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 in the EU and US. The document is an attempt to reassure Europeans about US privacy laws, but as we explain below, Europeans are right to be worried.

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,“ where they exist, 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.
- Judicial oversight has often been weak on privacy. Judicial review has often been successfully avoided through use of the “state secrets” privilege and assertions that plaintiffs lack “standing” to challenge abusive practices.

U.S. protections are even less protective of Europeans’ privacy in many areas

- The Privacy Act applies only to only U.S. citizens and lawful permanent residents. Data on EU citizens collected by the U.S. is not regulated by the Privacy Act.
- The Foreign Intelligence Surveillance Act (FISA) permits the interception of EU citizens’ communications where it is not permitted of U.S. citizens.

Protection for electronic communications privacy in the U.S. is marked by gaping holes:

- 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.
- An email message in the U.S. is subject to multiple different legal standards during its lifecycle based on irrational criteria such as its age and whether it is “stored” or “in transit.”
- Overall, U.S. electronic privacy laws are a confusing, inconsistent patchwork.
- A “third party doctrine” in U.S. privacy jurisprudence provides that communications that have been “voluntarily disclosed” to a third party—such as a cloud storage provider—no longer receive constitutional protection.
- Metadata (including the sender and recipient of a communication) receives much less privacy protection than the content of messages even though it can be equally or even more sensitive.
- The U.S. government argues that location tracking data should not receive constitutional privacy protection, and many police agencies are now accessing such data on very low legal standards.

The U.S. government has sweeping authority to spy on Americans and Europeans alike in the name of national security:

- The FISA Amendments Act (FAA) authorizes the government to engage in dragnet and suspicionless monitoring of communications between an individual inside and one outside the U.S. with no meaningful oversight.
- Section 215 of the Patriot Act authorizes the government to access “any tangible things” related to an “intelligence” or “terrorism” investigation. Several senators have revealed that the government is relying upon a secret interpretation of Section 215 that would “shock” Americans to learn.
- Using National Security Letter” subpoenas the government can require any service provider to hand over information it says is “relevant” to a counterterrorism or counter-intelligence investigation. Internal government inquiries have uncovered numerous serious abuses of these already lax requirements.

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