What Rules Regulate Government Access to Data Held by US Cloud Service Providers

CSA Legal Information Center
Sponsored Research
INTRODUCTION

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. CSA sets the pace as the industry leader in research, best practices and certification for the trusted cloud ecosystem.

The CSA Legal Information Center is an expert-led community resource for global legal issues impacting cloud computing. Our mission is to provide unbiased information about the applicability of existing laws and also identify laws that are being impacted by technology trends and may require modification. The CSA Legal Information Center includes whitepapers, webinars, an advice column and in-person events.

The CSA Legal Information Center is located at: https://cloudsecurityalliance.org/research/clic/

The CSA Legal Information Center is supported by our founding sponsor and corporate member Box. Founded in 2005, Box provides a secure content sharing platform that both users and IT love and adopt. Content on Box can be shared internally and externally, accessed through iPad, iPhone, Android, TouchPad and PlayBook applications, and extended to partner applications such as Google Apps, NetSuite and Salesforce. Headquartered in Palo Alto, CA, Box is a privately held company and is backed by venture capital firms Andreessen Horowitz, Draper Fisher Jurvetson, Emergence Capital Partners, Meritech Capital Partners, Scale Venture Partners, and U.S. Venture Partners. To learn more about Box, please visit www.box.com.

All trademarks, copyrights and logos are the property of their respective owners.

Author Acknowledgment
© 2013 Francoise Gilbert - IT Law Group – All Rights Reserved

Francoise Gilbert, JD, CIPP/US, focuses her legal practice on information privacy and security, cloud computing, and data governance. She was listed as one of the country’s top legal advisors on privacy matters in a recent industry survey and, for several years, has been recognized by Chambers, Best Lawyers, as leading lawyer in the field of information privacy and security. For the past two years, Ethisphere has identified her as “an attorney who matters” in the field of information privacy and security.

Gilbert is the author and editor of the two-volume treatise Global Privacy & Security Law (3,000 pages; Aspen Publishers, Wolters Kluwer Law and Business) (www.globalprivacybook.com), which analyzes the data protection laws of 65 countries on all continents.

She is the managing attorney of the IT Law Group (www.itlawgroup.com) and serves as the general counsel of the Cloud Security Alliance. She also keeps a blog on domestic and international data privacy and security issues (www.francoisegilbert.com). (650) 804-1235  fgilbert@itlawgroup.com
What Rules Regulate Government Access to Data Held by US Cloud Service Providers

Francoise Gilbert JD, CIPP/US

Lately, purchasers of cloud services have expressed concern about the idea that the U.S. government might be able to have access to data stored outside the United States by a provider of cloud services that is a subsidiary of a U.S. company. They point to the USA PATRIOT Act as the magic wand that allows the U.S. government unrestricted access to any data, anywhere, any time. In fact, the actual impact of the USA PATRIOT Act in this context is negligible.

The Patriot Act itself is actually a compilation of amendments to pre-existing laws that have been in existence since the 1970’s and 1980’s. To the extent the U.S. government can access data, it is not through the USA PATRIOT Act but through these laws and decades-old judicial decisions providing for extraterritorial power in limited circumstances.

What is the USA PATRIOT Act?

The USA PATRIOT Act is the short name for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (“Patriot Act”) a comprehensive document that was signed into law in 2001 after the September 11 attacks. The document is primarily a combination of amendments to existing laws, in order to make it easier for the U.S. government, in the context of criminal investigations, to conduct surveillance and access data with the purpose of preventing, detecting, and investigating terrorist acts.

The US laws that govern access to data and communications in the possession or custody of companies or entities located in the United States have been in existence since the late 1960s. They have been periodically amended to take into account the new types or forms of crimes or other offenses that they are intended to address, or the development of new technologies or techniques, such as the Internet, RFID or global positioning systems. The 2001 Patriot Act is only one of the many amendments to these laws.

Rules Regarding Government Access to Data

In the United States, numerous laws govern the circumstances and manner in which a state or federal investigator may have access to data, communications, information, documents, or premises. At the federal level, the basic rule written in the 4th Amendment to the U.S. Constitution grants Americans the right to be secure from unreasonable searches and seizures.

