April 16, 2008

Dr. Alex Türk
President, Article 29 Data Protection Working Group
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

Dear Dr Türk,

We would like to take this opportunity to raise with you and your colleagues our concerns regarding new extrajudicial surveillance of European and other foreigners' activities that is being conducted by the United States on the basis of traffic data and content communications. We believe that this surveillance contravenes the requirements for the protection of the private life under article 8 of the European Convention on Human Rights and accordingly the EU Directive 1995 on the processing of personal information and the 2002 E.Privacy Directive. Telecommunications service providers across Europe and around the world that provide communications services to Europeans are likely to be in breach of these laws. And the communications privacy of European citizens and those persons, including Americans, with whom they communicate, is in significant jeopardy.

The National Security Agency (NSA), the U.S. government agency responsible for electronic eavesdropping, has significantly enhanced its powers in recent years. Its 'Terrorist Surveillance Program' (TSP) is the ultimate system of communications surveillance, involving direct links into the communications infrastructure which provide the NSA with access to hundreds of millions if not billions of voice and data communications.

This surveillance program has generated significant concern and controversy in the United States. The Bush Administration and Congress are locked in debate over measures to safeguard the communications of U.S. citizens communicating within the U.S. It has also led to lawsuits in U.S. courts against major telecommunications companies.

But despite the debate that is underway in the United States over the privacy rights of Americans in their domestic communications, the legal obligations that should apply to U.S. telecommunications companies, and the boundaries of U.S. constitutional protections, the communications of European citizens remain open for abuse by the U.S. government.

Much of the world's communications travel through switching points in the United States. For example, most of the Internet traffic between Asia and Europe passes through the United States. The following map (source: Wired News) of the world's telephone communications illustrates this situation starkly.

Similarly, Internet transactions and email between Europeans is increasingly sent through servers in the U.S. We are submitting for your consideration the attached article from Wired News that summarises this situation.[1]

In many ways this situation is similar to the SWIFT case: transactions between two individuals in Europe may well transit through U.S. telecommunications companies and as a result will be made accessible to the U.S. government. The legal basis of this access is again questionable. European companies are once again utilizing a network that is now feeding information directly to the U.S. authorities.

As in the SWIFT case, this surveillance is enabled by complicit relationships between the U.S. Government and network operators. Since 2005 we have been learning more and more about the nature of these relationships. We

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

know the NSA is now able to tap into major domestic American telecommunications hubs, which permits the NSA to gain direct access to an unprecedented number of communications, and then filter, sift through, analyse, read, or share those communications as it sees fit. Furthermore, the NSA is not just targeting individuals but is also using data mining systems to evaluate the communications of millions of people both inside and outside the United States.[2]

This activity involves no oversight or legal protections for non-U.S. persons. As a result, the communications of European citizens are completely vulnerable to abuse. Such blanket access and mining of personal information often leads to false positives, for example. Through data-sharing agreements, the data gleaned from this surveillance program can and will be shared with other government agencies and foreign governments, including European governments. That means that a false positive generated by some NSA data-mining computer could have consequences for a European citizen in Europe.

We believe that this situation clearly violates European legal requirements for the fair and lawful processing of personal information. Even the most basic protections safeguarding data processing are being ignored by the Bush Administration, particularly with regard to communications that merely pass through the U.S. and do not involve U.S. persons.

This extensive surveillance of European communications is likely to chill free expression, violate privacy, reduce interpersonal trust, and generate uncertainty, corroding the freedom upon which democratic government, personal happiness, and social vitality depends. It could also inhibit businesses from communicating openly due to concerns over economic manipulation. Finally, by creating backdoors into our communications pipelines, the NSA has opened security holes that could be exploited by others, as we have already seen take place in Greece and Italy.[3]

Much can be done to improve this situation. The privacy of communications in Europe has never been more vulnerable, and we all need to reassess how to protect communications privacy in the modern age, particularly in light of domestic, foreign, and international developments. In particular:

---

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

3 See Susan Landau, "A Gateway for Hackers: The Security Threat in the New Wiretapping Law," Washington Post, August 9, 2007; online at http://www.washingtonpost.com/wp-dyn/content/article/2007/08/08/AR2007080801961.html; and 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; online at http://research.sun.com/people/slandau/PAA.pdf.

1. European officials and governments must work with the Bush Administration to ensure transparency and legal authorisation for surveillance. At the very least, European governments must work to gain strong assurances against widespread abuse and secondary use of the information gleaned from this surveillance, whether intended or not.

2. We must all consider the roles played by European telecommunications providers and their U.S. counterparts. In the light of the SWIFT case, a greater understanding of the agreements between these firms is needed. We must also look at Internet companies to see how access to emails is provided to the NSA or other surveillance programs in the light of the fact that domestic communications often utilize email services that reside on foreign servers. Special attention must also be given to the treatment of communications traffic data.

AMERICAN CIVIL
LIBERTIES UNION

3. We should all investigate and promote technological measures that can be developed to ensure communications privacy without regard to their destination, source, or even path.

4. We need each country to investigate the data-sharing agreements between its government and the U.S. to ensure that those governments are not utilizing foreign and extrajudicial communications surveillance measures to advance their own surveillance plans against their own citizens.

5. Finally, we must develop a means to educate Europeans about the nature of this surveillance program, and ensure that they are given options for avoiding the extrajudicial scrutiny of foreign governments.

We therefore would like to suggest that Article 29 Working Party undertake a study of this situation. There are many similarities between this situation and the SWIFT case – European companies are transacting with other companies that are making their data available to the U.S. Government without adequate oversight, transparency, or notification to their customers. This situation is also similar to the passenger-name record transfer issue in that international agreements were needed to ensure that data on European citizens is processed fairly and lawfully in a third country.

We would be pleased to provide you with any additional information and are prepared to meet with you in Brussels to discuss this case.

We thank you for this opportunity to bring this information to you and your esteemed colleagues.

Best regards,

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

AMERICAN CIVIL
LIBERTIES UNION