Data Privacy:
Where Should I House My Data?

Data Privacy: Where Should I House My Data?

As enterprise file sharing and collaboration tools become more widely used, it becomes increasingly important to understand how to protect information and preserve data privacy.

In the age of Edward Snowden and the NSA, there are increasing concerns about data privacy and especially about where to house data. The prevalence of cloud computing and cloud-based storage and collaboration services is only exacerbating these concerns. Many organizations are confused about regulations that protect data in different countries and jurisdictions, and don't know what steps to take to ensure their cloud collaboration vendor can provide adequate safeguards.

The leak of NSA secrets is only the most recent case of increased exposure of government data collection for national security, law enforcement, foreign relations, and economic purposes. Over the last few years, major technology firms have begun publicly releasing information about mounting government requests for customer data. Alarmed by the depth and breadth of these requests, Facebook, Google, Twitter, Microsoft, and Verizon, among others, are using transparency and publicity to highlight government inquiries into the data they hold. Echoing Snowden, many of these firms, competitors in the market, have come together to call for reform of the surveillance practices of nations[1].

Together, these instances highlight how government data collection efforts put companies in a difficult spot: organizations might have legal or ethical obligations to protect data in one jurisdiction while also having legal requirements to turn that information over in another. The move to cloud-based data storage and processing has only added to jurisdictional concerns.

While pushback and reform efforts are evolving, the reality remains that companies must operate within the law. Deciding where to house your data and how to move it is an exercise in both understanding the relevant legal regimes and the appropriate application of risk analysis in the decision-making process. An examination of those elements in regard to cloud-based data storage and processing follows.

The importance of geography for cloud systems

We now live in a world where location is extremely relevant and the legal system is thoroughly entrenched in governing data that rest within its borders.

However, examining the physical location of the data is only the first step. As outlined in the chart below, a host of other considerations must be made. While common sense would suggest local government access in the location of the corporate headquarters, there are several less obvious routes that governments might take. Even if a company is headquartered in one jurisdiction and houses data there, their presence in another jurisdiction might give enough cause for that jurisdiction to demand access to the data within the company's custody or control.

Information flow through the Internet is not geographically bound and often moves over the least congested path. This path may involve transmission through many countries. Any of these countries could claim jurisdiction over data as it passes

Even data that doesn't reside within a country's borders and doesn't transit through that country might still be accessible by that country's law enforcement and intelligence services.

through Internet service providers in those countries. Traffic flow can also be hijacked, and recent evidence has shown some major rerouting of strictly North American traffic through international locations[2]. It's still unknown whether this is the result of government actors or cyber-criminals. The conclusion though is the same: you can't know where your data flows.

Even data that doesn't reside within a country's borders and doesn't transit through that country might still be accessible by that country's law enforcement and intelligence services. Mutual legal assistance treaties (MLAT) are mechanisms by which one country's agents may request the assistance of another country in obtaining information over which they don't have direct physical or legal access. There are several of these bilateral and multilateral treaties. The general sense is that so long as the investigation is one that would be allowed under the laws of the assisting country, law enforcement will assist.

Geographic considerations in data warehousing

Physical Location	The laws of the political entity that govern the geographical boundary where the information is housed will give them jurisdiction over that information.
Corporate Headquarters	While the server may be remote and in a distinct political boundary different from the company or organization that manages it, the laws of the land where the company or organization is headquartered will govern them and will likely require access to information within their "custody."
Business Interests	Even if the organization is headquartered in one location and the data rest in another, if the organization has business interests in additional locales, those governments may be able to gain access by virtue of the organization's connection to those jurisdictions.
MLAT	Many countries are signatories to mutual legal assistance treaties that allow government agencies to access data in other jurisdictions so long as the other jurisdiction recognizes the legal authority under which the data is being sought.
Transmissions	If the organization is in one country and the data is in another, chances are it will transit through many other countries. The Snowden disclosures showed how the NSA relied on the fact that much of the world's information traffic flows through the United States[3].
Data Subjects	Some laws apply extraterritorially to data about residents in their jurisdiction. Many individual U.S. state data breach notification statutes do not require a business to operate in the state rather only that a breach involve data about residents of that state to be covered.

