Canadian Journal of Law and Technology

Volume 13 | Number 2 Article 5

6-1-2015

International Law Enforcement Access to User Data: A Survival Guide and Call for Action

Kate Westmoreland

Gail Kent

International Law Enforcement Access to User Data: A Survival Guide and Call for Action

Kate Westmoreland[*] *and Gail Kent*[**]

Effectively accessing and using online evidence is a critical part of modern investigations and prosecutions, but also has significant implications for users' privacy. The current system of international sharing of online data in criminal matters is a patchwork of domestic and international law that is slow, uncertain, and not well understood. This article provides an overview of the current system for foreign governments seeking user data from US-based Internet companies. After describing the way in which the system currently operates, it identifies problems with the system, and outlines the reform efforts that are beginning to emerge.

INTRODUCTION

Effectively accessing and using online evidence is a critical part of modern investigations and prosecutions. At the same time, responsible criminal justice and the rule of law require that there be appropriate respect for users' human rights, including privacy. Ensuring that each of these imperatives is met is a difficult task, involving interactions between domestic and international laws, and cooperation between public and private sector actors, in an area where technological developments easily outpace legal change.

Internet companies and Internet providers collect and retain a variety of user information, depending on their product offerings and business models. This could include subscriber information such as name, address, credit card details, session logs, Internet protocol (IP) addresses, email content and metadata, geo-location data, and search queries. For law enforcement officers and prosecutors, this information can be a veritable treasure trove of investigative leads and evidence. For users, the sensitivity of this data ranges from the mundane to the highly personal and there are different expectations about how government access to each type of data should be controlled.

Governments from around the world now regularly seek emails, social media records, or documents stored in the cloud.[1] Accessing these records often

---

[*] Kate Westmoreland is a San Francisco-based international lawyer who works with government, startups, and civil society on data privacy and human rights. She is a non-residential fellow with the Stanford Center for Internet and Society.

[**] Gail now leads for Facebook on global law enforcement and surveillance policy, but at the time of writing worked for the UK's National Crime Agency. She is a non-resident fellow at Stanford Center for Internet and Society and an associate at Oxford University Martin School.

[1] The United States National Institute of Standards and Technology defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage,

involves multiple parties from multiple jurisdictions because the user, service provider, and law enforcement officer may each be in a different country.[2] Domestic and international laws and policies are struggling to cope with this complexity, with unfortunate consequences for both user rights and criminal justice. The current system for government access to data held by service providers is governed by voluntary agreements, law enforcement co-operation arrangements, or formal international legal agreements (including mutual legal agreement treaties and letters rogatory).

There has been an increasing number of calls to reform the system of sharing online records for criminal matters. The current system does not meet the needs of governments, providers, users, actual and potential victims of crime, or privacy advocates.

Governments acknowledge the current system's deficiencies. A survey by the United Nations Office on Drugs and Crime (UNODC) on cybercrime found that "[g]lobally, less than half of responding countries perceive their criminal and procedural law frameworks to be sufficient."[3] In the United States, the President's Review Group on Intelligence and Communications Technologies reported that international requests for online records from the United States through the formal mutual legal assistance treaty system often takes an average of months, with some taking "considerably longer."[4] The lengthy delays arise not only due to an inadequate legal framework, but also from the fact that law enforcement officers, users, companies, and legal practitioners are often unfamiliar with how the system works.

This article seeks to fill the gap in knowledge by explaining the laws and processes for international requests for online records made to US-based companies in the context of criminal matters. It is a survival guide for those

---

applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.": U.S., National Institute of Standards and Technology, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, by Peter Mell & Timothy Grance (U.S. Department of Commerce, 2011) at 2, online: NIST <csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

2 See, e.g., Google, "Google Transparency Report," online: <www.google.com/transparencyreport> [Google, "Transparency"]; Microsoft, "Law Enforcement Requests Report," online: <www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency>; Yahoo, "Transparency Report," online: <https://transparency.yahoo.com>; Apple, "Transparency Reports," online: <https://www.apple.com/privacy/transparency-reports>; Twitter, "Transparency Report," online: <https://transparency.twitter.com>.

3 United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (Vienna: UNODC, 2013) at xviii, online: <www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>.

4 U.S., *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* (Washington, D.C.: 2013) at 227, online: <https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>.

involved with international law enforcement access to user data, as well as a call to action to address the deficiencies in the current system.

