UNITED STATES INTERNATIONAL TRADE COMMISSION

Washington, DC

In the Matter of

DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES **Inv. No. 332-540**

TESTIMONY OF CHRISTOPHER WOLF

I want to thank the Members of the United States International Trade Commission for the opportunity to present this testimony in connection with your investigation of Digital Trade in the U.S. and Global Economies.

I am director of the global privacy law practice at Hogan Lovells US and am the founder and co-chair of the Future of Privacy Forum, a Washington, DC-based think tank committed to advancing privacy in business-practical ways, whose Advisory Board is comprised of privacy scholars, advocates and businesspeople. The views I express are mine only, and are not made on behalf of any clients of Hogan Lovells or participants in the Future of Privacy Forum.

Digital trade in the U.S. and global economies can flourish only if there is adequate protection of data, especially personal data, and only if business and consumers have trust that data will be protected in the digital ecosystem. The privacy and security of personal data, and the respect for personal control of data must be paramount in the digital trade environment. At the same time, excessive, duplicative or inconsistent regulation designed to provide the needed protections can serve as a drag on robust digital trade.

In this testimony, I would like to set forth the current and proposed frameworks in the United States and the European Union – two jurisdictions responsible for significant global digital trade – and suggest a focus for the Commission as it considers digital trade and the environment best suited to its endurance and growth.

Digital trade is growing in part because technological advancements have made it easier and more cost effective for businesses to collect, use, share, and store vast amounts of personal information about people. The role that personal data plays in digital trade means that privacy increasingly is becoming an important issue. Data rarely stays in only one jurisdiction. Rather, the Internet, social media, and Cloud computing cross national borders, allowing data to be transmitted to any location in the world. Thus, the privacy problem is not restricted to any one jurisdiction. Indeed, the wonder of modern technology is the ability of people to access information and entertainment from virtually anywhere, and to send information globally.

Policymakers around the world are re-examining the legal frameworks that regulate the collection, use, sharing, and storing of personal information and are seeking to make more robust the protections afforded to such information, and increasing the legal obligations of business.

The privacy frameworks recently proposed by the European Commission, the White House, and the Federal Trade Commission (FTC) seek more protection of individuals. Each of the proposals is founded on the same underlying principles of fairness known as "Fair Information Practice Principles" or "FIPPS". However, despite common foundations, the privacy regimes from opposite sides of the Atlantic exhibit fundamental differences in approach and substance.

The Fair Information Practice Principles focus on empowerment of people to control their personal information and on safeguards to ensure adequate data security. FIPPs form the core of the 1980 OECD privacy guidelines on which both the U.S. and European models are based, and that were adopted "to harmonise national privacy legislation and, while upholding [ ] human rights, [ ] prevent interruptions in international flows of data."

Historically, the EU and U.S. have taken divergent approaches to implementing the FIPPs. In the U.S. where privacy interests are balanced with the right to free expression and commerce, and where the legal framework assumes that – as a practical matter – not every piece of personal information can be protected and policed, the framework provides the highest levels of protection for sensitive personal information, such as financial, health and children's data.

For example, the Gramm-Leach-Bliley (GLB) Act regulates how financial institutions collect, disclose, share, and protect personally identifiable financial information. The Health Insurance Portability and Accountability Act (HIPAA) regulates the use and disclosure of "protected health information" by such entities as physicians, hospitals, and health insurers. And the Children's Online Privacy Protection Act of 1998 (COPPA) and its recently updated regulations from the FTC, regulate online collection and use of the personally identifiable information of children.

A major, if not defining characteristic of U.S. privacy law, comes from the targeted enforcement actions against bad (or negligent) actors – principally by Federal Trade Commission. The FTC effectively has created a "common law" of what is expected from business when it comes to the collection, use, and protection of personal information. The FTC has authority to take enforcement action against "unfair or deceptive" practices. In the privacy context, this has resulted in enforcement actions against companies that have promised something in their privacy policies about the collection, use, or protection of personal information but, in practice, handled the personal information in ways that differed from the promised treatment.

Data security breach notification laws, requiring public disclosure of information security mishaps, have created a negative incentive for businesses to buttress the protection of personal data (to avoid having to report breaches to regulators and to the public). With the advent of the breach notification laws, the FTC developed new targets for enforcement – inadequate information security programs. A number of FTC enforcement actions have resulted in consent decrees requiring comprehensive data security programs that are regularly assessed and reported upon by independent outside auditors. (The FTC's security authority using the unfairness prong of its Section 5 jurisdiction currently is being challenged in a federal court litigation brought by a target of one of its investigations.)

The 2011 settlement by large online companies with the FTC contained, for the first time, requirements for comprehensive (and auditable) privacy programs, patterned on the FTC requirements in the data security area. These program requirements are seen as creating a new and heightened FTC standard for protection of consumer data.

In addition, Chief Privacy Officers (CPOs) are proliferating and gaining in importance in U.S. businesses, adding to the level of American privacy protection. CPOs ensure that there are documented and enforceable compliance and training programs in place within businesses to provide physical, administrative, and technical protections for personal data, and to ensure that new products and services take privacy considerations into account.

In this connection, a 2011 Stanford Law Review article, University of California at Berkeley Professors Kenneth Bamberger and Deirdre Mulligan presented findings from the first study of corporate privacy management in fifteen years. Bamberger and Mulligan effectively responded to the criticism of the U.S. privacy regime as lacking sufficient legal protections (what they termed "privacy on the books") with a descriptive account of privacy "on the ground." They explored the emergence of the Federal Trade Commission as a privacy regulator; the increasing influence of privacy advocates; market and media pressures for privacy protection; and the rise of privacy professionals, and concluded that, together, these factors played a major role in preventing violations of consumers' expectations of privacy in the United States.

The European Union's approach to protecting privacy (data protection) is in contrast to the U.S. approach. Currently, the EU has a region-wide Directive, with national laws in twenty-seven jurisdictions to implement the requirements of the Directive, purports to regulate every piece of personal information and is predicated on the notion that privacy is a fundamental human right. Thus, under the approach of across-the-board regulation, there are strict limits on the collection and use of information, although enforcement of those limits has been episodic.

Policymakers in the European Union firmly believe that the framework there is superior to that of the United States, and they have been steadfast in the belief that because the United States does not have an across-the-board privacy law, its protections are inadequate and transfers of personal data from the EU to the U.S. must be controlled and subject to special regulation. Viviane Reding, Vice President of the European Commission and Commissioner for Justice, Fundamental Rights and Citizenship, is skeptical of anything less than comprehensive U.S. privacy legislation akin to that in the EU.

The belief on the European side that the United States lacks adequate protections for personal data theoretically could mean that personal data could not be transferred across EU borders to the United States, bringing trans-Atlantic commerce to a grinding halt. To address that unthinkable result, legal mechanisms have been established, requiring expense and burden, to transfer data from the EU to the U.S. These mechanisms are the EU-U.S. Safe Harbor, which requires eligible businesses to certify compliance with the Safe Harbor principles of notice, choice, onward transfer, data integrity, security, access, and verification and enforcement; Model Contracts, which are standard contractual clauses approved by EU authorities that must be included in agreements that involve the transfer of personal data outside the EU; and Binding Corporate Rules, which are a set of comprehensive internal policies and procedures that allow for intra-company cross-border transfers, and that must conform to standards approved by EU authorities. Still, those mechanisms are costly and burdensome and, some say, an unnecessary drag on digital commerce that could be alleviated by the recognition of the US framework as "adequate" by the European Union. Countries including Uruguay, Argentine, and Israel

have been deemed adequate by the EU, allowing the free flow of data across borders without the mechanisms that U.S. businesses must employ.

Turning now to proposals for changes to or reforms in the privacy frameworks in the US and in the EU: In January 2012, the European Commission unveiled a new proposal for privacy in the EU, calling for a region-wide Regulation that would replace national laws passed in each EU Member State to implement the 1995 Directive on Data Protection and proposing strict new privacy rules (and penalties for violating those rules). Upon final passage of the Regulation, the current 1995 Data Protection Directive would be repealed. The proposed rules are intended to take into account the pervasive new technologies capable of collecting and sharing information about people, and to give individuals more control over their personal information.