[1] http://arstechnica.com/tech-policy/2013/12/microsoft-google-apple-call-for-end-to-nsas-bulk-data-collection/

[2] http://arstechnica.com/security/2013/11/repeated-attacks-hijack-huge-chunks-of-internet-traffic-researchers-warn/

[3] http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

One final consideration is the idea that the actual content of the data might render it subject to the jurisdiction of some government body, no matter the location. For instance, under Massachusetts state law, personal information about residents of the Commonwealth is subject to the data breach notification law regardless of holder of that information's ties to the state or the actual location of the data. Clearly, enforcement becomes an issue when laws apply extraterritorially.

Why care where your data is housed

Many organizations aren't concerned about law enforcement or intelligence service access to their data. They believe that if they aren't breaking any laws, then what is the concern? There are several problems with the "nothing to hide" argument. First, indiscriminate information gathering by government agents can stifle lawful activities, causing a chilling effect on people who fear a negative reaction to their legal yet novel or mores-challenging activities. Second, with sufficient ambiguity and breadth in the law, digging deep enough might allow a government to present a case of illegal activity absent criminal intent. Thirdly, some countries might utilize their intelligence gathering to provide an economic advantage to industry in their country. Information is one of your most valuable assets and shouldn't be shared, even with government, without safeguards.

Even if your organization isn't particularly sensitive to data access by law enforcement, your customers/consumers might be. Many organizations have found their international business customers asking more questions about where their data are going. While this has been true for a while with European organizations as a result of the Data Protection Directive's restrictions on cross-border data flow, even organizations outside the European Union (E.U.) and United States are starting to ask questions. They might be concerned about their data, their obligations under the laws of their country, or even their customers' risks and perceptions about treatment of sensitive information.

National breakdown

A full breakdown of the data protection laws, exceptions for law enforcement or national security, and practical adherence to those laws for every nation on earth would require volumes. What follows is a brief, selective overview. Many countries have laws that govern the general disclosure of information with enumerated exceptions for law enforcement. In addition, they have specific legislation that governs the access to data by government authorities and the burdens they must show to gain access, from just a desire for the information to a warrant signed by an independent judiciary based on probable cause of a criminal act. Many times the requirements may vary depending upon the nature of the information: live communications being most sensitive and requiring the highest burden and business information about customers being the lowest.

Europe has the highest levels of enforcement activity in the world with Germany, the United Kingdom, the Netherlands, and Spain leading the way.

The United States represents a special case. Prior to the Snowden revelations, the U.S. was seen as a benevolent overseer, guiding the global Internet for the benefit of humanity. But that vision has been shattered. A majority of the world's telecommunications traffic runs through switches and servers located in the United States or controlled by U.S. interests. This explains why U.S. companies receive special treatment when dealing with European Union citizen data. Most countries must meet certain minimal legal safeguards to be deemed "adequate" under the Data Protection Directive (DPD), the measure regulating the cross-border transfer and processing of E.U. citizen data. But even though the United States is not deemed adequate, organizations may certify under the U.S. Department of Commerce Safe Harbor program.

The requirement for adequacy in data protection laws is just one of the rigid standards under the DPD. Enforcement of these standards is handled by Data Protection Authorities in the nations that comprise the E.U. Europe has the highest levels of enforcement activity in the world with Germany, the United Kingdom, the Netherlands, and Spain leading the way. Most countries in Asia lack strong privacy-related laws and thus have limited enforcement activity. This might be changing as a result of the efforts by the Asia Pacific Economic Cooperation (APEC) group. APEC, which includes non-Asian nations such as the U.S., Canada, Australia, and New Zealand, has instituted a set of non-binding privacy principles. Many of these nations have or are considering instituting legal reforms to implement the privacy principles. Canada and New Zealand have both been deemed "adequate" for the data protection purposes, though enforcement is still significantly lower than in E.U. countries. Africa and South America have practically non-existent legal guidance in this area.