In addition, several federal laws, such as the Wiretap Act, Stored Communications Act, Pen Register Act, Foreign Intelligence Surveillance Act, Communications Assistance to Law Enforcement Act, or the Economic Espionage Act define the specific rules for access to data or communications.

A similar regime exists under State law. Most states have general surveillance laws. They may have specific laws, as well, to govern the use of certain technologies that can be used, among other things, for surveillance, such as RFID or GPS.
These laws depend on the nature of the data. For example, the Wiretap Act pertains to data in transit, whereas the Stored Communications Act pertains to data in storage. There are different provisions for access to content as opposed to access to non-content (i.e., identity of the sender, the recipient, time of the call or communication). The law may distinguish whether the person being investigated is a U.S. citizen or resident, or, instead an “agent of a foreign power” as is the case under the Foreign Intelligence Surveillance Act.

**How does Government Obtain Access to Data, Communications or Premises?**

The laws described above define the specific rules and requirements that must be met for a federal or state law enforcement agent to have access to specific data, premises, or equipment where the data are located. In most cases, the government representative is required to obtain a subpoena, a court order, or a warrant. In rare cases, it may be possible to have access to data without a subpoena, court order, or warrant; these circumstances are specifically identified in the applicable law, and are generally associated with extra-ordinary situations. The Stored Communication is an example of one of these many laws.

**Stored Communications Act**

Enacted in 1986, and codified as 18 USC §§ 2701-2711, the [Stored Communications Act](#) governs access to wire, oral, and electronic communications in storage (as opposed to communications in transit). The law contains general prohibitions against access to these data or communications, rules that allow disclosure of these data or communications by service providers (e.g., Verizon, AT&T). It also contains a series of exceptions for allowing the government to access data stored by communications and computing service providers. These rules are very complex and very detailed.

For example, under 18 USC §2703(a), a governmental entity may obtain access to content that has been held in storage for less than 180 days by an electronic communications service, after having obtained a warrant from a judge. The standard for obtaining a warrant is very high. In order to obtain the warrant, the officer must show that “probable cause” exists, based on the officer’s personal observation or hearsay information, to show that evidence of a crime would be found in the requested search.

There are different rules for obtaining access to the same information that would have been held by the same service provider for more than 180 days. In this case, a subpoena or court order would suffice. The requirements for a subpoena or a court order are less stringent. Thus, the same piece of information enjoys a lesser protection if it has been stored for a longer period of time.

However, in this later case, if the government opted to use a subpoena or a court order, then it would have to give prior notice to the subscriber or customer of that service. If the government wants to avoid having to provide the notification, then a warrant is required.

In addition to the dichotomy described above – i.e. more than 180 days v. less than 180 days in storage, there are also different rules that distinguish according to the nature of the information sought. While the rules above would apply for access to “content” (i.e., what was said, what was the message), there are different rules for access to “non-content” (i.e., when the message was sent, from whom, to whom).

Of course, there are different rules to regulated access to information that is “in transit”, as opposed to “stored”. The rules are found in the Wiretap Act.
Oversight: Annual Reports

The issuance of search warrants or orders allowing access to, or interception of data or communications is highly controlled. It is not enough that each law enforcement agent must provide substantial information to show why the search is needed, and identify the grounds to believe that the content is relevant or material. There are also reporting requirements.

For example, any judge who has issued an order for an interception (under the Wiretap Act), or has denied the request, must report, annually, to the Administrative Office of the United States Courts information about its approval or denial of requests for warrants or orders. The report must indicate the fact that the order was applied for, and the kind of order or extension application; the fact that the order or extension was granted, and the period of interception authorized; and the offense specified in the order, and the identity of the officer making the application.

 Concurrently, the U.S. Attorney General who has made the request for access must also file a report to the Administrative Office of the United States Courts. This report must also contain detailed information about each investigation, including, for example, the number of persons whose communications were intercepted, number of arrests resulting from the interception or number of convictions.

Based on the judge reports and the U.S. Attorney General reports, a compilation is prepared annually, and a summary report is provided to Congress. These reports are publicly available for anyone to review, and are posted on the Internet. For example, the Wiretap Report for 2011 can be found at http://www.uscourts.gov/Statistics/WiretapReports/WiretapReport2011.aspx.

