Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the European Union and the United States

Cloud computing is one of the Internet's great innovations, enabling individuals and small and medium size enterprises to enjoy state-of-the-art data processing services that until very recently were available only to large businesses. Cloud computing is now key to the functioning of smart phones, tablets, and the other wireless devices with which most people access the Internet. Consequently, cloud computing allows users to access cloud services from locations around the world irrespective of national borders. The ability of cloud consumers to exploit the full value of this innovation has been increasingly threatened over the last year by misplaced assertions that use of cloud services provided by a company subject to the U.S. legal process will routinely expose customer data to seizure by U.S. law enforcement authorities. As this controversy jeopardizes opportunities on both sides of the Atlantic and around the world for needed economic and employment growth, the record needs to be set straight.

The transatlantic privacy discussion is too often based on myths about the U.S. legal system—myths that obscure our fundamental commitment to privacy and the extensive legal protections we provide to data. Contrary to concerns raised by some, electronic data stored in the United States—including data of foreign nationals—receives protections from access by criminal investigators equal to or greater than the protections provided within the European Union.

This document dispels these myths and discusses certain aspects of U.S. laws that are often mischaracterized abroad, and that discourage citizens of other countries from storing their data with U.S. cloud providers.

Myth 1: The United States Cares Less about Privacy than the European Union.

Reality: The United States was founded on—and its modern-day laws, regulations, and practices reflect—a core belief in the importance of protecting citizens from government intrusion. Our most important legal document—our Constitution—set forth, more than two hundred years ago, a Bill of Rights that provided protection from unreasonable searches and seizures, and that continues to protect privacy today, including the privacy of electronic communications. The United States and the European Union are united in our common values regarding the fundamental importance of privacy protections and our deeply rooted commitment to continue to safeguard these values in the digital age.

Myth 2: The European Union Does a Better Job of Protecting Data from Law Enforcement Access than the United States.

Reality: Privacy protections limiting U.S. law enforcement access to electronic communications, a key area of modern data privacy concern, are among the highest in the world. They provide protections that are at least equivalent to—and often superior to—those provided by the laws and practices in many EU Member States.

Myth 3: U.S. Law Enforcement Authorities Are Less Protective of the Privacy Interests of Foreign Nationals than of U.S. Citizens.

Reality: In the key area of law enforcement acquisition of electronic communications, the stringent U.S. statutes protecting the privacy of email and voice communications apply equally to foreign nationals and U.S. citizens. Moreover, the United States does not discriminate with regard to judicial redress to obtain access to personal data collected for criminal investigations, and provides opportunities for any person, regardless of citizenship, to correct such data if it is believed to be inaccurate, as explained below.

Myth 4: The Patriot Act Gives the U.S. Government Carte Blanche to Access Private Data Stored in the "Cloud" or Elsewhere.

Reality: The Patriot Act continues to be the subject of serious misinterpretation and mischaracterization. While portions of the Act updated existing investigative tools, the Patriot Act did not eliminate the pre-existing, highly protective restrictions on U.S. law enforcement access to electronic communications information in criminal investigations—restrictions that are, as noted above, no less stringent than those found within the EU.

Myth 5: The Advent of "Cloud Computing" Changes Everything.

Reality: Even before the "cloud" became a popular concept, data was stored remotely and U.S. laws anticipated the need to protect such data. As a result, U.S. law has carefully regulated law enforcement requests for remotely stored data and other records since long before even the Internet—for this is an issue that predates both the Internet and cloud computing.

* * *

1. Myth: The United States Cares Less about Privacy than the European Union.

Reality: The United States was founded on—and its laws reflect—a core belief in the importance of protecting citizens from government intrusion. Our most important legal document—our Constitution—established, more than two hundred years ago, a federal government with limited powers and extensive checks and balances. Our Bill of Rights ensures the freedom to speak, assemble, and worship freely. It also provides protection from self incrimination, as well as from unreasonable searches and seizures. Each of these constitutionally guaranteed civil liberties protects important aspects of a person's privacy.

The approach to privacy in many parts of the European Union has evolved more recently, and reflects a different set of legal traditions and historical developments—indeed, traditions and developments that vary even among Member States—so it is understandable that there are differences in our respective schemes. Nonetheless, our systems share many common principles, including the recognition in the International Covenant on Civil and Political Rights (ICCPR) that "[n]o one shall be subjected to arbitrary

or unlawful interference with his privacy, family, home or correspondence." The United States and the European Union are united in our common values regarding the fundamental importance of privacy protections and our deeply rooted commitment to continue to safeguard these values in the digital age.