Under the new Regulation, individuals and organizations would only need to deal with one supervisory authority, located in the country of their main establishment or residence, rather than the fragmentary jurisdiction currently provided by the Directive. The Regulation would make organizations outside the EU subject to its provisions if they process personal data to offer goods or services to EU residents, or monitor their behavior. (A recent proposal to amend the Regulation proposal would extend even further EU jurisdiction over entities outside the region.)

A new principle of accountability would require data controllers to demonstrate their compliance with the law by maintaining extensive documentation on their processing, implementing appropriate security requirements, and performing impact assessments when required. This would replace the current requirement of administrative filings.

There are new rights to have data deleted (the "right to be forgotten") and to move data from one service to another ("data portability"), which would have a particular effect in relation to social media, but which also could affect the right to free expression and First Amendment rights in the United States and online generally.

Borrowing from the U.S.-developed concept of data security breach notification laws, data breaches would have to be reported to supervisory authorities without undue delay and, where feasible, within twenty-four hours – a time period most professionals experienced with data breach notification view as impractical. “Serious breaches” must also be reported to affected individuals.

Where consent is to be a ground for data processing, it must be explicit. Implied consent will no longer be possible and, once given, consent can be withdrawn at any time.

Fines may be imposed by supervisory authorities for breaches, reaching up to 2 percent of an organization's annual turnover in the most serious cases. This potential fining authority for failing to abide by the Regulation’s many still-to-be-clarified provisions is viewed by many as potentially draconian.

The draft Regulation has entered the political process of the EU ordinary legislative procedure, under which agreement will need to be reached between the European Parliament and the Council.

In the United States, the Obama Administration in 2012 announced its "Privacy Blueprint" for the United States, calling for legislation containing a Privacy Bill of Rights and proposing enforceable codes of conduct developed through a so-called "Multistakeholder Process."

The cornerstone of the Administration's privacy blueprint is the Consumer Privacy Bill of Rights, which adapts the decades-old Fair Information Practice Principles to the interconnected and interactive world. The Privacy Bill of Rights applies to commercial uses of personal data and seeks to provide greater privacy protection for consumers and greater regulatory certainty for businesses.

There are seven core rights that comprise the Privacy Bill of Rights:

1. Individual Control: Consumers have a right to exercise control over what personal data organizations collect from them and how they use it.

2. Transparency: Consumers have a right to easily understandable information about privacy and security practices.

3. Respect for Context: Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.

4. Security: Consumers have a right to secure and responsible handling of personal data.

5. Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate.

6. Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.

7. Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

The Administration's blueprint contemplates a multistakeholder approach spearheaded by the Department of Commerce that will produce enforceable codes of conduct that implement the Privacy Bill of Rights. The multistakeholder approach is championed by the Administration due to the "flexibility, speed, and decentralization necessary to address Internet policy challenges." This process is designed to avoid a one-size-fits-all approach and instead opts for flexibility and a tailored standard. In addition to flexibility, the speed with which the multistakeholder process is expected to be able to produce solutions – as compared to the regulatory or law making process – is also appealing due to the constantly evolving nature of privacy issues.

Under the sponsorship of the United States Department of Commerce, one multistakeholder process is underway with respect to Mobile Application Privacy and additional multistakeholder processes are expected to be initiated soon.

Referring to the differences in national privacy laws that create challenges for businesses that wish to transfer data across national borders, the Administration has stated that it is "critical to the continued growth of the digital economy that they strive to create interoperability between privacy regimes." The Administration expresses its desire to promote international interoperability by pursing mutual recognition of commercial privacy frameworks, international codes of conduct based on the multistakeholder process, and bilateral or multilateral enforcement cooperation.

Finally, the Administration has called on Congress to adopt the Consumer Privacy Bill of Rights, asking Congress to provide the FTC and State Attorneys General with the power to enforce those rights and asking for a national standard for security breach notification that would replace the patchwork of state breach notification laws that are currently in effect in forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands.

In 2012, the Federal Trade Commission – the lead federal regulator of privacy practices by business -- issued a report on privacy containing that agency's expectations and hopes for the collection of personal information. Entitled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," the Report is intended to articulate "best practices" for companies that collect and use consumer data, and to assist Congress as it considers new privacy legislation.

The Report calls for companies to implement (1) privacy by design, (2) simplified consumer choice, and (3) greater transparency; and it recommends that Congress pass baseline privacy legislation. The Report also encourages companies to incorporate substantive privacy protections (e.g., data security, collection limits, retention and disposal practices, and data accuracy) and maintain comprehensive data management procedures throughout product and service life-cycles. In addition, companies are called upon to give consumers a choice about their data at a time and in a context in which the consumer is making the decision, and to obtain affirmative express consent before collecting sensitive data or making material retroactive changes to privacy representations. The Report proposes that privacy notices should be clearer, shorter, and more standardized.

In the Report, the FTC recommends new targeted legislation to address the practices of information brokers, and recognizes that the more sensitive the data, the greater the protections needed. The new framework applies to both online and offline contexts and to data that is "reasonably linkable" to specific consumers, computers or devices.

As is evident from these descriptions of the EU, White House, and FTC 2012 proposals, there indeed are common aspects to the EU and U.S. proposals. Both call for implementation of the "Privacy by Design" concept intended to build in privacy sensitivity and consideration into every stage of the development of products and services. Both recognize the importance of accountability by those who collect and use personal data. Both reflect the principle that people should not be surprised by the use of their personal data collected for one purpose but used for another purpose. There is no disagreement about the need for informed consent about the collection and use of personal information (although the kind of consent envisioned in each jurisdiction differs as to various categories of data). Finally, the U.S. view of what constitutes "personal data" seems to be moving toward the EU's: the FTC refers to data that can be "reasonably linked to a specific consumer, computer or other device," a standard very close to —and arguably even broader than—the EU definition of personal data.

Big differences in approach emerge from the fact that the United States, while proposing a first-ever federal privacy law with a "Privacy Bill of Rights," still intends to rely on a variety of self-regulation (more

precisely, co-regulation, since self-regulatory rules could be enforced by law enforcement). And the U.S. proposed rules do not contemplate a "right to be forgotten," a major feature of the EU proposal and one that First Amendment scholar Professor Jeffrey Rosen has labeled "the biggest threat to free speech on the Internet in the coming decade."

Similarly, there is no right to "data portability" in the U.S. proposals as there is in the EU plan. The EU proposal contemplates broad jurisdiction to enforce its law, even extending to U.S. businesses without a physical presence in the EU, under certain circumstances. And even though the EU has borrowed the data breach notification idea from the United States, it proposes a presumptive obligation to provide notice within twenty-four hours of a breach, a time frame widely regarded as wholly unworkable by those who have worked under the U.S. data breach laws. Finally, the EU proposes a schedule of monetary fines of up to 2 percent of an entity's global worldwide turnover for violations of the proposed Regulation—an amount that many stakeholders view as unreasonable due to the discretion given to enforcers in assessing such a fine.

Separate and apart from the proposals in the U.S. and the EU for new privacy frameworks, and distinct from the current legal and regulatory frameworks governing the collection, use and handling of personal data, is the issue of government access (including law enforcement, regulatory and national security access) to data stored in the Cloud. Cloud service providers outside the United States and others have made allegations about government access to the effect that data sent to US-based Cloud providers is at greater risk than data sent to Cloud providers in other jurisdictions. My law firm has prepared a white paper on that issue (attached as an Appendix to this Testimony) and will be issuing further studies with respect to that issue demonstrating that claims about US governmental access to data in the cloud compared with other governments' access are exaggerated and often misstated. Those exaggerations and misstatements have the potential of impeding digital trade to the detriment of US-based Cloud providers.