Thus, these investigations are not started lightly. The perspective of having to prepare so many reports and statements would already be a deterrent. In addition, each such investigation is very costly. For example, according to the report on wiretaps installed in 2011, the average cost of an “interception” ranges from $4,000 to close to $600,000 (New York Organized Crime Task Force), with a median around $50,000 per interception.

Foreign Intelligence Surveillance Act and Amendment

The Foreign Intelligence Surveillance Act (FISA), enacted in 1978, prescribes procedures for physical searches and electronic surveillance of activities of foreign entities and individuals where a significant purpose of the search or surveillance (and the collection of information) is to obtain “foreign intelligence information.”

The term “foreign intelligence information” is defined to include information that relates to actual or potential attacks or grave hostile acts of a foreign power or an agent of a foreign power, sabotage, international terrorism, weapons of mass destruction, clandestine intelligence activity by or on behalf of a foreign power, or similar issues.

As for the other laws described in this article, the Patriot Act only amended FISA, and since the 2001 amendments, FISA has been further amended by other laws. The 2001 amendments resulting from the Patriot Act enlarged the scope of the existing law to apply when “a significant purpose” of the search or surveillance is the collection of foreign intelligence, whereas the scope of FISA was initially limited to searches where “the primary purpose” was the collection of foreign intelligence.

FISA allows the President of the United States, through the U.S. Attorney General, to authorize electronic surveillances in order to acquire foreign intelligence. To conduct such electronic surveillance, the government agent must seek an order from the FISA Court (or “FISC”), a special court that oversees surveillance activities under FISA. The application to
conduct the surveillance must set out the facts to support a finding by the FISC judge reviewing the application that there is probable cause to believe that the proposed target is a foreign power. The application must also describe the premises or property that is the proposed subject of the search or surveillance.

The U.S. Attorney General’s representative making the request for the surveillance must certify, in writing and under oath, that the electronic surveillance is solely directed at the acquisition of communications between or among foreign powers, and that the proposed procedures meet the “minimization procedures” requirement. The U.S. Attorney General’s representative must immediately transmit, under seal, a copy of this certification procedure to the FISC.

FISA was amended in 2008 through the FISA Amendment Act (FAA) to permit the U.S. Attorney General and the Director of National intelligence to jointly authorize the targeting of non-U.S. persons reasonably believed to be located outside the United States, in order to acquire foreign intelligence information. The FAA was to expire at the end of December 2012. It has been extended though the FISA Amendment Acts Reauthorization Act of 2012, H.R. 5949, which was signed into law by President Obama in early January 2013. Targeting under the FAA requires a determination by the U.S. Attorney General and the Director of National Intelligence that exigent circumstances exist because intelligence important to the national security of the United States may be lost.

There are numerous limits to the way in which the targeting may be conducted. Minimization procedures must be used to protect American residents. These minimization procedures are intended to ensure that the acquisition of information is limited to targeting persons reasonably believed to be located outside the United States. In addition, the targeting must be conducted in a manner consistent with the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable searches and seizures.

The U.S. government does not have jurisdiction over non-U.S. entities located outside the U.S. territory. The FAA does not grant U.S. governmental entities the right to access servers held outside the United States. It only defines the rules that federal agents must follow to target communications made by non-U.S. persons believed to be located abroad, in order to acquire foreign intelligence information.

Access to Data Held in a Foreign Country

What happens when an investigation would require access to data held in a foreign country? Generally, a U.S. prosecutor or investigator will not be permitted to conduct an investigation, or interview witnesses abroad. In most cases, the help of the local government will be necessary. To this end, over the years, the different nations have entered in a variety of bilateral or multilateral treaties that define how they will cooperate in certain matters.

For example, the United States is a party to several Mutual Legal Assistance Treaties (MLAT) for the purpose of gathering and exchanging information in an effort to enforce public laws or criminal laws. There are numerous MLATs related to police and law enforcement cooperation. There are also MLATs with respect to tax evasion.

In addition to the MLAT, the United States is also a member of the Council of Europe Convention on Cybercrime, which it ratified in 2007. The Convention governs electronic surveillance, sharing of evidence, and computer crime. It allows governments to request and provide mutual assistance in the investigation and prosecution of a number of crimes, such as hacking, unauthorized access to computer systems, child pornography, or copyright infringements.