Knowing where your data is, knowing where it went to get there, and understanding the basic security technology in play are important to protecting the privacy of your customers. Here are some recommendations to help you do so.

Region (Rank)[4] North America	Strengths	Weaknesses	Special Notes
United States ★[5] (7)	The Electronic Privacy Communications Act (ECPA) provides protection for data stored in "remote computing services" including legal restrictions against voluntary disclosures to law enforcement for data stored in the cloud. The U.S. is a strong rule-of-law jurisdiction.	Lack of clarity of extrajudicial processes for collection of data. National Security Letters can get customer data (but not content) and require confidentiality by the recipient.	The U.S. is situated in a unique and unequal power position relative to other nations in terms of raw access to data.
Mexico	Federal law requires judicial warrant for interception of electronic communications (though evidence suggest widespread disregard for the law).	2012 legislation allows collection of geolocation data without a warrant.	Reported use of FinFisher spying software by Mexican authorities.
Canada	Prior judicial authorization required for electronic surveillance.	Foreign intelligence exception to allow electronic surveillance without a warrant. Peace officer exception in urgent situations to prevent unlawful acts. Law applies to anything under custody and control of Canadian entity. May voluntary give up information without warrant unless contains personal information and is not requested pursuant to a lawful authority under Canadian privacy laws.	

[4] Rank is based on "An Analysis of Service Provider Transparency Reports on Government Requests for Data" (Aug 27, 2013) by Christopher Wolf. Taiwan for example, at number 1, had the higher number of governmental requests on major internet services per capita for it's respective population.

[5] The ★ symbol in the chart represents countries that are members of the UK-USA Agreement for sharing of signals intelligence. It's colloquially known as five eyes.

Region (Rank)[4] Europe	Strengths	Weaknesses	Special Notes
United Kingdom (2)	Data Protection Act 1998 provides protection of privacy.	Limited judicial oversight for information requests. Extraterritoriality codified in Anti-terrorism, Crime and Security Act of 2001. Evidence of intelligence services hacking of service providers outside of the U.K.	Telecommunication service providers must store data for 6 to 24 months.
Germany (6)	Limited to within Germany's physical borders.	Anti-Terrorism Law provides German security architecture direct access to personal data.	Under court order, authorities may release a "Federal Trojan" to infiltrate computer systems and obtain information without notifying the system owner.
Switzerland	Not a member of the E.U. but data protection laws deemed adequate. Violations of the principles of the Federal Data Protection Act not justifiable based on public or private interest. Subjects must be informed of interception of communications.	Internet service providers required to retain data for law enforcement purposes.	Swiss cloud providers trying to leverage privacy friendly laws and attract business.
France (4)	Privacy protected by implementation of Data Protection Directive.	Judicial police officer may access data, including abroad. Express permission for access to foreign servers accessible through a local computer.	Anti-terrorism law includes provisions for protecting economic and scientific concerns.
Belgium (8)	Law on Protection of Personal Data of 1992 is the Belgium implementation of the DPD.	Investigative judge may require assistance of experts to decrypt communications between parties. Refusal to assist can result in criminal sanctions	Yahoo!, originally fined for failure to turn over personal data in cybercrime case (arguing that authorities should have gone to U.S. government for assistance in accordance with treaties in place), vindicated when Belgium court overturns ruling stating no basis in law to require them to turn over data.
Portugal (9)	Law enforcement required to act in conformance with Portugal's implementation of the DPD when assisting authorities in other countries.		

Region (Rank)[4] Europe (cont'd)	Strengths	Weaknesses	Special Notes
Spain	Limited access by law enforcement to cloud data, no provision in the law.[6]		Google just recently fined upwards of $1 million for violation of data protection act.
Denmark	Limited to within Germany's physical borders.	Anti-Terrorism Law provides German security architecture direct access to personal data.	Under court order, authorities may release a "Federal Trojan" to infiltrate computer systems and obtain information without notifying the system owner.
Sweden	Not a member of the E.U. but data protection laws deemed adequate. Violations of the principles of the Federal Data Protection Act not justifiable based on public or private interest. Subjects must be informed of interception of communications.	Internet service providers required to retain data for law enforcement purposes.	Swiss cloud providers trying to leverage privacy friendly laws and attract business.

