

télécommunications.

Mais, malgré la discussion courante aux Etats-Unis sur les droits de la vie privée des américains dans leurs communications dans le pays, les engagements légaux qui devraient s'appliquer aux compagnies américaines de télécommunications, et les limites des protections constitutionnelles, les communications des citoyens européens demeurent ouvertes pour l'abus par le gouvernement des Etats-Unis.

Une grande partie des communications du monde entier voyage par des centres de commutation aux Etats-Unis. Par exemple, la plupart du trafic sur l'internet entre l'Asie et l'Europe passe par les Etats-Unis. La carte suivante (source: *Wired News*) des communications de téléphone illustre cette situation d'une manière frappante.

Pareillement, des transactions et l'email de l'internet entre européens sont envoyés de plus en plus par des serveurs dans les Etats-Unis. Nous soumettons pour votre considération l'article joint de *Wired News* qui récapitule cette situation.[1]

Cette situation ressemble de plusieurs manières au cas SWIFT: des transactions entre deux individus en Europe pourraient bien passer par des compagnies de télécommunications américaines et, par conséquence, seraient accessibles au gouvernement américain. La base légale de cet accès est de nouveau contestable. Encore une fois, des compagnies européennes sont en train d'utiliser un réseau qui fournit des informations directement aux autorités américaines.

---

1 Ryan Singel, "NSA's Lucky Break: How the U.S. Became Switchboard to the World," Wired Magazine, Oct. 10, 2007; http://www.wired.com/politics/security/news/2007/10/domestic_taps.

Ainsi que dans le cas SWIFT, cette surveillance est facilitée par des rapports de collusion entre le gouvernement américain et les opérateurs du réseau. Depuis 2005, on apprend de plus en plus sur la nature de ces rapports. Nous savons que la N.S.A. est maintenant capable de brancher sur les hubs importants, ce qui la permet de gagner l'accès direct à un nombre de communications sans précédent, et puis de filtrer, passer au crible, analyser, lire ou partager ces communications comme elle veut. D'ailleurs, la N.S.A. ne vise pas seulement des individus, mais en plus elle emploie des systèmes de data-mining pour évaluer les communicatons des millions de personnes à l'intérieur ou à l'extérieur des Etats-Unis.[2]

Cette activité n'entraîne aucun règlement ni protection légale pour des personnes qui demeurent en dehors des Etats-Unis. Par conséquence, les communications de citoyens de l'Europe sont tout-à-fait vulnérables à l'abus. L'accès et l'exploitation (*mining*) des informations personnelles sur une échelle si grande mènent souvent aux positifs faux, par exemple. Par des accords de partage de données (*data sharing*), les données qui sont collectionnées par ce programme de surveillance pourraient être et seront partagées avec d'autres agences du gouvernement et avec d'autres gouvernements, y compris des gouvernements européens. Cela veut dire qu'un positif faux qui est produit par un quelconque ordinateur de data mining de la N.S.A. pourrait avoir des conséquences pour un citoyen européen en Europe.

A notre avis il est clair que cette situation viole les exigences légales européenes relatives au traitement juste et légal des informations du caractère personnel. L'administration du président Bush ne tient aucun compte des protections même les plus fondamentales qui sauvegardent le traitement automatisé des données (*data processing*), en particulier à l'égard de communications qui ne font que passer par les Etats-Unis, ne concernent pas des américains.