Thus, in practice, federal prosecutors who need access to data will frequently take advantage of the methods provided in the applicable MLATs, treaties, or conventions, since they are not allowed to communicate directly with foreign authorities, or witnesses, or to undertake travel to a foreign country.
In some cases, law enforcement may attempt to obtain access to information held abroad by making the request from the U.S. affiliate of a company located abroad who may have custody or control over the documents or information at stake. United States courts have held that a company with a presence in the United States is obligated to respond to a valid demand by the U.S. government for information (made under one of the applicable U.S. laws) so long as the company retains custody or control over the data. In this case, of course, the key question is whether and the extent to which the U.S. company does have the required level of “custody or control” to be forced to respond to the government request.

The seminal case is *In re Grand Jury Proceedings Bank of Nova Scotia* (740 F.2d 817, 11th Cir., 1984) where the court required the U.S. branch of a bank to produce documents that were held in the Cayman Islands, and were needed in criminal proceedings in the United States. This principle of extraterritorial reach has been followed elsewhere, for example in Australia. In the case *Bank of Valletta PLC v. National Crime Authority* [1999] FCA 1099, the Australian Branch of a Maltese bank was required to produce documents held in Malta for use in an Australian criminal proceeding.

**Similar Laws Abroad**

While the rules that pertain to government access to data and communications in the United States have received a lot of attention from the media, the United States is not alone in using sophisticated investigations methods to obtain access to information needed for criminal investigations, the fight against illegal drug sales or terrorism. Many other countries also have laws authorizing government investigations for national security and other purposes. These laws are necessary for providing the proper structure and rules for government investigations.

Described below are several countries that limit or regulate access by their governments to data stored on their national territory. Some of these countries give their law enforcement or intelligence services extensive powers that are substantially similar, and at times greater, than those of their U.S. counterparts.

**Canada**

In Canada, Part II of the *Security Intelligence Service Act*, allows designated judges from the Federal Court to issue warrants authorizing the interception of communications and obtaining any “information, record, document or thing”. The warrant may authorize entering any place, and “searching, removing and examining any thing, or installing, maintaining or removing any thing” in order to conduct the investigation.

The *National Defense Act* gives the Minister of National Defense powers that are similar to those granted by the U.S. Foreign Intelligence Surveillance Act, such as the power to authorize the Communications Security Establishment to intercept communications for obtaining foreign intelligence. The Minister may only issue an authorization if satisfied that: (i) the interception will be directed at foreign entities located outside Canada; (ii) the information to be obtained could not reasonably be obtained by other means; (iii) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and (iv) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defense or security.

Further, several provisions of *PIPEDA*, the Canadian federal law on protection of personal data, allow national security policies to take precedence over privacy rights. For example, PIPEDA allows an organization to collect, use, or disclose an individuals’ personal data *without the knowledge or consent of the individual* in connection with an investigation or if the
information relates to national security, the defense of Canada, international affairs, or an investigation, or to comply with a warrant or subpoena.

PIPEDA also contains an exception to individual’s right of access to information about them held by organizations, when the organization has disclosed personal information to governmental agencies as described above. If an individual requests that the organization inform him about disclosure of information made to the intelligence services, the organization must notify in writing and without delay the government agency to whom the disclosure was initially made and cannot respond to the individual until it receives the government agency’s response.

India

In India, the Information Technology Act of 2000 as amended, gives extensive powers of investigation to the Indian government for combatting terrorism. For example, the Information Technology Act allows the monitoring and collection of "traffic data" (data telecommunications traffic) for the protection of cyber security. In addition, it gives the police the power to enter any public place and search and arrest without a warrant any person suspected of having committed or of committing or about to commit any act prohibited by the law. It also allows the Indian government to intercept, monitor, or decrypt communications made from mobile phones, computers and other devices or to monitor and collect traffic data to protect cyber security and public order, and prevent the commission of a crime.

United Kingdom

The United Kingdom’s Regulation of Investigatory Powers Act (2000) (RIPA) defines the powers of public agencies to carry out surveillance and investigations, to intercept and use communications, and to do other related investigations, to follow people, and use human intelligence sources.

The law allows public agencies to take part in such activities for national security and for detecting crime, preventing disorder, public safety, and public health. RIPA allows the interception of communications, uses of communications data, following people, and use of covert human intelligence sources. It may require individuals or companies to supply decrypted information that has been previously encrypted. Failure to disclose this information may be subject to up to 2 years in jail.