2. Myth: The European Union Does a Better Job of Protecting Data from Law Enforcement Access than the United States.

Reality: As discussed below, the United States provides numerous protections from law enforcement access to electronic communications, a key area of modern data privacy concern. In addition, the United States has an extensive and highly effective system of layered oversight, including criminal prosecutions of government officials who access computer systems without authorization or for an unauthorized purpose. These protections match, and indeed in many instances exceed, protections available under EU law.

The United States Provides Broad Protections for the Privacy of Electronic Communications

The United States was a pioneer in safeguarding the privacy of telephone and email communications in criminal investigations. With very limited exceptions, law enforcement agents in the United States are prohibited from intercepting[1] the contents of voice and email communications in criminal investigations unless an independent judicial authority finds that stringent evidentiary and procedural requirements have been met. In particular, specific information must be presented to an independent judicial authority establishing probable cause to believe that specific named individuals are using or will use the targeted telephone or other device to commit specific identified offenses.

Law enforcement agents must also demonstrate the specific need for the proposed electronic surveillance and provide a detailed discussion of the other investigative procedures that have been tried and failed, are reasonably unlikely to succeed if tried, or are too dangerous to employ. This is to ensure that such intrusive techniques are not resorted to in situations where traditional investigative techniques would suffice to expose the crime.

U.S. law also ensures that such authority is used only as long as necessary. For example, if an interception request is ultimately approved, criminal investigators are only permitted to intercept the subject communications for a maximum of 30 days, unless the time period is specifically extended by a court. In addition, throughout the limited period of interception, the investigators must actively minimize the interception of all non-pertinent communications.

[1] In this context, "intercepting" means listening to, reading or recording the contents of private communications in real time, commonly referred to as a "wiretap." The limited exceptions to this prohibition include, for example, emergencies involving an immediate danger of death or serious physical injury. *See* 18 USC § 2518(7).

These standards for conducting criminal investigations are among the highest in the world. The laws and practices in EU Member States are often far more permissive than in the United States when it comes to accessing the contents of telephone and email communications. For instance, not all EU Member States require independent court orders to authorize the interception of voice or email communications, and many Member States authorize interception if the communications are "relevant," a lower standard than probable cause and all the other U.S. requirements. Indeed, publicly available figures indicate a heavier reliance by EU law enforcement authorities on electronic surveillance to intercept the contents of private voice and email communications by several EU Member States, including Italy, Germany, France, and the Netherlands, than by the United States. When relative population sizes are taken into account, the disparity in the use of electronic surveillance by the United States and EU Member States becomes even more apparent.

The United States also is a world leader in protecting the privacy of stored email communications sought in criminal investigations. Before the contents of stored email communications can be divulged, U.S. law enforcement authorities must, at a minimum, obtain a court order or grand jury subpoena. In most cases, however, U.S. authorities obtain a search warrant from an independent judicial authority authorizing the seizure. To obtain such a warrant, the agents must present specific evidence establishing probable cause to believe that the particular email account will contain evidence of the crime under investigation (and not just that the account is under the control of a suspected criminal). This is essentially the same standard used when a U.S. judge decides whether to authorize the search of someone's home. Moreover, if a warrant is constitutionally required, defects in applying for one, or failure to obtain one, may result in a ban on the prosecution's use of the evidence, no matter how incriminating it is. (This is known as the "exclusionary rule" under U.S. constitutional law.) The United States is not aware of any other country in the world that employs a more stringent evidentiary standard in this context.

The exacting nature of these U.S. privacy protections has been evident in cases where European law enforcement authorities have requested U.S. assistance in obtaining stored email correspondence from U.S.-based Internet service providers, and have shared with the U.S. government how onerous they find the U.S. legal requirements in comparison to their own domestic legal standards.