With this background, I would like to respectfully suggest that the Commission pay close attention to the proposals for new privacy and data protection frameworks and consider the following issues:

1) How can data protection and privacy be achieved without unnecessarily interfering with digital trade?

2) How should proposals for new privacy frameworks be evaluated in light of the goal of digital free trade? Are there specific aspects of the proposals that are likely to present impediments to digital free trade?

3) How can interoperability and mutual recognition of privacy/data protection frameworks be achieved and will the proposed privacy frameworks or any aspects of them interfere with the goal of interoperability and mutual recognition?

4) Will the EU rules on the "adequacy" of other nations' privacy frameworks act to create impediments to digital trade in circumstances where interoperability and mutual recognition are appropriate?

Finally, I note that in the State of the Union Address, President Obama recently announced the Administration's intention to begin negotiations for an EU-U.S. Free Trade Agreement with the goal of reducing barriers to trade and investment, and to improving the trans-Atlantic economies. In February 2013, the so-called U.S.-EU High Level Working Group issued a report recommending the launch of trade and investment negotiations between the United States and the European Union and specifically mentioning the desirability of harmonizing and making more compatible regulations and standards to advance trans-Atlantic trade. The Commission's focus on impediments to digital trade in its forthcoming Report can provide valuable information and insights relevant to the upcoming EU-U.S. Free Trade Agreement negotiations especially with respect to the potential for more compatible regulations and standards for the protection of data, including especially personal data.

Thank you for the opportunity to present this Testimony to the Commission.

Prepared February 28, 2013

Appendix

A Global Reality: Governmental Access to Data in the Cloud

A Hogan Lovells White Paper

A Global Reality: Governmental Access to Data in the Cloud

A comparative analysis of ten international jurisdictions

Governmental access to data stored in the Cloud – including cross-border access – exists in every jurisdiction

by

Winston Maxwell, Paris, France
Christopher Wolf, Washington, DC*

23 May 2012

Updated 18 July 2012

Introduction

Cloud computing is revolutionizing the way companies use information technology. Cloud service providers make it possible for businesses and consumer users across the globe to access services via the Internet, reducing costs and increasing efficiency. That's why Cloud computing continues to grow.

As Cloud computing adoption by business has increased, some people have expressed concern over the possibility of governmental access to data in the hands of a Cloud service provider. "[B]oth Cloud users and providers of Cloud services are struggling to understand when and how governments can access users' data."[1]

This White Paper examines the extent to which access to data in the Cloud by governments in various jurisdictions is possible, regardless of where a Cloud provider is located. "Governmental access," as that term is used here, includes access by all types of law enforcement authorities and other governmental agencies, recognizing that the rules may be different for law enforcement and national security access.

Governments need some degree of access to data for criminal (including cybercrime) investigations and for purposes of national security. But privacy and confidentiality also are important issues. This paper does not enter into the ongoing debate about the potential for excessive government access to data and insufficient procedural protections. Rather, this White Paper undertakes to compare the nature and extent of governmental access to data in the Cloud in many jurisdictions around the world.

Both Cloud users and providers of Cloud services are struggling to understand when and how governments can access users' data.

Misconceptions About Governmental Access

Drawing on practical and anecdotal experience, it seems to us that businesses often assume knowledge of the laws regulating governmental access to data in their home jurisdictions, and they make further assumptions about the legal regimes abroad where Cloud service providers may be located. For example, especially in Europe the **2001 USA PATRIOT Act** ("Patriot Act") has been invoked as a kind of shorthand to express the belief that the United States government has greater powers of access to personal data in the Cloud than governments elsewhere. However, our survey finds that even European countries with strict privacy laws also have anti-terrorism laws that allow expedited government access to Cloud data. As one observer put it, France's anti-terrorism laws make the Patriot Act look "namby-pamby" by comparison.[2] Frequently, there are misconceptions about what the law allows, at home and abroad.

Businesses often assume knowledge of the laws regulating governmental access to data in their home jurisdictions, and they make further assumptions about the legal regimes abroad where Cloud service providers may be located.

* Special thanks to Hogan Lovells colleagues Bret Cohen and Steven Spagnolo for their assistance in preparing this White Paper, and to Tim Brookes (Australia), Susan Goodman (Australia), Srishti Natesh (Australia), Mark Hayes (Canada), Oana Dolea (Canada), Lars Stoltze (Denmark), Kristian Pedersen (Denmark), Lionel de Souza (France), Stefan Schuppert (Germany), Martin Pflueger (Germany), Jeanne Kelly (Ireland), Eiichiro Kubota (Japan), Kiyoko Nakaoka (Japan), Gonzalo Gállego (Spain), Belén Gámez (Spain), Quentin Archer (UK), Mac Macmillan (UK), and Viktor Braun (UK) for their assistance in the study of the laws around the world.

[1] Georgetown University Law Center March 2012 seminar announcement, "Law Enforcement Access to the Cloud," http://www.law.georgetown.edu/news/events/cloudseminar.html.

[2] Steven Erlanger, *Fighting Terrorism, French-Style*, N.Y. TIMES, March 30, 2012, http://www.nytimes.com/2012/04/01/sunday-review/the-french-way-of-fighting-homegrown-terrorism.html.

Such misconceptions encourage speculation that governmental access to data stored in the Cloud is more likely in some places than in others, and that the best way to limit such access is to use Cloud service providers present only in "safe" jurisdictions – places where data are thought to be free from troublesome governmental access. Thus, some believe (and some providers have advertised) that choosing a Cloud service provider based on its location will make data stored in the Cloud more secure and less subject to governmental access.[3]

Summary of Conclusions

On the fundamental question of governmental access to data in the Cloud, we conclude, based on the research underlying this White Paper, that it is not possible to isolate data in the Cloud from governmental access based on the physical location of the Cloud service provider or its facilities. Government's ability to access data in the Cloud extends across borders. And it is incorrect to assume that the United States government's access to data in the Cloud is greater than that of other advanced economies.

The United States Ambassador to the European Union, William E. Kennard, recently spoke at the 2012 European Cloud Computing Conference in Brussels and made the following observation, which is confirmed by our study:

> While some cloud providers here in Europe have recently made the fear of unlimited U.S. Government access to data a selling point for their services, this is an inaccurate assessment and completely ignores the facts. . . . While our systems may differ in approach, let me assure you that we have in place protections that are fundamentally similar to those in Europe. In a number of critical areas, the U.S. provides more restrictions to the access of personal data than do European Member States.[4]

Some erroneously believe the best way to limit governmental access to data is to use Cloud service providers present only in "safe" jurisdictions – places where data are thought to be free from troublesome governmental access.

In addition to domestic legal frameworks enabling governmental access to data within a country, **Mutual Legal Assistance Treaties ("MLATs")**, which are in effect between and among countries around the world, can provide governments the ability to access data stored in one jurisdiction but needed for lawful investigative purposes in another. Despite the procedural hurdles that may exist to request and obtain information pursuant to MLATs, these treaties make borders and the physical location of data much less significant barriers to governmental access.

The existence of MLATs diminishes any argument that data stored in one jurisdiction is immune from access by governmental authorities in another jurisdiction. For example, Germany signed a Mutual Legal Assistance Treaty in Criminal Matters with the United States in 2003 and a Supplementary Treaty to the Mutual Legal Assistance Treaty in Criminal Matters in 2006. Both treaties entered into force on October 18, 2009 and allow authorities in each country to request and receive information located in the other's jurisdiction (including information stored in third-party facilities).

The existence of Mutual Legal Assistance Treaties greatly diminishes any argument that data stored in one jurisdiction is immune from access by governmental authorities in another jurisdiction.

On a related issue, there is significant discussion today about the power of a government to require a party in its jurisdiction to access and produce data stored in *another* jurisdiction, based on principles of physical presence of the party (not the data, or where the party is headquartered). In other words, the fact that a business located in one country may have chosen to store its data in the Cloud in another country does not mean that the business is immune from governmental demands for the production of that off-shored data. Of the countries we surveyed, Germany and Japan are the only two that, in some instances, limit the data that the government can access to that which is physically located on servers within their national borders.