Cette surveillance étendue de communications européenes est susceptible à décourager la libre expression, violer la vie privée, réduire la confiance entre personnes, et produire de l'incertitude, minant la liberté sur laquelle dépendent le gouvernement démocratique, le bonheur personnel, et la vitalité sociale. En même temps, elle pourrait empêcher des entreprises de pratiquer la communication ouverte à cause d'inquiétudes relatives à la manipulation économique. Enfin, en créant des portes arrières à nos canalisations de communication, la N.S.A. a ouvert des brèches de sécurité qui pourraient etre

2 Eric Lichtblau et James Risen, "Spy Agency Mined Vast Data Trove, Officials Report," New York Times, December 24, 2005; http://www.nytimes.com/2005/12/24/politics/24spy.html

exploitées par d'autres personnes—une chose qu'on a déja vue en Grèce et en Italie.3

Il y a beaucoup de choses qu'on pourrait faire pour améliorer cette situation. La sécurité de communicatons en Europe n'a jamais été plus vulnérable, et nous devrions tous réevaluer comment nous pouvons protéger la sécurité de communications dans l'âge moderne, voyant en particulier les développments en Europe, à l'étranger, et sur le plan international.

En particulier:

1. Les fonctionnaires et les gouvernements européens doivent travailler avec l'administration du président Bush pour assurer et la transparence et l'autorisation légale de la surveillance. Pour le moins, les gouvernements européens doivent travailler pour gagner des assurances fortes contre l'abus étendu et l'usage secondaire des informations glanées de cette surveillance, qu'ils soient faits exprès ou non.

2. Nous devons tous considérer le rôle joué par les fournisseurs de télécommunications européens et leurs confrères américains. En vue du cas SWIFT, il nous faut une plus grande compréhension des accords entre ces sociétés. En plus, il faut étudier les compagnies d'internet pour voir comment la N.S.A. ou d'autres programmes de surveillance gagnent accès aux emails, voyant que des communications à l'intérieur d'un pays utilisent souvent les services d'email qui demeurent sur les serveurs à l'étranger.

3. Nous devrions tous étudier et favoriser des mesures technologiques qui pourraient être dévelopés pour assurer la sécurité de communicaitons sans égard à leur destination, leur source ou même leur chemin.

4. Chaque pays doit étudier les accords de partage de données (*data sharing*) entre son gouvernement et les Etats-Unis pour faire certain que ces gouvernements n'utilisent pas des mesures de surveillance de communication qui sont extra-judiciaires ou étrangères à leur pays pour avancer leurs propres projets de surveillance contre leurs propres

---

3 Susan Landau, "A Gateway for Hackers: The Security Threat in the New Wiretapping Law," Washington Post, August 9, 2007; http://www.washingtonpost.com/wp-dyn/content/article/2007/08/08/AR2007080801961.html; et Steve Bellovin, Matt Blaze, Whitfield Diffie, Susan Landau, Peter Neumann, Jen Rexford, "Risking Communications Security: Potential Hazards of the Protect America Act," IEEE Security and Privacy (Jan/Feb 2008), pp. 18-27; http://research.sun.com/people/slandau/PAA.pdf.

citoyens.

5. Enfin, il faut dévéloper des moyens pour renseigner les européens sur la nature de ce programme de surveillance, et assurer qu'ils sont offert des choix pour pouvoir éviter l'examen minutieux par des gouvernements étrangers.

Donc, nous voudrions suggérer que l'article 29 Working Partry étudie cette situation. Il y a beaucoup de ressemblances entre cette situation et le cas SWIFT: des compagnies européenes traitent avec d'autres compagnies qui rendent leur données disponibles au gouvernement des Etats-Unis sans assez de règlement, de transparence ni d'avertissement à leurs clients. En même temps, cette situation ressemble à celle du transfert d'archives relatives aux noms de voyageurs dans la mesure où des accords internationales seront nécessaires pour assurer que des données relatives aux citoyens d'Europe sont traitées légalement et justement dans un troisième pays. Nous sommes heureux de vous fournir des informations supplémentaires et nous sommes prêt à vous rencontrer à Bruxelles pour échanger des idées sur ce sujet.

Nous vous remercions pour l'occasion de vous apporter cette information à vous et à vos collègues estimés.

Agréez, cher monsieur, mes sentiments respectueux,

Barry Steinhardt
Director, Technology and Liberty Program
American Civil Liberties Union

AMERICAN CIVIL
LIBERTIES UNION