Significantly, law enforcement officials in the United States may be prosecuted criminally or sued for money damages civilly if they illegally intercept voice or email communications. U.S. service providers are also barred from voluntarily providing traffic or subscriber data or the content of stored email communications to U.S. government agents in response to informal requests (*i.e.*, requests not accompanied by a formal legal order directing production of the data), except in very limited circumstances.[2] U.S. providers that violate

[2] For example, electronic communication service providers are permitted to voluntarily disclose the contents of communications to a government entity if the provider believes in good faith that an emergency involving danger of death or serious physical injury requires disclosure without delay of information related to the

this ban are subject to civil suit and penalties. In a recent comparative survey of global practices, the United States and Japan were determined to be the only two countries studied that prohibited service providers from voluntarily disclosing customer data to their governments in response to informal requests (except in those limited cases).[3] The other countries in the study included Denmark, France, Germany, Spain, and the United Kingdom.

The United States Has Adopted an Extensive Regime of Layered Oversight of Privacy Protections

Privacy protection in the United States is ensured not only by these strict legal standards for gathering evidence but also by a layered system of oversight and enforcement of privacy protections, including criminal prosecutions.

Pursuant to EU laws, Member States are required to establish public data protection authorities with "complete independence" in the exercise of the functions entrusted to them. The absence of such data protection authorities in the United States is sometimes cited as evidence that the European Union does a better job of protecting privacy. However, the model adopted within the European Union is not the only, or necessarily the optimal, legal structure for ensuring independent and effective oversight. Even the European Commission has observed in recent proposed legislation that Member State data protection authorities, notwithstanding their "complete independence," have been "unable to ensure consistent and effective application of the [EU data protection] rules."[4] In contrast, the multilayered privacy protection system long adopted in the United States has proven to be robust and effective.

One of the keys to the success of the U.S. system is that the extensive system of checks and balances between the powers exercised by the different branches of our government (executive, legislative, and judicial) mandated by our Constitution ensures that none of these branches acts in "complete independence" from the others. Strong protections in specific legislation and the check of judicial authority establish bulwarks for the protection of data. Rather than a weakness in the protection of privacy, these rigorous checks and balances in the U.S. system of government are enduring strengths.

Moreover, within the executive branch itself, there is a multi-layered system of oversight authorities, which includes Chief Privacy Officers in federal agencies specifically charged to ensure compliance with applicable privacy laws and regulations. In addition, there are more than 70 Inspectors General, many of whose appointments are subject to congressional confirmation, assigned to various U.S. government agencies. These Inspectors General separately conduct, coordinate, and supervise audits and investigations

---

emergency. *See* 18 U.S.C. Section 2702(b)(8). "Service provider" as used in this paper refers to providers covered by 18 U.S.C. Section 2701 et seq.

[3] Winston Maxwell and Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud*, A Hogan Lovells White Paper (May 23, 2012), pp. 2-3, 13.

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century*, European Commission, (Brussels, 25.1.2012), at p. 4.

of their respective agencies, including on data protection and privacy issues. Federal law provides that agency heads may not prevent an Inspector General from initiating or carrying out an investigation and often requires Inspectors General to report the results of their reviews to Congress.

Pursuant to our constitutional framework, the legislative branch also plays an important oversight role in ensuring compliance with privacy laws and regulations. The Government Accountability Office—an agency within the legislative branch—regularly investigates executive branch agencies, including compliance with privacy and data protection laws and policies. In addition, numerous congressional committees have an oversight role with respect to the executive branch, including privacy and data protection issues. These congressional committees have regularly conducted hearings on privacy-related issues, including the Patriot Act.

In addition to administrative and congressional oversight and enforcement, the United States has a strong and documented record of criminal prosecutions of government officials for unauthorized access to data or access for an unauthorized purpose, with prison sentences possible in the most serious cases. We are not aware of any similar record of prosecutions elsewhere in the world.

Finally, the judicial branch also acts as a check on both the executive branch and the legislative branch. The stringent oversight that the judicial branch exercises over the executive branch and its investigative techniques regarding electronic communications, as discussed above, is another example of the checks and balances inherent in the U.S. system.

3. Myth: U.S. Law Enforcement Authorities Are Less Protective of the Privacy Interests of Foreign Nationals than of U.S. Citizens.

