ITIF
The Information Technology & Innovation Foundation

The False Promise of Data Nationalism

BY DANIEL CASTRO | DECEMBER 2013

ITIF recommends the United States engage its trade partners in developing a "Geneva Convention on the Status of Data" that establishes international legal standards for government access to data.

Is data more secure and private when it is stored within a country's borders? A growing number of policymakers around the world seem to believe so, as various countries have created policies requiring certain data to be stored domestically, often in violation of the principles of free trade agreements.[1] These misunderstandings about the security and privacy of data result in policies that negatively affect innovation, productivity, trade, and consumer welfare.

The notion that data must be stored domestically to ensure that it remains secure and private is false. In regards to security, while certain laws may impose minimum security standards, the security of data does not depend on where it is stored, only on the measures used to store it securely. In regards to privacy, data owners, whether they are consumers or businesses, can rely on contracts or laws to limit voluntary data disclosures so that data stored abroad receives the same level of protection as data stored domestically. The primary situation in which differences may arise between countries is in the government-mandated disclosure of data, such as for law enforcement purposes.

This report provides a short guide to the implications of storing data on servers in foreign countries, with a foreign-owned service provider, or both, under various conditions. While the specifics vary depending on the particular country, in general, national laws restricting cross-border data flows are not needed to prevent inadvertent or voluntary disclosure of data. However, so that mandatory disclosures of data do not become an insurmountable hurdle for future trade in digital goods and services, ITIF recommends the United States engage its trading partners in developing a "Geneva Convention on the Status of Data" that establishes international legal standards for government access to data.

TYPES OF DATA DISCLOSURES

There are three ways that data may be released: inadvertent disclosures, voluntary disclosures, and mandatory disclosures.

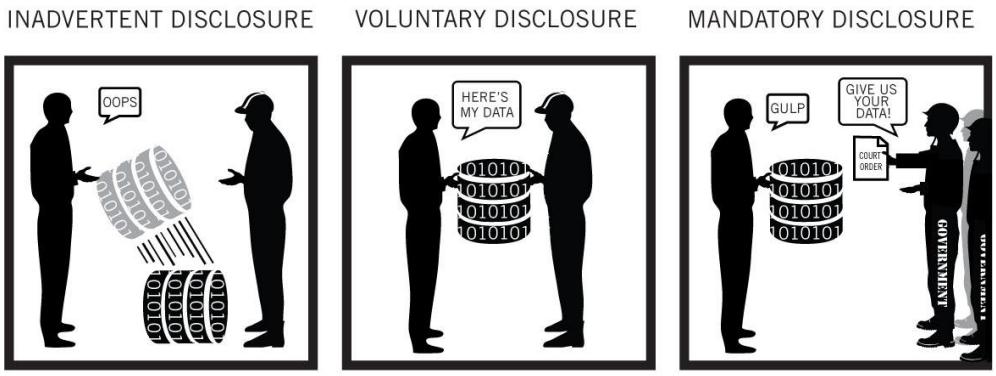

Figure 1: Types of data disclosures

Inadvertent disclosures occur when entities unintentionally disclose data about themselves or data entrusted to them by their clients or customers. Inadvertent disclosures are the result of security failures, such as hackers breaking into a corporate network to steal data, government agencies tapping into telecommunication links, or employees mistakenly posting sensitive data in a public forum. Organizations invest in security controls to mitigate the risk of inadvertent disclosures. Some countries may have laws requiring minimum security standards in certain situations or imposing fines for failure to prevent inadvertent disclosures.

Voluntary disclosures occur when one entity willingly shares data with others. Laws or contracts can limit voluntary disclosures of data as well as unauthorized use. An example of a statutory protection would be regulations preventing the disclosure of certain types of personally identifiable information to third parties, such as rules preventing doctors from sharing their patients' personal health data. Contracts can also be used to prevent voluntary disclosures. For example, a business might share its payroll data with its accounting firm, and ensure that the accounting firm does not disclose its data to other third parties by signing a confidentiality agreement. Or, consumers who back up their files using an online storage service can ensure that their information is not misused by the service provider by reviewing and ensuring the adequacy of the terms of service.

Mandatory disclosures occur when a government compels an entity to disclose certain data. A government may compel the data owner directly or compel a third-party with whom the data owner has voluntarily shared data. Governments impose certain legal obligations on third parties to disclose data, regardless of any other legal arrangements they may have with the data owner. For example, medical labs may be required to disclose confidential data about infectious diseases, banks may be required to disclose data on suspicious financial transactions, and accountants may be required to disclose audit findings. Third parties may also be obligated to disclose data for national intelligence and other law enforcement purposes. Third parties may not be required to notify the owner of the original data that

they have made a mandatory disclosure, and at times they even may be legally prohibited from doing so.

