Privacy "Myths" Listed by the U.S. Government Aren't So Mythical

The U.S. Mission to the European Union recently issued a document listing five alleged "myths" about privacy and law enforcement access to personal information in the European Union and United States. The document is an attempt to reassure Europeans who, hearing about laws such as the U.S.A. Patriot Act, are concerned about their data being accessed by the U.S. government. However, U.S. privacy laws are, in fact, far from adequate to protect Europeans' privacy, and such concerns are entirely legitimate.

Myth #1

The United States Cares Less about Privacy than the European Union.

The U.S. mission insists that it's a myth that "The United States Cares Less About Privacy than the European Union," citing our "common values" and "deeply rooted commitment to safeguard those values." While "values" and "commitments" are to be applauded, when it comes to concrete laws and institutions, the United States has the weakest privacy protections of any advanced western democracy:

- The U.S. has no overarching law comparable to the European Privacy Directive.
- The few sectoral laws we have in areas such as communications, financial, and medical privacy are weak and riddled with loopholes.
- There are no independent privacy or data protection officials. Our "Privacy Officers" report to and work at the behest of their agencies' directors.
- The privacy protections of the Fourth Amendment to the U.S. Constitution have none of the sweep or force of the European declarations of rights such as the ECHR. Current jurisprudence has largely failed to keep pace with new practices and technologies.

Myth #2

The European Union Does a Better Job of Protecting Data from Law Enforcement Access than the United States.

The U.S. mission asserts that *"The United States Provides Broad Protections for the Privacy of Electronic Communications."* That contention is increasingly untenable.

In fact, electronic communications privacy in the U.S. is governed by a patchwork of confusing legal standards that have been interpreted inconsistently by the courts, creating uncertainty for users, service providers, and law enforcement agencies. Because the law has not kept pace with technological developments, the vast amount of personal information generated by today's digital communication services may no longer be adequately protected.

In short, there are gaping holes in legal protections afforded to electronic communications, including:

- **Archaic laws.** The principle electronic privacy law in the U.S. was enacted in 1986, before many of the technologies now used to communicate were even invented—including text messaging, cloud email providers, and the World Wide Web. One result is that the law currently makes a nonsensical distinction between communications that are "stored" and those that are "in transit." Indeed, a single email is subject to multiple different legal standards in its lifecycle, from the moment it is being typed to the moment it is opened by the recipient to the time it is stored with the email service provider. Overall, U.S. electronic privacy laws are a confusing, inconsistent patchwork.

- **The third-party doctrine.** The so-called "third party doctrine" provides that communications that have been "voluntarily disclosed" to a third party no longer receive constitutional protection. The U.S. Supreme Court has held, for example, that police do not need a judicial warrant to obtain a citizen's bank records, because that citizen has voluntarily shared them with the bank. In the age of cloud computing, this doctrine is a dangerous anachronism. Enormous amounts of private data – including our emails, our personal documents, and our location -- are "shared" with our digital service providers, thereby forfeiting constitutional protection.

- **The metadata exemption.** An archaic, judicially created distinction between content and metadata currently holds sway in U.S. privacy law. Metadata, such as the sender and recipient of a communication, can be accessed by the government without a warrant on the jurisprudential theory that such information is less worthy of privacy protection. Yet the identities of the parties a person has corresponded with can be at least as—and even more—personal than the content of those communications.

- **Location tracking.** The U.S. government has been arguing in court that location tracking data should not receive constitutional privacy protection. As the ACLU has discovered, hundreds of law enforcement agencies around the U.S. are currently accessing such highly personal data under inconsistent legal standards.

The U.S. mission states that *"The United States provides numerous protections from law enforcement access to electronic communications."* However, the proper question is not whether those protections are "numerous," but whether they are effective and up to date. The answer is no.

Layered protections

The US document also claims that "*The United States Has Adopted an Extensive Regime of Layered Oversight of Privacy Protections*." The document cites the checks and balances provided by the three-branch architecture (executive, legislative, and judicial) of the U.S. government, internal oversight officials within U.S. executive agencies, Congress's investigative and oversight powers, criminal prosecutions for unauthorized data access, and the availability of the courts as a check on executive power.

The reality is that many of these "layers" are paper thin, and the U.S. system as a whole fails to provide effective privacy protection. Among the layers cited in the document:

- **Privacy officers**. The United States is one of only two OECD nations (with Japan) that do not have an independent privacy or data protection official. Many agencies do not have a "Chief Privacy Officer"(CPO) at all. Even where they do exist, these officials are appointed by, and report to, the heads of their agencies, and have little or no independent authority. The Chief Privacy Officer of the Department of Homeland Security, for example, often touted by U.S. officials as an example of effective oversight, is appointed by and reports directly to the Secretary of Homeland Security, and her ability to initiate investigations is limited by both law and practice. She does receive complaints, but has no independent authority to resolve them or order a remedy. Similarly, the law creating a CPO for the Justice Department provides that, rather than being an independent official, she reports to the Attorney General and her first responsibility is to "advise" and " assist" the AG on privacy and civil liberties matters. (This video shows the current CPO Nancy Libin explaining how her role differs from Europe's independent DPAs.)