Reality: This myth rests on a misunderstanding of U.S. law—with regard to both protections and remedies. First, in the key area of electronic communications, the stringent statutes protecting the privacy of email and voice communications in criminal investigations, discussed above, apply equally to foreign nationals and U.S. citizens. Second, the United States does not discriminate between U.S. citizens and foreign nationals with regard to judicial redress to obtain access to personal data collected for criminal investigations, and provides opportunities for any person, regardless of citizenship, to correct such data if it is believed to be inaccurate.
There are several U.S. laws that specifically provide judicial redress options for individuals who suffer damages pertaining to data protection and privacy violations, including in the context of law enforcement operations. These include the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, the Federal Tort Claims Act, and the Mandatory Victims Restitution Act. The judicial redress options under these laws are equally available to foreign nationals and U.S. citizens.

In the United States, the Privacy Act of 1974 allows individuals to access and correct information that federal government agencies have obtained about them and it provides for judicial redress to enforce those rights. The fact that the Privacy Act applies only to U.S.

citizens and aliens who are lawful permanent residents of the United States is sometimes mistakenly cited as evidence that U.S. law gives preferential treatment to U.S. citizens in this regard. However, law enforcement records collected for criminal investigations are regularly exempted from these provisions of the Privacy Act, in a manner similar to analogous exemptions in EU data protection laws. Consequently, foreign nationals and U.S. citizens are on equal footing with regard to access and correction of exempt criminal law enforcement records under the Privacy Act.

Notwithstanding these exemptions, foreign nationals and U.S. citizens alike can invoke other administrative processes to correct their law enforcement investigation data. For instance, anyone, regardless of citizenship, may seek review of the accuracy of data maintained by the applicable Department component. If an individual is dissatisfied with the component's response, the individual may appeal to the Justice Department's Office of Privacy and Civil Liberties, which will review the component's determination as a matter of administrative discretion. If he or she is still dissatisfied, the Department may permit the individual to file a statement of disagreement regarding the accuracy of the information and request that it be included in the file. In addition to the procedures for correcting criminal investigative files, Department regulations allow any person regardless of citizenship to request access to his or her own criminal history data in FBI files and request correction of any errors.

Finally, the Freedom of Information Act gives any person, regardless of citizenship, the right to request access to records and information that a federal agency maintains about him or her. All agencies of the U.S. executive branch are required to disclose records upon receiving a written request, absent an applicable exemption. Anyone, regardless of citizenship, can go to court to enforce this requirement.

4. Myth: The Patriot Act Gives the U.S. Government Carte Blanche to Access Private Data Stored in the "Cloud" or Elsewhere.

Reality: The Patriot Act has been the subject of serious misinterpretation and mischaracterization. The portions of the Act relevant here updated existing investigative tools in order to make investigations of terrorism and other national security threats more efficient and effective, while retaining important protections for privacy and civil liberties. The Patriot Act maintained highly protective restrictions on U.S. law enforcement access to electronic communications information.

Moreover, U.S. law, including revisions concerning investigative authorities implemented by the Patriot Act, does not go as far as the expansive authorities granted to law enforcement authorities in a number of EU Member States to collect data stored in the cloud and elsewhere. For example, in some Member States, government officials are authorized to issue warrants for the interception of content (wiretaps) without any independent court approval, and in the case of one Member State, whenever determined necessary for national security, prevention and detection of serious crime, or safeguarding the economic well-being of the country.

In addition, these authorities in the United States are available only in certain limited circumstances and are subject to important constraints. For example, under the authority to obtain "business records" that was amended by the Patriot Act, the government may obtain such records only if it first gets a court order, and only if the judge finds that the records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. The Attorney General approves guidelines that establish the circumstances under which a national security investigation may be opened. Finally, the recipient of such a business records order may challenge the legality of the order in court.

National Security Letters are another authority that was amended by the Patriot Act, and they also are the subject of significant misunderstanding. The authority to issue National Security Letters is available only where the records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. Furthermore, the law specifically limits the type of information that may be obtained with a National Security Letter. For example, National Security Letters may be issued to wire or electronic communications service providers only to obtain limited, non-content information (*e.g.*, names, addresses, length of service, and billing records). National Security Letters do not permit the government to obtain the content of communications. Although a National Security Letter may require that the recipient not disclose the National Security Letter to the subscriber or account holder, the provider that receives the letter may challenge that requirement in court.

In short, the Patriot Act did not fundamentally alter the protections U.S. law affords to communications information. Moreover, the United States is hardly exceptional with respect to establishing special procedures to govern national security investigations—the laws of most, if not all countries in Europe provide similar mechanisms to facilitate rapid access to information by government authorities under such circumstances.[5] International practice, no less than the language of the relevant laws themselves, has shown the U.S. legal framework provides a greater level of protection than the laws of many other countries.