This White Paper examines the laws of ten countries, including the United States, with respect to governmental authorities' ability to access data stored in or transmitted through the Cloud, and documents the similarities and differences among the various legal regimes. All ten of these countries have strong legal protections on civil rights and due process.

Notably, **every single country that we examined vests authority in the government to require a Cloud service provider to disclose customer data in certain situations, and in most instances this authority enables the government to access data physically stored outside the**

[3] In December 2011, European Commission Vice-President Viviane Reding criticized Cloud service marketing that suggested that an EU location shielded data from governmental access. Scott M. Fulton, *EU's Reding to Cloud Providers: Stop Sheltering Yourself from US Patriot Act*, READWRITEWEB, May 2, 2012, http://www.readwriteweb.com/cloud/2011/12/eus-reding-to-cloud-providers.php.

[4] Remarks by William E. Kennard, United States Ambassador to the European Union at the 2012 European Cloud Computing Conference (Mar. 12, 2012), http://useu.usmission.gov/kennard_032112.html.

country's borders, provided there is some jurisdictional hook, such as the presence of a business within the country's borders. Even without that "hook," MLATs can be used to allow access to data across borders.

Every single country that we examined vests authority in the government to require a Cloud service provider to disclose customer data in certain situations, and in most instances this authority enables the government to access data physically stored outside the country's borders, provided there is some jurisdictional hook.

Furthermore, as we describe in this White Paper and as illustrated in the chart at the end, in jurisdictions *outside* the United States, there is the real potential of data relating to a person, but not technically "personal data," stored in the Cloud being disclosed to governmental authorities *voluntarily*, without legal process and protections. In other words, governmental authorities can use their "influence" with Cloud service providers – who, it can be assumed, will be incentivized to cooperate since it is a governmental authority asking – to hand over information outside of any legal framework. **United States law specifically protects such data from access by the government outside of legal process.**

U.S. law prohibits the voluntary disclosure of ***any type*** of Cloud customer data to the government without a formal legal request, unless certain limited exceptions apply, such as in the event of an emergency involving death or serious bodily injury requiring disclosure. Cloud providers in the U.S. face civil and criminal penalties for violating the laws against voluntary disclosure to the government. Furthermore, the ability of a third-party Cloud service provider voluntarily to hand over customer data may also be restricted by contract.

We conclude that civil rights and privacy protections related to governmental access to data in the Cloud are not significantly stronger or weaker in any one jurisdiction, and that any perceived locational advantage of stored Cloud data can be rendered irrelevant by MLATs. Our review reveals that businesses mislead themselves and their customers if they rely on an assumption that selecting Cloud service providers based in one jurisdiction or another better insulates data from governmental access. Instead, our study indicates that it is in business' interest to support governmental cooperation in this area, as it is the consistent and reasonably restrained exercise of existing legal authorities that will enable the economic growth and other benefits of Cloud computing.[5]

[5] We also note that often overlooked are governmental requirements for long-term retention of data, a requirement that does not exist in the United States. For example, EU "Directive 2006/24/EC" is a Directive issued by the European Union and relates to telecommunications data retention. Service providers in member states must store citizens' telecommunications data for six to twenty-four months, stipulating a maximum time period. Under the Directive, police and security agencies are able to access, in most cases with judicial permission, details such as IP address and time of use of every email, phone call, and text message sent or received. Obviously, a law that perpetuates the existence of data that might not otherwise be available to governmental authorities (because it would have been deleted) is a factor to be considered in evaluating the favorability of one jurisdiction over another as a service provider location.

Our review reveals that businesses are misleading themselves and their customers if they contend that restricting Cloud service providers to one jurisdiction better insulates data from governmental access.

Methodology

To conduct our examination, we consulted with experienced local counsel knowledgeable about data protection and governmental access law in each of the jurisdictions on which we report, asking the following questions for each jurisdiction:

1. May government require a Cloud provider to disclose customer data in the course of a government investigation?
2. May a Cloud provider voluntarily disclose customer data to the government in response to an informal request?
3. If a Cloud provider must disclose customer data to the government, must the Cloud provider notify the customer?
4. May government monitor electronic communications sent through the systems of a Cloud provider?
5. Are government orders to disclose customer data subject to review by a judge?
6. If a Cloud provider stores data on servers in another country, can the government require the Cloud provider to access and disclose it?

We start with an overall review of MLATs. These treaties effectively make a country's borders less significant for purposes of governmental access to data, and likewise make less significant the location of a Cloud service provider within one country's borders as opposed to another country's borders. We then review the situation with respect to governmental access in the United States and proceed to examine the situations in Australia, Canada, Denmark, France, Germany, Ireland, Japan, Spain, and the United Kingdom. We conclude with an observation about the current proposals for reform of data protection laws in

the EU, which would leave unchanged the current approach regarding governmental access to data.

1. MUTUAL LEGAL ASSISTANCE TREATIES

Governmental authorities are able to reach data stored on the servers of a Cloud service provider over whom they do not have jurisdiction through an **MLAT** with a foreign nation where the Cloud service provider is based. For example, the United States and member states in the European Union have entered into bilateral MLATs that allow governmental authorities on both sides of the Atlantic to request access to data stored on the servers of a Cloud service provider physically located in or subject to the jurisdiction of the foreign nation.

Pursuant to an agreement governing MLATs between the U.S. and EU member states, a request for data shall only be denied on data protection grounds in "exceptional cases." That is, most MLAT requests for data will be honored by the recipient party. Currently, Article 13(3) of Framework Decision 2008/977/JHA of the Council of the European Union allows transfers of personal data for law enforcement purposes even to countries whose privacy regimes have not been found "adequate" by the EU where there are "appropriate safeguards." The phrase "appropriate safeguards" is widely interpreted to include international agreements such as MLATs.

Other treaties, such as the multilateral Council of Europe Convention on Cybercrime, as well as informal relationships between law enforcement agencies, also allow for governmental access to data in the "possession, custody, or control" of Cloud service providers over whom the requesting country does not otherwise have jurisdiction.

The existence of these treaty relationships diminishes any perceived advantage of placing data with a Cloud service provider in a jurisdiction believed to permit less governmental access than other jurisdictions covered by the treaties. For all practical purposes, the laws permitting governmental access by the requesting country have their reach extended through operation of the treaties.

2. UNITED STATES

Any discussion of U.S. government access to data in the Cloud needs to begin with the Patriot Act, which commonly, but erroneously, is believed to have created invasive new mechanisms for the United States government to get information. The reality is that most of the investigatory methods in the Patriot Act were available long before it was enacted. And those investigative tools had, and still have, limitations imposed by the United States Constitution and by statute. It is more accurate to say that the Patriot Act did not create broad new investigatory powers but, rather, expanded existing investigative methods, and retained Constitutional and statutory checks on abuse.

Even with the Patriot Act, it is generally the case in the United States that the more substantive the data sought by the government, the greater the government's burden of demonstrating a strong legal justification to obtain that data. That is, there are greater restrictions on accessing the contents of electronic files and communications ("content data") than for other information associated with those files such as the file owner's contact information and server log information ("non-content data").

In most circumstances, governmental access to data stored by a Cloud service provider is regulated under the Electronic Communications Privacy Act ("ECPA"). Under ECPA, if a government body seeks disclosure of customer data from a Cloud service provider, it can only do so if a legal mechanism is used – if a judge issues a **search warrant** or special **ECPA court order**, or if the government issues a valid **subpoena** to the provider. The legal mechanism to be used depends on the category of information:

- A search warrant issued upon a finding of **probable cause** that a crime has been committed is required under ECPA when the government seeks email that is stored in the Cloud for 180 days or less, whereas an ECPA court order or subpoena can be used to request stored email more than 180 days old, or any documents or data stored in the Cloud.[6]

- A judge can issue an ECPA court order for Cloud data only if the government demonstrates that there exist **reasonable grounds to believe** that the data sought are relevant and material to an ongoing investigation.