- **Agency Inspectors General.** The IGs are not even relevant to a discussion of privacy and data protection. Their authority is limited to instances of waste, fraud, and abuse. They have no jurisdiction over violations of data protection laws or agreements.

- **The Courts.** The U.S. government has all too often been able to block the federal courts from reviewing its actions by citing the "state secrets" privilege and other "national security" imperatives. It has also shielded surveillance practices from judicial review by asserting that plaintiffs lacked "standing" to challenge those practices. As a result of these doctrines, many privacy violations have escaped judicial review and supervision.

Myth #3

U.S. Law Enforcement Authorities Are Less Protective of the Privacy Interests of Foreign Nationals than of U.S. Citizens.

The U.S. paper says that "in the key area" of "email and voice communications in criminal investigations," U.S. protections apply equally to U.S. citizens and foreign nationals. The paper trumpets that narrow set of data, however, precisely because in so many other areas, U.S. protections *are* less protective of Europeans' and other foreigners' privacy.

For example, The Privacy Act applies only to only U.S. citizens and lawful permanent residents. None of the travel data, financial data, and other information on EU citizens collected by the U.S. is regulated by the Privacy Act.

Similarly, the Foreign Intelligence Surveillance Act (FISA) permits the interception of EU citizens' communications where it is not permitted of U.S. citizens. This critical distinction in FISA is the legal basis for the massive communications interception program run by the U.S. Intelligence Community.

But the clearest evidence of the distinction between the U.S. and Europe was provided by the U.S. government itself. In a just-released paper being circulated to EU officials, the U.S. government criticizes the EU's Draft Directive precisely because it does offer more protection than U.S. law. In the

paper, the United States is especially critical of the crucial monitoring role played by Europe's Data Protection officials.

Myth #4

The Patriot Act Gives the U.S. Government Carte Blanche to Access Private Data Stored in the "Cloud" or Elsewhere

The U.S. document claims this is a myth, but the reality is that there are few meaningful restrictions on the U.S. government's authority to monitor communications—and, in particular, communications between foreigners abroad and Americans—in the name of national security.

- **The FAA.** Although much debate has focused on the Patriot Act, the most significant new surveillance authority available to the United States is the FISA Amendments Act of 2008, or the FAA. That act authorizes the government to engage in dragnet and suspicionless monitoring of communications between an individual in the United States and foreigners abroad. The government need not disclose its targets to any court, it need not have any reason to believe its targets are suspected criminals, and it need not even identify to any court the email addresses, phone numbers, or telecommunication switches it intends to monitor. Instead, the FAA allows the government to seek year-long surveillance orders from a secret court if, among other things, a "significant purpose" of its year-long surveillance program is to acquire "foreign intelligence." That term is defined so broadly, however, as to be meaningless. It encompasses, for example, information relating to "foreign affairs." Thus, the FAA exposes virtually *every* communication between an individual in the United States and a non-American abroad to dragnet U.S. surveillance.

- **Section 215.** Section 215 of the Patriot Act authorizes the government to seek an order from a secret court requiring any person or entity to turn over "any tangible things" to the FBI if they are related to an investigation into "clandestine intelligence activities" or "international terrorism." Although a version of this authority existed prior to 9/11, the government has recently relied upon a secret interpretation of Section 215 that would, according to several U.S. senators, shock Americans to learn. As one of those senators explained, there is a "gap between what the public thinks the law says and what the American government secretly thinks the law says."

- **National Security Letters.** Similarly troubling are National Security Letters, which are subpoenas issued by the government to internet service providers, credit card companies, cell phone providers, and others, requiring that they hand over information if it is "relevant" to a counterterrorism or counter-intelligence investigation. Internal government inquiries have uncovered serious abuses of these already lax requirements. We now know, for example, that between 2003 and 2005: the FBI severely under-reported its use of NSLs; the FBI used NSLs to collect information about individuals two or three times removed from the actual subjects of its investigations; FBI supervisors issued hundreds of unlawful requests that relied on false claims of emergency; and, perhaps most alarmingly, 22 percent of the files audited contained unreported legal violations. A later report tells a similar story.

In short, the U.S. government has broad authority to monitor electronic communications and data in the name of national security. Its publicly described authority allows the interception of virtually all

communications between the European Union and the United States, and its still-secret interpretations of certain authorities make it impossible to know how invasive its surveillance powers truly are.

Myth #5

The Advent of "Cloud Computing" Changes Everything

Europeans are rightly concerned about U.S. government access to data that is offered on the Cloud but is physically located on servers in United States. There is no doubt that records held in the United States are subject to U.S. law and susceptible to all the inadequacies in U.S. law described above. Among other things, while the U.S. document remains focused on protections against access for criminal law enforcement purposes—which are themselves inadequate—such data is even more easily accessible for other purposes such as "foreign intelligence."

The advent of the Cloud doesn't change the law, but it does intensify the consequences of many of the gaps in U.S. privacy protections, and increase the risk for Europeans as more and more data crosses the Atlantic.

Jointly Prepared By The American Civil Liberties Union (ACLU) and Friends of Privacy USA.