HOW VARIOUS SCENARIOS AFFECT THE SECURITY AND PRIVACY OF DATA

Determining which laws govern the disclosure of data can be complicated. Multiple countries may assert jurisdiction over data due to the nationalities of the individuals or organizations that own the data, the service providers storing the data, the individuals or organizations accessing the data, and, if the data contains personally identifiable information (PII), the individuals described in the data. In addition, countries may try to assert jurisdiction based on where the data is stored. The standards for determining jurisdiction may vary by country, but generally speaking, if an organization has a physical presence in a particular country, because it either does business in that country or employs service providers there, then it may be under the jurisdiction of that country. When an organization does not have a physical presence in a particular country (e.g., it has no staff or physical property in that country), various other factors may be used to determine whether that country has legal jurisdiction over a foreign organization (e.g., whether the organization directly markets its services in that country, whether it provides its products and services in other languages, etc.). Even if a country determines that its laws should apply to a foreign organization, it is often impractical to attempt extra-territorial enforcement.

The following scenarios provide an overview of how the security and privacy of data can be affected by where it is stored and with whom it is stored. In addition, the scenarios explore how various factors affect the rules governing disclosure, such as if the data owner is an individual or an organization, if the data includes PII or non-PII, and if the data owner has a physical presence in a foreign country. Clearly, the scenarios here are not exhaustive and only provide a sample of the various arrangements that might exist. For example, some multi-national organizations have subsidiaries in multiple countries with a multitude of business partners sharing data on citizens around the globe creating even more complex situations. However, the scenarios here illustrate the implications for the privacy and security of data in a variety of common arrangements.

Summary of Scenarios

As described below, the security of data does not depend on where it is stored, only on the measures used to store it securely. Security controls may be strong or weak in a foreign country, just as they can be strong or weak domestically. In addition, if a country mandates certain security requirements, companies providing services in that country, whether foreign or domestic, cannot avoid responsibility for these standards by storing data in another country as they can be held liable for violations of the law committed by their service providers.

Similarly, voluntary disclosures need not be negatively affected by where data is stored, since data owners should sign contracts only with service providers who agree to the same limitations on voluntary disclosures that the data owner must abide by. In addition, to the service contract, domestic and foreign laws may apply. Domestic laws limiting disclosure

by third-parties apply to domestic companies, even if they store their data in another country. If a foreign service provider improperly discloses data, the domestic company can still be held responsible under domestic law, and can in turn pursue action against its foreign service providers to recoup any losses. Data owners should consider the challenges that they might face in enforcing claims against foreign service providers when selecting a service. Contracts between data owners and their service providers generally add to any protections that may be based on geography.

Geography plays the most prominent role in government-mandated disclosure of data. In some situations, when a company is operating outside of the jurisdiction of a particular foreign country, it can prevent some government-mandated disclosures by not using service providers located in that foreign country. This is the only situation that cannot be resolved by technical measures or contract law, and if left unaddressed, this condition presents a serious threat to the global free flow of data.

Scenario 1: An Individual Sharing Non-PII With A Third Party

Let's begin with a simple example. Alice is a citizen and resident of Country A. She is considering where to store her data, none of which contains PII. She is considering alternative arrangements for storing her data, including storing the data with a domestic company whose servers are located in Country B, a service provider based in Country B whose servers are located in Country A, and a service provider based in Country B whose servers are located in Country B. How would each choice affect the security and privacy of her data?

		Type of disclosure		
		Inadvertent	**Voluntary**	**Mandatory**
Location of server and nationality of service provider	**Both servers and service provider in Country A**	Depends on security of service provider and laws in Country A.	Depends on contract with service provider and laws in Country A.	Depends on laws and treaties in Country A.
	Servers in Country B and service provider in Country A	Depends on security of service provider and laws in Country A and Country B.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Servers in Country A and service provider in Country B	Depends on security of service provider and laws in Country A and Country B.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Both servers and service provider in Country B	Depends on security of service provider and laws in Country B.	Depends on contract with service provider and laws in Country B.*	Depends on laws and treaties in Country A and Country B.

* The laws of Country A would also apply if Country A has jurisdiction over the service provider.