Government Investigations v. Privacy Protection

It is certain that there is an inherent opposition between governments’ requests for access in the context of criminal investigations or the fight against drugs or terrorism, and the basic rights of individuals to privacy in their home or their papers. The laws that regulate government access to data and communications have attempted to address this opposition between the individual interest of a person, and the community’s interest in fighting crime and terrorism, and have provided numerous safeguards, requirements and controls to limit abuses, but they have also ultimately recognized that national security trumps personal privacy.

In the European Union, for example, the basic document that defines the principles of privacy protection for all individuals recognizes that there are cases where privacy rights have to defer to other rights. It has carved out from the blanket protection of individuals with respect to the processing of personal data, the ability for governments to have access to, or use of, personal information in connection with investigations that pertain to national security, defense and related areas. Specifically, Article 13 of Directive 95/46/EC provides that “member states may adopt legislative measures to restrict the scope of the obligations of data controllers and the rights of data subjects, when necessary to safeguard national security, defense, public security, or the prevention, investigation, detection and prosecution of criminal
offenses”. These exceptions have been implemented in the national data protection laws of the Member States. Other EU or national laws define the rules that apply to the collection and sharing of personal data in connection with government investigations for national security similar purposes.

A similar carve-out is provided in the E.U.-U.S. Safe Harbor Principles. The comments that precede the definitions of the Safe Harbor Principles in the seminal Safe Harbor documents provide: “adherence to these principles may be limited to the extent necessary to meet national security, public interest, or the requirements of law enforcement”.

Expect Intelligence Services to Have Significant Powers in Most Countries

Intelligence services, in their fight against terrorism, espionage, money laundering, child pornography, drug trafficking, and the like, have significant investigatory powers in most countries. The concerns and the need for information on one end, and the need for some secrecy on the other, are generally the same in all countries. These services frequently cooperate with each other across borders.

If a cloud service provider receives a request from the secret services, intelligence services, or other law enforcement authority of the country in which it is located, in the manner prescribed by applicable law, it will not have much choice other than providing access to the company’s data or equipment, unless the request is defective and does not follow the applicable rules. In this case, the service provider may opt to fight the request and argue, for example, that it is illegal, does not conform to the legal requirements or is too broad. This is true in any country, and it applies just as much when the government authority is that of the United States, Canada, India, or any other country.

The problem of the prerogatives and powers of the United States Intelligence services may actually be less serious than in other countries because U.S. laws contain strict and detailed rules, provide a lot of transparency and require law enforcement to make numerous disclosures of their activities. There are many control measures (e.g., annual reports) or detailed procedures (e.g., warrant or a court order), and procedural rules. In other countries, access to equipment, servers or storage systems by law enforcement, or intelligence or secret services may be much less regulated. The lack of transparency may cause the public to be unaware of the extent of the government surveillance.

Conclusion

Users of cloud services should remain aware that wherever their data are stored or hosted by a third party, it may be possible to a government – or several governments concurrently - to obtain access to these data, especially when there are overarching reasons for such access, such as national security or the prosecution or prevention of serious crimes. This has always been the case, even when data were held in server farms across the street from one’s corporate headquarters. Cloud changes the dynamic because today, these same data may be held in several servers located anywhere in the world, and consequently may be subject to requests for access by many more entities, in many more countries, and under many more laws.

Providers of cloud services have a dual responsibility. They must understand and abide by the rules that apply to their business, and they have an obligation to their customers to respond to government or other request for access to data in their custody in a responsible manner and in accordance with their Terms of Service. When a CSP receives a government request for access, it has the responsibility to evaluate this request for access and determine whether it is conform to applicable law. If it is, and if this is legally and physically possible to do so, the CSP should take the necessary steps to inform the customer in a manner that is consistent with the provisions of its Terms of Service.
On the other hand, consumers of cloud services should, as part of their due diligence before engaging a CSP, evaluate the CSP’s awareness of these highly complex issues and understand the CSP’s Terms of Service, so that they can be assured that the CSP’s practices or standards are consistent with the consumer’s expectation. Most CSP’s Terms of Service warn customers that the CSP may be required to provide information in response to facially valid request for access from a government entity.

// Palo Alto, California, February 2013.