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

The U.S. 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 suspicion less 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.

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