Figure 1: Factors affecting disclosure for an individual with non-PII, by type and location of data

As shown in Figure 1, on a technical level, inadvertent disclosures do not depend on the country in which a service provider is based or the country where data is stored. Data security depends on the technical, physical, and administrative controls implemented by the service provider which can be strong or weak, regardless of where that data is stored. To the extent that a particular country has mandatory security standards for organizations under its jurisdiction, a country's laws may set a baseline of security, although in practice many service providers will exceed minimum standards and adopt industry best-practices. Individuals interested in achieving high-levels of security, should obtain a service contract specifying the security practices that the service provider will use and closely evaluate the security measures used to protect their data. In addition, a country may use its laws to impose liability or other requirements on an organization that experiences a security breach. Just as individuals can specify certain security requirements in their service contracts, they can also use these contracts to obtain financial compensation or other remedies in the event of a security breach.

With regards to voluntary disclosures, all service providers, no matter where they are based or where they store their data, are responsible for unauthorized voluntary disclosures that conflict with their terms of service. In addition, service providers are bound by the laws of the countries in which they operate. Domestic service providers storing data domestically must comply with domestic law. Domestic service providers storing data abroad and foreign service providers storing data domestically are responsible for abiding by both foreign and domestic laws. Finally, foreign service providers storing data on servers located abroad are responsible for the laws limiting voluntary disclosure in their countries.

Consumers potentially gain additional protections against voluntary disclosure of their data by storing their data abroad with a domestic provider or with a foreign service provider since the service provider may be subject to laws in multiple countries limiting certain types of disclosures. For example, a service provider that discloses data from its customer may be in violation of trade secret laws and cyber crime laws, in addition to likely being in breach of its contract. In this case, being under multiple jurisdictions provides more, not fewer, restrictions on voluntary disclosures.

In this scenario, the only way that consumers might have fewer protections against the voluntary disclosure of their data compared to storing data in-country with a domestic provider would be if they store data with a foreign service provider using servers located abroad under the following three conditions: 1) the foreign service provider does not offer terms of service equivalent to the protections under domestic law; 2) the foreign service provider is outside of the jurisdiction of her home country; and 3) the foreign service provider operates in a country with weaker restrictions on voluntary disclosures than in the consumer's domestic country. In practice, these conditions often do not hold. For example, large providers such as Google, Yahoo, and Facebook, are often under the jurisdiction of many governments since they have a presence in many different countries. And competition in the marketplace should encourage service providers to adopt policies preferred by consumers. In addition, outside of blocking access to these services or punishing users who access them, there is little countries can do to prevent their citizens from accessing foreign services on the global Internet.

Finally, mandatory data disclosures occur under domestic laws when the data is stored on domestic servers by a domestic provider or under domestic or foreign laws when the data is stored out-of-country or with a foreign provider. In addition, many countries have signed treaties to provide assistance to other countries for law enforcement purposes.[2] Under these mutual legal assistance treaties (MLATs), law enforcement officials in one country can compel access to data stored by a third party in another country. When two countries have signed an MLAT, there will likely be little difference in the types of mandatory disclosures that law enforcement officials can compel based on the physical location of where the data is stored.

Scenario 2: A Company Sharing Non-PII with a Third Party

Now instead of an individual, let's consider a company sharing data with a third party. Acme Corp is based in Country A and does business exclusively in Country A. Again, none of the data contains PII or is owned by anyone else (e.g., records on the number of widgets produced by Acme Corp). How would different choices affect the privacy and security of the company's data?

		Type of disclosure		
		Inadvertent	**Voluntary**	**Mandatory**
Location of server and nationality of service provider	**Both servers and service provider in Country A**	Depends on security of service provider and laws in Country A.	Depends on contract with service provider and laws in Country A.	Depends on laws and treaties in Country A.
	Servers in Country B and service provider in Country A	Depends on security of service provider and laws in Country A and Country B.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Servers in Country A and service provider in Country B	Depends on security of service provider and laws in Country A and Country B.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Both servers and service provider in Country B	Depends on security of service provider and laws in Country B.	Depends on contract with service provider and laws in Country B.*	Depends on laws and treaties in Country A and Country B.

* The laws of Country A would also apply if Country A has jurisdiction over the service provider.

Figure 2: Factors affecting disclosure for a company with non-PII, by type and location of data

It turns out that there is no difference between Scenario 1 and Scenario 2 with regards to inadvertent disclosures, voluntary disclosures, or mandatory disclosures. Notice that in both scenarios voluntary disclosures can be limited by legal agreements between the data owner and its service provider, regardless of whether the data owner is an individual or a company. In practice, companies will have more resources available to them than individuals will to investigate and enforce the terms of service. When a company provides data to its service provider, it should obtain a contract defining exactly how the service provider can use its data. It does not matter where a service provider is located or where it

stores data, as long as the company can enforce its contract, either in a domestic court or in a foreign court.