Region (Rank)[4] Africa & S. America	Strengths	Weaknesses	Special Notes
Africa			
South America	Limited access by law enforcement to cloud data, no provision in the law.		In Brazil, extreme protectionist legislation would mandate in country data centers for all information on Brazilians.

[6] *http://cloudscorecard.bsa.org/2013/assets/PDFs/country_reports/Country_Report_Spain.pdf*

Region (Rank)[4] Asia–Pacific	Strengths	Weaknesses	Special Notes
Japan	Warrant issued by a judge required for access. No special rules for anti-terrorism or national security investigations. No voluntary disclosure allowed without a warrant. Limited to data within Japan's physical borders.		There are no special rules regarding government access to cloud data during the course of national security or terrorism investigations.
Taiwan (1)			
Hong Kong (3)		Very broad laws giving authorities virtually unlimited access to stored data.	
Singapore (10)	Warrant required to access cloud based data.[7]		
Australia (5)	Privacy Act of 1988 provides protection of privacy.	Voluntary disclosures allowed if organization reasonably believes necessary to assist law enforcement. Computer access warrants issued by government minister requires recipient confidentiality. Requests extend to outside Australia but controlled by Australian companies.	Intelligence and defense agencies mostly exempt from the Privacy Act.
New Zealand			

Recommendations

- **Perform a full risk analysis.** Risk is a product of probability of occurrence of an event and the impact of that event on the organization. Any organization should undertake a comprehensive risk analysis that explores the entire range of conceivable threats and their impacts. Where previously government activity was deemed a baseline and generally left out of the risk analysis, it's now an important consideration. The legal environment of the vendor also must be considered and weighed against other threats and factors.
- **Validate assumptions.** Prior to 2013, most organizations realized the threat from hackers and cyber-criminals and actively worked to secure their networks against them. What was revealed in 2013 is that governments (both foreign and domestic) might also be working against the security of the organization and that insider threats (à la Edward Snowden) might be more damaging than outside threats. It's important for organizations to know the laws, understand how the governments act on those laws, and not be misled by popular accounts or rumors. You can't perform a full risk analysis without accurate information about what the threats are.

[7] *http://cloudscorecard.bsa.org/2013/assets/PDFs/country_reports/Country_Report_Brazil.pdf*

- **Encrypt your data in transit.** You might not be aware of which jurisdictions your data is being transmitted through. There have been cases of entire streams of Internet traffic being rerouted through other countries, possibly for government surveillance or fraudulent purposes. Encrypting data in transit works and it is a must. This includes using encryption techniques such as forward secrecy and ephemeral session keys that preserve the security of the information even if it is captured and stored for future analysis.
- **Encrypt your data at rest.** When your data are being stored, they should be secured, preferably with encryption keys you don't share even with your vendor or service provider. While the service provider might have policies that protect you, they can't protect you against the Edward Snowdens in their organization nor can they protect you against the laws they are obligated to follow.
- **Be transparent about law enforcement access.** Nearly every set of privacy principles has some form of transparency principle (Fair Information Practice Principles, Data Protection Directive, Privacy by Design, Generally Accepted Privacy Principles). Some laws require providers not to notify their customers in certain cases. Beyond this, you should seek to be as transparent as possible. This not only puts your customers on notice for their own benefit but might help rein in law enforcement placing unnecessary burdens and requests on your business.
- **Expect transparency from your provider.** You can't be transparent to your own customers if your providers aren't transparent with you about their legal obligations. Many providers try to whitewash government access to data with contractual language of the form "we will respond to all lawful government access requests." Does this mean when their subsidiary in China gets a requests for information related to your finances, they will comply? Demand clarity in contractual language.

Choosing where to locate your data for storage or processing and when and where you can move your data shouldn't be done in a vacuum, nor should they be undertaken lightly. Cloud computing and remote storage can relieve many organizations of the technological burdens of understanding the mechanics under the cloud, but this doesn't relieve them of the burden of understanding the laws of the nations in which that cloud operates.