- Prosecutors and other government investigators may issue subpoenas requesting Cloud data directly to Cloud service providers if the data are relevant to the investigation.

If the government requests customer content data from a Cloud service provider through an ECPA court order or a subpoena, the government must notify the customer before obtaining the requested data from the provider unless it can demonstrate that providing prior notice would result in danger to a person's physical safety or compromise the

[6] An influential U.S. appeals court recently held that a search warrant is always required to access the contents of email stored in the Cloud pursuant to a search warrant, regardless of the number of days the emails have been stored with the Cloud provider. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). We note that this court only has jurisdiction over federal cases brought in four states, although other appeals courts could decide to follow the reasoning of the case and adopt its ruling.

investigation, in which case notice may be delayed. Where such delay is not sought by the government, the customer can challenge the governmental request. However, no prior notice is required to customers when the government requests (i) non-content data or (ii) content data via a search warrant, although customers can challenge the validity of search warrants in court after the data are produced.

United States

It is generally the case in the United States that the more substantive the data sought by the government, the greater the government's burden of demonstrating a strong legal justification to obtain that data.

Significantly, ECPA prohibits Cloud service providers from **voluntarily** disclosing customer data stored on their servers to the government without having received a formal legal request, unless certain limited exceptions apply, such as a provider's good faith belief that an emergency involving danger of death or serious physical injury requires disclosure.

And ECPA prohibits the United States government from intercepting electronic data in transit unless a judge determines that there exists **probable cause** to believe that the data will contain evidence of a federal crime, and that normal investigative procedures (i) have been tried and failed, (ii) reasonably appear to be unlikely to succeed if tried, or (iii) are too dangerous. When the government cannot obtain the required evidence in time and there is an emergency situation involving a danger of death or serious physical injury, issues of national security, or organized crime, the government can intercept electronic data without a judicial order, but must apply for an order within forty-eight hours after the interception has occurred.

Outside of these customary methods of access to Cloud data under ECPA, the U.S. government can access Cloud data through **FISA Orders** and **National Security Letters ("NSLs")** during the course of certain counterterrorism or foreign intelligence investigations.

- A judge can issue a FISA Order authorizing the government to obtain **content data** if the government demonstrates that there exist **reasonable grounds to believe** that the data sought are relevant to an investigation to obtain foreign intelligence or to protect against international terrorism or spying.[7]
- Government investigators may issue special administrative subpoenas called NSLs directly to Cloud service providers. NSLs request certain **non-content data** about their customers – specifically subscriber information, length of service, and certain transactional records – if the government certifies that the request is relevant to an investigation to protect against international terrorism or spying. **The United States government may not use NSLs to obtain access to the *content* of electronic records and documents stored on a Cloud service provider's servers.**

FISA Orders and NSLs were available to the United States government even before the Patriot Act was enacted. The Patriot Act merely expanded some of the provisions of these access methods. For example, it added "gag order" provisions prohibiting recipients of FISA Orders or NSLs from disclosing the fact that they have received an NSL, except as necessary to comply with or challenge the request, and expanded the types of information obtainable through FISA Orders.

There are, however, meaningful limitations on United States government access to Cloud data through FISA Orders and NSLs. First and foremost, their use is limited to certain counterterrorism or foreign intelligence investigations, so the government cannot use these methods to obtain documents and records for the sole purpose of investigating domestic criminal activity. A Cloud service provider has the ability to oppose a FISA Order before the issuing court, and also can seek judicial review of an NSL, which can be set aside "if compliance would be unreasonable, oppressive, or otherwise unlawful." A Cloud service provider also may petition the court to overturn the "gag order." And even though FISA Orders can require a Cloud provider (or any other business) to produce "business records" (a term that would encompass Cloud data), the United States government rarely requests them. In 2010, the government only made 96 applications for FISA Orders granting access to business records.[8]

The United States, like other countries, takes the position that it can use its own legal mechanisms to request data from any Cloud server located anywhere around the world so long as the Cloud service provider is subject U.S. jurisdiction: that is, when the entity is based in the United States, has a subsidiary or office in the United States, or

[7] The recent appeals court decision discussed *supra* note 6 also suggests that the government must obtain a search warrant to access the contents of email even when requested pursuant to a FISA Order, which would require the higher "probable cause" standard to authorize a FISA Order when the contents of email are sought.

[8] *See* Letter from Ronald Welch, Ass't Att'y Gen., U.S. Dep't of Justice, to The Hon. Harry Reid, U.S. Senate Majority Leader (Apr. 29, 2011), http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf.

otherwise conducts continuous and systematic business in the United States.

In sum, governmental authorities in the United States cannot access data stored in the Cloud at will. Rather, governmental authority is circumscribed by the United States Constitution and state constitutions, judicial oversight, and laws and procedures enacted through the democratic process. In addition, and relevant to the concerns of foreign countries about their nationals' data, a recent ruling by a United States appeals court one level below the Supreme Court confirmed that statutory protections are extended to *non-United States citizens* for data physically maintained in the United States and stored in the Cloud.[9]

3. AUSTRALIA

The Australian government may require a Cloud service provider to disclose customer data in the course of a governmental authority's investigation by requesting that a judge issue a **search warrant** if there are reasonable grounds for suspecting that there is evidential material relevant to an indictable or summary offense.

A Cloud service provider is permitted to voluntarily provide customer data to the government without a search warrant if the data does not constitute "personal information," which is broadly defined as information or an opinion about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion. However, a Cloud service provider can voluntarily disclose personal information to the Australian government if it reasonably believes that the use or disclosure is reasonably necessary to, among other similar reasons, prevent, detect, investigate, prosecute, or punish violations of law or serious breaches of standards of conduct, including corruption, abuse of power, dereliction of duty, or "any other seriously reprehensible behaviour." There is no general requirement that a Cloud service provider must notify its customers prior to disclosing their data to the government.

Requests for data issued to Australian companies and organizations extend to data held in Cloud servers located outside of Australia, provided that the suspected criminal offense or security matter that is the subject of the warrant occurred wholly or partly in Australia or concerns persons who are Australian citizens or residents. Therefore, the Australian government can require a Cloud service provider to obtain data from both domestic and foreign servers through the preceding legal mechanisms.

[9] *Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726 (9th Cir. 2011).

Australia

A Cloud service provider can voluntarily disclose personal information to the Australian government if it reasonably believes that the use or disclosure is reasonably necessary to, among other similar reasons, prevent, detect, investigate, prosecute, or punish violations of law or serious breaches of standards of conduct, including corruption, abuse of power, dereliction of duty, or "any other seriously reprehensible behaviour."

There are special access mechanisms for requests for Cloud data pertaining to terrorism or counterintelligence investigations. The government may require the production of customer data through a **computer access warrant**, which authorizes the Australian Security Intelligence Organisation ("**ASIO**") to access data where there are reasonable grounds to believe that the data will substantially assist in the collection of intelligence in a matter that is important to national security. Computer access warrants are issued by a government Minister, not a judge. In conducting a search under a computer access warrant, ASIO is authorized, if necessary, to add, delete, or alter other data held in the target computer. For the investigation of a serious terrorism offense, the Australian Federal Police can request a judge to issue a **production notice** permitting the government to access customer data where the data are relevant to, and will assist in, the investigation. Recipients of these notices are under strict obligations of confidentiality.

The government may intercept electronic communications for the purposes of national security and the investigation of serious crimes, provided that it first obtains an **interception warrant**. The Attorney General may issue interception warrants for the purpose of national security if the subject of the intercepted communication is "reasonably suspected of engaging in activities prejudicial to security," and the interception will assist the government in obtaining intelligence relevant to national security. Eligible judges or nominated members of the Administrative Appeals Tribunal may issue interception warrants for law enforcement purposes if the information to be obtained by intercepting a communication would likely assist in the investigation of a serious crime.