Scenario 3: An Individual Sharing PII with a Third Party

Now consider a modification to scenario 1. As before, Alice is a citizen and resident of Country A. Now she is considering where to store her PII (e.g., personal health records). How do different choices affect the security and privacy of her data?

		Type of disclosure		
		Inadvertent	**Voluntary**	**Mandatory**
Location of server and nationality of service provider	**Both servers and service provider in Country A**	Depends on security of service provider and laws in Country A.	Depends on contract with service provider and laws in Country A.	Depends on laws and treaties in Country A.
	Servers in Country B and service provider in Country A	Depends on security of service provider and laws in Country A and Country B.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Servers in Country A and service provider in Country B	Depends on security of service provider and laws in Country A and Country B.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Both servers and service provider in Country B	Depends on security of service provider and laws in Country A and Country B.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.

Figure 3: Factors affecting disclosure for an individual with PII, by type and location of data

There is no difference between scenario 1 and scenario 3 for inadvertent disclosures and mandatory disclosures. For voluntary disclosures, Country A may try to impose its rules on foreign service providers operating in Country B solely on the basis of the fact that the foreign service provider knowingly has PII about its citizens.[3] In practice, most countries will not pursue many of these actions because of the complexity of extra-territorial enforcement.

Scenario 4A: A Company Sharing Domestic PII with a Third Party

Now let's consider more complicated examples. As before, Acme Corp, based in Country A, does business exclusively in Country A. However, now the company's data includes PII, and all of the PII is about citizens of Country A (e.g., names of customers and their purchase history). How would different choices affect the security and privacy of the company's data?

		Type of disclosure		
		Inadvertent	**Voluntary**	**Mandatory**
Location of server and nationality of service provider	**Both servers and service provider in Country A**	Depends on security of service provider and laws in Country A.	Depends on contract with service provider and laws in Country A.	Depends on laws and treaties in Country A.
	Servers in Country B and service provider in Country A	Depends on security of service provider and laws in Country A and Country B.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Servers in Country A and service provider in Country B	Depends on security of service provider and laws in Country A and Country B.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Both servers and service provider in Country B	Depends on security of service provider and laws in Country A and Country B.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.

Figure 4A: Factors affecting disclosure for a company with domestic PII, by type and location of data

There is no difference between scenario 2 and scenario 4A for inadvertent disclosures and mandatory disclosures. As in scenario 3, a country may try to impose its rules on foreign service providers operating abroad if the foreign service provider knowingly has PII about its citizens, although extraterritorial enforcement is likely to be limited. In addition, foreign service providers may be subject to additional constraints based on laws in their own country limiting how they voluntarily disclose data, even though the data concerns citizens in another country.[4]

And note that Acme Corp is still subject to domestic laws limiting voluntary disclosures even if a third party stores data on its behalf. This means that Acme Corp would be liable for any violations committed by its service provider even if these violations are legal in the country where the service provider is operating. In the event of a violation, citizens or their government could bring legal action against Acme Corp, and Acme Corp could in turn take legal action against the foreign service provider. Since Acme Corp cannot escape its legal responsibilities by storing data offshore, it has an incentive to ensure that its contract with its service provider does not allow the service provider to disclose data in violation of domestic law.

Scenario 4B: A Company Sharing Foreign PII with a Third Party

Now let's consider a revision of the previous scenario. Acme Corp is based in Country A but has some customers in Country B (although it has no physical presence in Country B). How would different choices affect the security and privacy of the company's data, particularly data on residents of Country B?

		Type of disclosure		
		Inadvertent	**Voluntary**	**Mandatory**
Location of server and nationality of service provider	**Both servers and service provider in Country A**	Depends on security of service provider.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Servers in Country B and service provider in Country A	Depends on security of service provider.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Servers in Country A and service provider in Country B	Depends on security of service provider.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Both servers and service provider in Country B	Depends on security of service provider.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.

Figure 4B: Factors affecting disclosure for a company with foreign PII, by type and location of data

This scenario is the same as scenario 4A, with the exception that domestic providers storing data domestically also may be subject to foreign laws in the case of voluntary and mandatory disclosure of data about foreign citizens. Once again, extraterritorial enforcement may be limited in practice.

Scenario 5: A Domestic Company Operating Abroad Sharing Foreign PII with a Third Party

In the final scenario, Acme Corp, based in Country A, has a satellite sales office in Country B and stores its data with a service provider. How would different choices affect the security and privacy of the company's data?