This article emphasizes law and policies as they are currently applied. While it outlines the international context and some of the areas where the law may be changing, it primarily focuses on the way in which the United States government and US-based providers currently apply the law. In the future, it seems likely that there will be more non-US-based providers holding international user data. However, at the moment, US-based providers dominate much of the global market[5] and US law and practice therefore impacts a significant percentage of international Internet users. It is also worth noting two other parameters for this article:

- It deals only with data for criminal matters, not for other intelligence purposes; and
- It focuses on online data of the type held by Internet companies and Internet providers, not telecommunications carriers.[6]

I. TYPES OF INTERNATIONAL LEGAL COOPERATION

To obtain online data, investigators and prosecutors have four main options:

(1) ad hoc arrangements with providers;
(2) law enforcement cooperation;
(3) letters rogatory; and
(4) mutual legal assistance.

This section will outline these forms of cooperation in general terms. The discussion below will explain how they operate in the US context.

(a) Ad Hoc Arrangements with Providers

Depending on the domestic laws of the states where the law enforcement officer and Internet provider are located, an officer may be able to obtain some types of user data directly from the Internet company. In practice, whether this avenue is available in a particular case depends not only on domestic privacy and communications laws, but also on company policies and terms of service. In the context of online records, this is one of the most commonly used forms of international legal cooperation, and this is what is referred to in company transparency reports as user data requests from international governments.

---

[5] For example, the largest social networks in Brazil and India are US companies. Brazil has 41.2 million tweeters. India has 90 million Facebook users. Facebook and YouTube are the biggest Internet platforms globally, with 1.35 billion and 1 billion users each respectively. Statistica, "Leading social networks worldwide as of August 2015, ranked by number of active users (in millions)" (2015), online: < www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users > .

[6] This article uses the terms "Internet provider" and "Internet company" to refer to providers of Internet-based communications and storage services. This broadly aligns with the providers subject to the *Stored Communications Act*, 18 U.S.C. § 2701-2712 (2006) [*SCA*].

In practice, the majority of requests made to the largest Internet companies are made through direct requests to companies or through law enforcement cooperation, as explained in section 4.2 below. Figure 1 shows that in the first half of 2014, Google received 31,698 requests for user data. Of these requests, 19,159 were made by foreign governments directly contacting Google (i.e., not through law enforcement cooperation or mutual legal assistance treaties (MLAT)).[7] The 12,539 requests that are listed as having been made by the US government include requests made for US domestic purposes *and* requests that were made in response to an MLAT request.

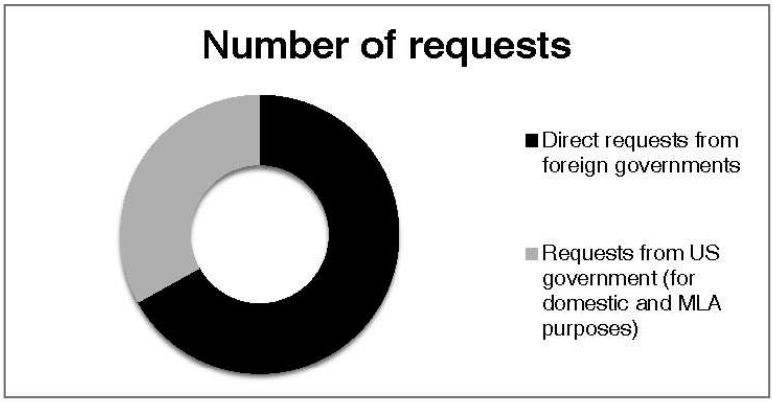

Figure 1: Number of government requests for user data received by Google between July and December 2014.

(b) Law Enforcement Cooperation

Law enforcement cooperation is when law enforcement officers in one state share information that they have obtained using domestic processes with law enforcement officers in another state. These law enforcement agencies can include police, customs, or financial intelligence units. Law enforcement cooperation can be based on country-to-country bilateral relationships, or through international organizations. The most well-known example of a multilateral institution that enables bilateral law enforcement cooperation is INTERPOL, which was established in 1956 and has 190 member states.[8] Article 2(1) of INTERPOL's *Constitution* states that INTERPOL's aim is "[t]o ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in

---

7 Google, "Transparency," s*upra* note 2.

8 INTERPOL, "About INTERPOL: Overview," online: < www.interpol.int/About-INTERPOL/Overview > .

the spirit of the 'Universal Declaration of Human Rights.'"[9] Regional examples such as EUROPOL and AMERIPOL carry out similar functions.

Some multilateral treaties on transnational crime have provisions encouraging parties to provide law enforcement cooperation to one another.[10] Article 23 of the Council of Europe Convention on Cybercrime (*Budapest Convention*) obliges parties to cooperate with one another "to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."[11] Sometimes the basis for law enforcement cooperation is spelled out in a memorandum of understanding (MOU). These MOUs have a less-than-treaty status at international law and are usually not publicly available.[12] Whether an agency can hand over information to a foreign agency may be governed by that state's domestic laws (including laws on privacy and police powers), even if an MOU exists.