4. CANADA

Canadian governmental authorities can obtain **search warrants** through which a judge can order the search and seizure of evidence located on a Cloud computing server where there are reasonable and probable grounds to believe that a criminal offense has been committed, and that the search will yield evidence of that criminal offense. In addition, Canadian governmental authorities can seek **production orders** to compel Cloud service providers to

produce specific evidence where there are reasonable grounds to believe that an offense has been or will be committed. Both search warrants and production orders must be authorized by a judge. Some federal and provincial regulatory agencies have the power to issue **administrative orders** requiring the production of records necessary to an investigation. In some cases, administrative agencies are required to obtain a production order or search warrant from a judge.

A Cloud service provider is permitted to voluntarily provide customer data to a government official requesting such production without a search warrant, or other formal mechanism, unless the disclosure contains personal information and it is not requested pursuant to lawful authority under Canadian privacy laws. There is no general requirement that a Cloud service provider must notify its customers prior to disclosing their data to the government. Canadian requests for data are not limited to data located in Canada. Generally, a company subject to Canadian jurisdiction must turn over any relevant data over which it has "custody or control," either because it can access the data itself or because it can cause a third party, such as a subsidiary corporation, to access or obtain the data. Therefore, the Canadian government can require a Cloud service provider to obtain data from both domestic and foreign servers through the preceding legal mechanisms.

Canada

A company subject to Canadian jurisdiction must turn over any relevant data over which it has "custody or control," either because it can access the data itself or because it can cause a third party, such as a subsidiary corporation, to access or obtain the data.

In addition to the preceding legal mechanisms, Canada's **2001 Anti-Terrorism Act** implemented a number of investigative powers similar to those found in the United States' Patriot Act. In addition, the Canadian Security Intelligence Service can obtain an **investigation warrant** to obtain data relating to a threat to the national security of Canada by arguing to a judge that other investigative procedures have been tried and have failed and that the matter is an urgent national security matter.

Generally, prior judicial authorization is required before the government can conduct electronic surveillance. However, without judicial authorization, the government can intercept communications of foreign entities for the purpose of obtaining foreign intelligence or for the protection of the government's computer systems and networks, provided that prior approval is obtained from the Minister of National Defense. In addition, the Canadian Criminal Code allows a peace officer to intercept electronic communications if: (1) the urgency of the situation is such that a proper authorization could not be obtained; (2) the interception is immediately necessary to prevent an unlawful act that would cause serious harm to a person or property; and (3) either the originator or the intended recipient of the communication is the one who is likely to cause the harm or the one who is likely to be harmed.

Canada currently is considering an expansive new law to increase the government's ability to obtain data from private entities. On February 14, 2012, Bill C-30 was introduced in Canada's House of Commons. This bill would significantly expand the Canadian government's investigative powers, especially with respect to electronic communications and storage. Some of Bill C-30's proposed provisions are as follows:

- Canadian governmental authorities would be able to issue orders that require Cloud service providers to preserve data without prior authorization by a judge.

- Telecommunications providers (including ISPs) would be required to install the technological capability to provide surveillance data, when ordered to do so by the Minister of Public Safety and Emergency Preparedness, and would be prohibited from disclosing the existence of the surveillance. No judicial oversight would be required.

- The Canadian government would be able to obtain a warrant for the installation of a transmission data recorder which would record all communications to or from a server. (Currently, warrants only can be obtained to intercept telephone calls and to install a telephone number recorder.)

The introduction of Bill C-30 was met with criticism from a number of stakeholders, including the Office of the Privacy Commissioner and civil rights groups, and it is unclear if, and to what extent, the bill is likely to be revised before it might be passed into law.

5. DENMARK

Under the law in Denmark, government officials can request that a judge issue a **search warrant** to obtain customer data from a third-party Cloud server if there are specific reasons to presume that evidence of an offense can be obtained during the search. Various government agencies in Denmark also have the authority to issue **administrative orders** to obtain data from Cloud service providers if related to the investigation of an offense over which the government agency has jurisdiction.

Cloud service providers can voluntarily provide the government with data stored on Cloud servers, provided

that disclosing the data does not violate other laws, such as laws prohibiting disclosure of personal data without a valid reason. Providing data to law enforcement pursuant to a police investigation on a voluntary basis is considered a valid reason. There is no general requirement that a Cloud service provider must notify its customers prior to disclosing their data to the government.

While Denmark has adopted anti-terrorism laws, these laws do not alter the government's ability to access Cloud data in terrorism investigations. Due to the serious nature of such investigations, however, it is likely that a judge would be more willing to grant a search warrant.

If a Danish Cloud service provider stores customer data on servers located in another country, the government can access data located on those servers with a search warrant, provided that the data can be reached and searched from the site of the Denmark-based provider. Otherwise, the extent to which the Danish government may access data on servers located in other countries depends on the level of judicial cooperation between the concerned countries.

Denmark

Under the law in Denmark, government officials can request that a judge issue a search warrant to obtain customer data from a third-party Cloud server if there are specific reasons to presume that evidence of an offense can be obtained during the search.

The government must obtain a court-issued warrant before intercepting electronic communications. The court will issue the warrant only if the interception is related to a government investigation that concerns an offense of a certain seriousness (including terrorism). In certain limited situations, the government may intercept communications without prior court approval where exigent circumstances dictate that the interception would be ineffective if a court order were first to be obtained.

6. FRANCE

French government officials can request access to an organization's data stored on the servers of a third-party Cloud computing service in a number of situations, including for criminal and administrative investigations. In general, the government can obtain a **search warrant** issued by a judge or issue a **requisition letter** directly to a third-party Cloud service provider, both of which would require that the Cloud service provider produce customer data relating to a criminal investigation.

No law expressly prohibits a Cloud service provider from voluntarily providing a customer's information to the government, with certain exceptions such as the provision of personal or telecommunications data. There also is no general requirement that a Cloud service provider must notify its customers prior to disclosing their data to the government; in fact, a Cloud service provider is not entitled to disclose a government request for information to its customer.

France

French government officials can request access to an organization's data stored on the servers of a third-party Cloud computing service in a number of situations, including for criminal and administrative investigations.

French law expressly permits governmental authorities to obtain all information relevant to an investigation from a computer system so long as the data are accessible from that computer system. Therefore, the French government can require a Cloud service provider to obtain data from both domestic and foreign servers through the preceding legal mechanisms.

Other than the hours during which searches can be conducted during an investigation involving national security, organized crime, or terrorism, the obligations imposed on government officials requesting access to data stored in the Cloud remain unchanged.

In criminal investigations, a judge may order the interception, recording, and transcription of electronic communications where the requirements of the investigation call for it. For investigations into terrorism, national security, and other serious crimes, governmental authorities are provided with expanded electronic surveillance capabilities, and a court may authorize the interception and recording of electronic communications during even the preliminary stage of an investigation if justified by the needs of the investigation. For so-called "security interceptions," no court order is required. Providers of encryption services are also required to hand over encryption keys to government officials under certain conditions. As noted above, France's anti-terrorism laws have been characterized by some as tougher than the Patriot Act.[10]

France also has extended data retention obligations to hosting providers, who are required under French law to keep log data and data relating to the identity of persons who have posted material on social networking services, for example.

[10] *Fighting Terrorism, French-Style*, *supra* note 2.

7. GERMANY

Under German law, criminal prosecutors and certain regulatory agencies may request a **court order** to obtain access to an organization's data stored on the servers of a third-party Cloud computing service. To obtain such an order, the government must demonstrate to a judge that there exists a sufficient reason to believe that the data contains evidence relevant to a criminal offense.