		Type of disclosure		
		Inadvertent	**Voluntary**	**Mandatory**
Location of server and nationality of service provider	**Both servers and service provider in Country A**	Depends on security of service provider.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Servers in Country B and service provider in Country A	Depends on security of service provider.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Servers in Country A and service provider in Country B	Depends on security of service provider.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.
	Both servers and service provider in Country B	Depends on security of service provider.	Depends on contract with service provider and laws in Country A and Country B.	Depends on laws and treaties in Country A and Country B.

Figure 5: Factors affecting disclosure for a company with foreign PII, by type and location of data

Just as economic isolationism inevitably leads to lower productivity for firms and higher costs for consumers, "data isolationism" will similarly lead to poor economic outcomes.

This scenario is the same as scenario 4B, although Country B may be better able to exercise its jurisdiction over Acme Corp since the company has a physical presence in the country. In scenario 4B, County B would have little recourse if Acme Corp ignored its laws.

RECOMMENDATIONS

The Internet has radically transformed how goods and services are delivered, and trade in digital goods and services is now a vital part of the globally networked economy. In the United States alone, exports of digitally-enabled services totaled $356 billion in 2011, having grown $74 billion since 2007.[5] Moreover, the rise of cloud computing has created unprecedented economies of scale for storing and processing data in large facilities such that it is often impractical and more expensive to restrict data to smaller data centers located in different countries.

A free and open Internet depends on the ability of individuals and companies to engage in commerce without geographic restrictions. Just as economic nationalism inevitably leads to lower productivity for firms and higher costs for consumers, "data nationalism" will similarly lead to poor economic outcomes. The importance of trade in digital goods and services in our global economy suggests that there is an increasing need for clarity on jurisdictional questions about data, particularly regarding government access to data. The need for transparency and consistency in how countries treat data has been made even more urgent by the recent public revelations about the extent to which various government agencies have engaged in surveillance of electronic data and communications. The uncertainty surrounding the extent to which countries may be compelling the disclosure of

confidential information further compounds this problem and limits the ability of companies in many countries to do business abroad.

Given that the complexity surrounding global data flows will only continue to grow and become more important to the global economy, ITIF makes two recommendations. First, countries should not restrict the flow of data beyond their own borders. Doing so does not protect consumers or businesses in any meaningful way from the risk of inadvertent or voluntary disclosures. Second, the United States should engage its trading partners in developing a "Geneva Convention on the Status of Data" that establishes international legal standards for government access to data. A multilateral agreement could settle questions of jurisdiction, establish rules of transparency, create better cooperation for legitimate law enforcement requests, and limit unnecessary access by governments to data on citizens of other countries. A multilateral agreement could also clarify which country's laws take precedence when companies encounter conflicting rules. By working to create a global pact on issues of government access to data, countries previously involved in mass electronic surveillance can also reassure people at home and abroad that they respect individual privacy and that they will hold each other accountable in the future.

ENDNOTES

1. Stephen Ezell, Robert Atkinson, and Michelle Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy," Information Technology and Innovation Foundation, September 25, 2013, http://www.itif.org/publications/localization-barriers-trade-threat-global-innovation-economy.
2. Winston Maxwell and Christopher Wolf, "A Global Reality: Government Access to Data in the Cloud," Hogan Lovells, July 18, 2012, http://www.hoganlovells.com/files/News/c6edc1e2-d57b-402e-9cab-a7be4e004c59/Presentation/NewsAttachment/a17af284-7d04-4008-b557-5888433b292d/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf.
3. See, for example, the COPPA Rule. http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions
4. See, for example, the HIPAA Privacy Rule.
5. U.S. International Trade Commission, "Digital Trade in the U.S. and Global Economies, Part 1," (Washington, DC: 2013), http://www.usitc.gov/publications/332/pub4415.pdf.

ACKNOWLEDGEMENTS

The author wishes to thank the following individuals for providing input to this report: Rob Atkinson, Alex Key, and Sue Wonder. Any errors or omissions are the author's alone.

ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with the Information Technology and Innovation Foundation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

FOR MORE INFORMATION, CONTACT ITIF BY PHONE AT 202.449.1351, BY EMAIL AT MAIL@ITIF.ORG, ONLINE AT WWW.ITIF.ORG, JOIN ITIF ON LINKEDIN OR FOLLOW ITIF ON TWITTER @ITIFDC AND ON FACEBOOK.COM/INNOVATIONPOLICY.