5. Myth: The Advent of "Cloud Computing" Changes Everything.

Reality: "Cloud computing" may be a recently developed term, but, of course, data exists on physical servers. As has always been the case since the development of the Internet, data transmitted over the Internet is stored on a server located in a particular country or countries, and the rules establishing access to the data by U.S. law enforcement authorities have not changed. Moreover, even before the "cloud" became a popular concept, U.S. laws anticipated the need to protect data that was stored remotely. A part of the Electronic Communications Privacy Act, called the Stored Communications Act, contains specific provisions that protect data stored with remote computing services by establishing procedures for law enforcement to request and obtain such information from providers.

[5] Kromann Reumert, *Government Access to Data in 'the Cloud'* (March 11, 2012), at pp. 3-4; Maxwell and Wolf, *id.* at p. 1.

Beyond this, the United States also places stringent restrictions on the extra-territorial collection of data by law enforcement. The issue of when an entity present in a jurisdiction can be compelled to produce data that is in its possession or control—but which is stored in another jurisdiction—predates not only the "cloud," but computers themselves. As a result, the United States has restricted such law enforcement requests since long before the advent of cloud computing or the Internet—for this is an issue that predates both. Such requests are vetted at high levels within the U.S. Department of Justice and can be challenged in court.[6]

The U.S. approach is consistent with internationally agreed upon rules in this context. In 2001, the Council of Europe Cybercrime Convention, which the United States, Japan, and 34 European states have ratified, set out a legal framework for law enforcement and judicial access to computer data. The procedural law provisions of the Convention obligate each party to enact legislation enabling its authorities to search or similarly access a computer system in its territory in order to seize data stored therein. In addition, the Convention requires each party to enact legislation enabling its authorities to compel production, from any individual person or legal person (typically a corporation) in its territory, of computer data that is stored in a computer system or storage medium that is in the person's possession or control. The geographic scope of this rule is left to domestic law to define; countries may choose to limit it to data in the party's territory, but the Convention does not prohibit a party from applying it to data in the possession or control of a person within the party's territory even where the data itself is located outside the party's territory.

In this manner, the Cybercrime Convention establishes a regime for effective and swift international cooperation for law enforcement purposes, in recognition of the reality that both crime and computer data travel quickly across borders. Importantly, countries that are parties to the Convention are required to ensure that implementation and application of its rules, including production orders for data stored on remote servers, are subject to appropriate legal safeguards for the protection of human rights and liberties within their domestic legal systems. As a result of these and other provisions, the Cybercrime Convention has provided a secure and effective international framework for ensuring that electronic data is available to law enforcement authorities when needed for the investigation and prosecution of crimes, in a manner consistent with applicable international human rights commitments.

Moreover, a recent comparative survey of global practices determined that law enforcement authorities in all ten of the countries studied—including Denmark, France, Germany, Spain, and the United Kingdom, as well as the United States—have comparable legal authorities to obtain data from cloud servers located within their territory.[7] Significantly, however, and as noted above, the United States has an internal procedure severely restricting the exercise of this extra-territorial jurisdiction in any criminal case.

---

[6] *See* the US Attorneys' Manual, http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00279.htm.

[7] Maxwell and Wolf, *id*. at pp. 2-3, 13.

In contrast, EU Member States routinely seek and obtain direct access to data located in the United States, including data on U.S.-based cloud servers. In fact, in one case, Belgian authorities imposed criminal sanctions on a U.S.-based Internet company for refusing to disclose the personal data of certain e-mail users directly to a Belgian prosecutor. Although the case is proceeding, the Supreme Court of Belgium has held that Belgian law, specifically section 88ter of the Belgian Criminal Code of Procedure, permitted the prosecutor to unilaterally compel the production of such data, despite the fact that both the company and the data were located entirely outside of Belgium.

Given the extent to which personal communications and business transactions have moved online, it is not surprising that records of such activities have become increasingly relevant to law enforcement investigations of all types, ranging from money laundering to human trafficking to child pornography. However, the perception that the United States is somehow unique or more aggressive than EU counterparts in seeking access to such data for law enforcement purposes is inaccurate, as shown above. In sum, then, data stored in the United States is at least as protected from law enforcement access—and in many cases more protected—than data stored within the EU.