In addition, under the **Telecommunications Act**, German prosecutors have a right to request certain non-content data (e.g., telephone numbers, addresses, birth dates) stored by telecommunications service providers to the extent necessary to prosecute violations of law, to avert danger to public safety or order, or to discharge legal functions of the government. This customer data must be disclosed to the government by the telecommunications provider upon request, with no prior court order. A Cloud service provider would be considered a telecommunications service provider to the extent it provides certain communications services to third parties (such as instant messaging, web conferencing, or email services). These required disclosures come with a "gag order" provision that prohibits the telecommunications service provider from disclosing to third parties, including its customers, the fact that it received the request.

Moreover, German data protection authorities may request information regarding data stored on the servers of a Cloud service provider to verify compliance with the **Data Protection Act** and are granted the right to request access to a Cloud service provider's servers to conduct audits (to the extent necessary to verify compliance with German data protection law).

In certain circumstances, a Cloud service provider may not voluntarily disclose customer data to government authorities. For example, where a Cloud service provider is considered a telecommunications service provider under the Telecommunications Act, disclosure of any customer content data to the government without explicit statutory permission would be a breach of the Cloud service provider's obligation to maintain the secrecy of telecommunications. In addition, Cloud service providers cannot disclose personal data without explicit statutory permission, such as through the Telecommunications Act or Data Protection Act. Otherwise, there do not appear to be any specific laws expressly prohibiting the disclosure of customer data.

In general, the target of a government search – including a customer of a Cloud service provider – must be informed by the government about the search. This notice must take place as soon as it can be effected without endangering the purpose of the investigation. However, as noted below, for investigations into serious criminal offenses, national security, or terrorism, the Federal Office of Criminal Investigation (BKA) may, in some instances, conduct a search or monitor ongoing telecommunications without providing notice to the target or to other affected persons.

In principle, a court order for a search at a Germany-based Cloud service provider may not be extended to a search of the provider's services located abroad, even though technically such servers may be accessible through the provider's computing equipment. Therefore, to request data located on the servers of a German Cloud service provider that are located outside of Germany, the German government would need to request assistance from governmental authorities in the country in which the servers are located. A request for customer data under the Telecommunications Act or Data Protection Act, on the other hand, might encompass servers located abroad, although the law is unclear on this.

The above rules also apply to investigations involving national security or terrorism. However, given the weight of the criminal offenses in these cases, the courts may grant the government more leeway when determining whether to permit a search for these types of investigations. In addition, the BKA may, in investigations concerning serious criminal offenses, national security, or terrorism, use a "Federal Trojan" (a government-issued computer virus) to search a Cloud provider's servers, monitor ongoing communications, or collect communication traffic data without the knowledge of the target. The government can use a Federal Trojan if a serious danger exists, such as a risk to a person's life, the security of the state, terrorism, or important interests of the general public. The BKA also may request that a Cloud provider produce information because it is a telemedia service provider. Other federal intelligence services also are authorized to request information stored by a "service provider of teleservices or telecommunications," but the request must be ordered by the responsible Federal Ministry, the Federal Chancellery, or the Federal State Authority.

The German government may apply for a court order allowing for the interception and recording of electronic communications without the knowledge of the subject of the surveillance if there is evidence that the subject committed a serious offense, the offense is "of particular gravity in the individual case," and other means of establishing the facts would be much more difficult. In addition, in exigent circumstances the prosecutor's office may issue such an order, but its continued validity is contingent upon subsequent confirmation by the court. In the event that an order has been issued or confirmed by the court, the government is not required to notify the subject of the surveillance until notice can be effected without endangering the purpose of the investigation. Finally, the G10 Act provides German intelligence services with the authority to monitor and record telecommunications in the

investigation of a serious crime or a threat against national security, such as terrorism. The intelligence service is not required to obtain a court order. Rather, the surveillance must be ordered by the responsible Federal Ministry or Federal State Authority.

Germany

For investigations into serious criminal offenses, national security, or terrorism, the Federal Office of Criminal Investigation (BKA) may, in some instances, conduct a search or monitor ongoing telecommunications without providing notice to the target or to other affected persons.

8. IRELAND

The Irish government may require a Cloud service provider to disclose customer data through a **search warrant**, which a judge may issue if there are reasonable grounds to suspect that the data contain evidence relating to an arrestable offense. A Cloud service provider that constitutes an "electronic communications service" is required to retain certain non-content data resulting from the use of its service for one year. Irish government authorities can issue a **disclosure request** to access this data if required to detect, investigate, or prosecute a serious offense (carrying a maximum sentence of greater than five years) or a tax offense, for national security purposes, or to save human life. There is comparatively limited judicial oversight of disclosure requests; a High Court judge is nominated to ascertain whether the government is complying with the law and issue a report on this to the Irish Prime Minister.

No law expressly prohibits Cloud service providers from voluntarily providing customer data in response to a government request. However, if that customer data contains personal data, disclosing it to the government could violate Irish data protection law if the disclosure is not authorized by law. There is no general requirement that a Cloud service provider must notify its customers prior to disclosing their data to the government.

As with the rule in the United States, so long as there is an entity in Ireland over which the Irish government can assert jurisdiction, Irish authorities can require the entity to produce customer data from a Cloud server located in another country but under the entity's control. Therefore, the Irish government can require a Cloud service provider to obtain data from both domestic and foreign servers through the preceding legal mechanisms.

Irish law allows for disclosure requests to be made on broad national security grounds, even where not directly connected to a criminal investigation. Furthermore, the Irish courts may be more permissive of government requests in the context of national security investigations.

Ireland

As with the rule in the United States, so long as there is an entity in Ireland over which the Irish government can assert jurisdiction, Irish authorities can require the entity to produce customer data from a Cloud server located in another country but under the entity's control.

Under Irish law, the Minister for Justice may authorize the interception of electronic communications where necessary for national security or in furtherance of a criminal investigation. A wiretap can only be used for the investigation of a serious offense if investigations not involving interception will fail to produce the relevant evidence in a timely manner and there is a reasonable prospect that the intercepted evidence would be of material assistance. Once a Ministerial authorization has been provided, there appear to be few limitations on the ability of government to access the information.

9. JAPAN

In Japan, government officials can request and obtain access to an organization's data stored on the servers of a third-party Cloud computing service through the use of **search warrants** issued by a judge where it is reasonably supposed that the servers contain data relevant to a suspected crime. Japanese civil courts and the Japanese legislature can order third parties to produce data as well, which could extend to data residing on Cloud servers located in Japan.

Japanese law generally prohibits Cloud service providers from voluntarily disclosing to governmental authorities customer communications, non-content customer data, personal information, and telecommunications logs without a search warrant or statutory authorization. There is no general requirement, however, that a Cloud service provider must notify its customers prior to disclosing their data to the Japanese government pursuant to a search warrant.

Japan

There is no general requirement that a Cloud service provider must notify its customers prior to disclosing their data to the Japanese government pursuant to a search warrant.

The ability of Japanese officials to access Cloud data depends on the location of the server storing the data. If

the server is located in Japan, the data are accessible through a search warrant. If the data reside on a server located outside of Japan, government officials must rely on cooperation with government authorities in other countries to assist in obtaining the data.[11]

There are no special rules regarding government access to Cloud data during the course of national security or terrorism investigations.

Under Japanese law, the government may intercept electronic communications in connection with an investigation of serious crimes. However, the government can only resort to wiretapping if there is no other way to obtain the evidence, and in such cases it must first obtain a court-issued warrant. Only prosecutors and police officers the rank of superintendent and above may seek a warrant authorizing the interception of electronic communications.

10. SPAIN

Under Spanish laws, government authorities are entitled to request and obtain access to data considered necessary for a government investigation. The procedures followed by different authorities vary. Generally speaking, government authorities are not required to obtain a court warrant issued by a judge to enter the premises of an investigated entity. However, these powers are limited by the constitutional **inviolability of domicile** principle, which prohibits the government from executing a search without consent or a court warrant at the "registered office" of a company – usually the location of the company's legal representation or where its main activities are carried out – unless there is a "flagrant" criminal offense (i.e., the criminal is caught in the act of committing the offense).

Spain

Under Spanish laws, government authorities are entitled to request and obtain access to data considered necessary for a government investigation.

It would be lawful for a Cloud service provider to voluntarily provide customer service data to a government official at the official's request, except for investigations of the Cloud service provider's registered office or where otherwise prohibited by a specific law, such as data protection law. There is no general requirement that a Cloud service provider must notify its customers prior to disclosing their data to the government.

When an entity is subject to Spanish laws, government authorities are entitled to investigate its conduct and request and access data wherever it is stored. Therefore, the Spanish government can require a Cloud service provider to obtain data from both domestic and foreign servers through the preceding legal mechanisms.

Where there is an exceptional or urgent need in the case of terrorism or organized crime, the police are allowed to enter and search the premises of a company without the need for a court warrant or the owner's consent, including Cloud servers.

Generally, the government must obtain a court-issued warrant in order to intercept electronic communications. Such warrants must be founded on sufficient evidence that the intercepted communication would be material to a criminal investigation, and the process is subject to judicial oversight. In certain limited instances, the government may perform electronic surveillance without first obtaining a court-issued warrant.

11. UNITED KINGDOM

The United Kingdom ("UK") government may require a Cloud service provider to disclose customer data in the course of a government investigation through a number of legal mechanisms. The government can request that a judge issue a **search and seizure warrant**, which the court will grant if the government can demonstrate that there exist reasonable grounds to believe that a criminal offense (other than a minor criminal offense) has been committed and the data are likely to be of substantial value to an ongoing criminal investigation.

British governmental authorities also can obtain a **disclosure order** for communications data – i.e., certain non-content data such as traffic, usage, and customer data about users of a telecommunications service – if necessary for national security; to prevent or detect crime or disorder; to ensure the economic well-being of the UK; to ensure public safety; to protect public health; to assess or collect any tax or any charge payable to the government; or to prevent or mitigate death or injury to a person. These orders must be proportionate for the purposes for which they are sought, particularly with reference to the rights of third parties who are not being investigated. A Cloud service provider would most likely be considered a "telecommunications service" if it provides Cloud-based communications services (e.g., instant messaging, web conferencing, or email services). In cases where the government believes that the investigation might be

[11] Under a recently revised criminal procedure law, Japanese law enforcement officials may obtain copies of data located on a remote server if a computer in Japan is able to create, change, or delete data on the server, even if the server is located outside of Japan. Although computers of Cloud providers may be able to change or delete customer data, the Japanese Ministry of Justice currently takes the position that computers of Cloud providers are not subject to the law. It is not certain, however, whether Japanese courts would read this same limitation into the law.

compromised by requesting that the Cloud service provider collect the data itself, it may apply for an authorization to obtain the communications data directly, which could involve wiretapping, hacking, or even a physical dawn-raid. These measures, however, likely only would be used in extreme circumstances.

United Kingdom

The government may intercept communications if doing so is "necessary" in the interests of national security; for the prevention or detection of a serious crime; to safeguard the economic well-being of the UK; or in response to a request under an international mutual legal assistance agreement. There is no need for court approval and the details of such an "interception warrant" must be kept secret.

No law expressly prohibits a Cloud service provider from voluntarily transmitting customer data in response to a government request, although if personal data are involved, any disclosure would need to comply with data protection law. There is no general requirement that a Cloud service provider must notify its customers prior to disclosing their data to the government. In fact, notification may even be prohibited or risky in certain circumstances, such as when notification would compromise an investigation.

Where British governmental authorities have a warrant or order to obtain electronic data, they have the power to require the search of any information contained in the computer and accessible from the premises. In other words, as long as foreign Cloud servers can be accessed from premises in the UK, the police could require the Cloud service provider to also turn over data located on the foreign servers.

Under the Intelligence Services Act, British Secretaries of State have broad powers to issue warrants for the British Security Service, the Intelligence Service, or the Government Communications Headquarters to enter into property and seize any data that may be required. Where there are terrorism or national security threats, these agencies would be far more likely to exercise their powers under these laws.

The government may intercept communications if doing so is "necessary" in the interests of national security; for the prevention or detection of a serious crime; to safeguard the economic well-being of the UK; or in response to a request under an international mutual legal assistance agreement. However, the government actor must first apply to the Secretary of State for an "interception warrant." There is no need for court approval and the details of an "interception warrant" must be kept secret. In addition, as noted above, governmental authorities can apply for an authorization to directly obtain "communications data" by use of a wiretap, but it is likely that such measures would be used sparingly.

12. EUROPEAN UNION LEGAL REFORM

In January 2012, the European Commission proposed a new Regulation and new Directive concerning the privacy of personal data. The Regulation would apply to commercial collection and use of personal data and generally is viewed as increasing protections for personal data. However, the Directive – which is directed at law enforcement access to personal data – is generally viewed as providing law enforcement with continued substantial access to personal data. Concerning the law enforcement data access Directive, the European Data Protection Supervisor, Peter Hustinx, has said:

> The proposed rules for data protection in the law enforcement area are unacceptably weak. In many instances there is no justification whatsoever for departing from the rules provided in the proposed Regulation. The law enforcement area requires some specific rules, but not a general lowering of the level of data protection.[12]

The European Data Protection Supervisor is concerned in particular with legal uncertainty about further use of personal data by law enforcement authorities, the fact there is no requirement for law enforcement authorities to demonstrate compliance with data protection requirements, the low standards for transfers of personal data to other countries, and the limited powers of data protection supervisory authorities. In short, the proposals for reform of privacy rules in the EU do not contemplate altering the current environment in which law enforcement has significant access to data in the Cloud.

European Union

Proposals for reform of privacy rules in the EU do not contemplate altering the current environment in which law enforcement has significant access to data in the Cloud.

[12] Press Release, European Data Protection Supervisor, *EDPS applauds strengthening of the right to data protection in Europe, but still regrets the lack of comprehensiveness*, EDPS/12/7, March 7, 2012, *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/12/7&format=HTML&aged=0&language=EN&guiLanguage=en.

Graphical Illustration

The chart that follows graphically illustrates the descriptions set forth above concerning governmental access to data in the Cloud, by jurisdiction.

GOVERNMENTAL AUTHORITIES' ACCESS TO DATA IN THE CLOUD: A COMPARISON

	May government require a Cloud provider to disclose customer data in the course of a government investigation?	May a Cloud provider voluntarily disclose customer data to the government in response to an informal request?	If a Cloud provider must disclose customer data to the government, must the customer be notified?	May government monitor electronic communications sent through the systems of a Cloud provider?	Are government orders to disclose customer data subject to review by a judge?*	If a Cloud provider stores data on servers in another country, can the government require the Cloud provider to access and disclose the data?
Australia	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
Canada	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
Denmark	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
France	Yes	Yes, except for personal data without a legal purpose, electronic communications	No	Yes	Yes	Yes
Germany	Yes	Yes, except for personal data without a legal purpose, electronic communications	Yes, except may withhold until disclosure no longer would compromise the investigation or in investigation of serious criminal offenses, national security, or terrorism	Yes	Yes	No, not without cooperation from the other country's government, except for telecommunications customer non-content data
Ireland	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
Japan	Yes	No – must request data through legal process	No	Yes	Yes	No, not without cooperation from the other country's government**
Spain	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
United Kingdom	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
United States	Yes	No – must request data through legal process	Yes, for content data, except when the government obtains a search warrant or unless disclosure would compromise the investigation	Yes	Yes	Yes

* "Review by a judge" encompasses either an initial review when issuing the court order, warrant, etc. or subsequent review when the court order, warrant, etc. is challenged by the service provider or customer.

** Under a recently revised criminal procedure law, Japanese law enforcement officials may obtain copies of data located on a remote server if a computer in Japan is able to create, change, or delete data on the server, even if the server is located outside of Japan. Although computers of Cloud providers may be able to change or delete customer data, the Japanese Ministry of Justice currently takes the position that computers of Cloud providers are not subject to the law. It is not certain, however, whether Japanese courts would read this same limitation into the law.