Many governments have law enforcement liaison officers or legal attachés stationed around the world who help facilitate law enforcement cooperation. The UK National Crime Agency, for example, has 120 international liaison officers covering 150 different countries.[13] The FBI has 64 legal attaché offices,[14] which provide an important contact point for foreign officers seeking online data from US-based companies. Officers may also cooperate by connecting through informal, officer-to-officer relationships that they have made through international operations, or even conferences, travel, or other personal connections.

---

9 INTERPOL, *Constitution of the ICPO-INTERPOL*, I/CONS/GA/1956(2008), art. 2(1), online: < www.interpol.int/About-INTERPOL/Legal-materials/The-Constitution > .

10 See, e.g., *United Nations Convention against Corruption*, 9 December 2003, 2349 U.N.T.S. 41, art. 48(2) (entered into force 14 December 2005) [*UNCAC*]; *United Nations Convention against Transnational Organized Crime*, 12 December 2000, 2225 U.N.T.S. 209, art. 27(2) (entered into force 29 September 2003) [*UNTOC*]; *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, 20 December 1998, 1582 U.N.T.S. 41, art. 9(1) (entered into force 11 November 1990) [*Drugs Convention*].

11 Council of Europe, Committee of Ministers, *Convention on Cybercrime*, 23 November 2001, 2001 C.E.T.S. 185, art. 25(1), online: < conventions.coe.int/Treaty/EN/Treaties/Html/185.htm > [*Budapest Convention*].

12 Kate Westmoreland, "Sharing Evidence across Borders: The Human Rights Challenge" (2012) 30 Australian YB Intl L. 161 at 172 [Westmoreland, "Sharing Evidence"].

13 U.K., National Crime Agency, "About Us: What We Do" (London, U.K.), online: < www.nationalcrimeagency.gov.uk/about-us/what-we-do > .

14 U.S., Federal Bureau of Investigations, "About Us: International Operations" (FBI), online: < www.fbi.gov/about-us/international_operations > .

(c) Letters Rogatory

A letter rogatory is a formal request for assistance from the courts in one country to the courts in another country, usually by way of the diplomatic channel. A letter rogatory is:

> [T]he customary method of obtaining assistance from abroad in the absence of a treaty or executive agreement. . ..[It] is a request from a [US] judge. . .to the judiciary of a foreign country requesting the performance of an act which, if done without the sanction of the foreign court, would constitute a violation of that country's sovereignty.[15]

As the US Department of State notes, prosecutors should assume that a letter rogatory will take "a year or more" and even in urgent cases will likely take at least a month.[16] Thus, in practice, letters rogatory have been relegated to a measure of last resort. One factor that gives letters rogatory a continuing role is that some countries (including the United States) generally only allow government agencies (and their prosecuting agencies) to use the mutual assistance process and therefore defendants in criminal cases can only access information that may assist them through a letter rogatory.[17] Given their limited role in law enforcement access to user data, this article will not consider letters rogatory in detail.

(d) Mutual Legal Assistance

Mutual legal assistance (MLA) is the formal government-to-government process for sharing information in criminal matters. MLA covers a wide range of assistance, and commonly includes:

- service of documents;
- search and seizure;
- restraint and confiscation of proceeds of crime;
- provision of telephone intercept material; and
- taking of evidence from witnesses.[18]

For the purposes of this discussion, the most relevant type of assistance is search and seizure because this is the mechanism that law enforcement can use to compel access to online records. However, it is important to remember that search and seizure of online records is only one aspect of the range of assistance encompassed by most MLA relationships.

---

[15] U.S., Department of Justice, *Criminal Resources Manual* (1997), s. 275, online: < www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00275.htm > .

[16] *Ibid.*

[17] See Robert Neale Lyman, "Compulsory Process in A Globalized Era: Defendant Access to Mutual Legal Assistance Treaties" (2006) 47:1 Va. J. Intl L. 261.

[18] See e.g., *Model Treaty on Mutual Assistance in Criminal Matters*, GA Res 45/117, UNGAOR, 1990, U.N. Doc. A/45/49 (1990), art. 1(2) [*UN Model Treaty*].

Mutual legal assistance can be made on the basis of an MLAT or, if both states' domestic laws allow for it, on the basis of reciprocity. Many States have negotiated bilateral MLATs and there are also multiple regional MLATs.[19] These bilateral and regional MLATs apply to a broad range of criminal matters, including, for example, money laundering, organized crime, and serious crimes such as murder and sexual assault.

There are also many multilateral treaties on transnational or international crime that have MLA provisions.[20] These provisions create MLA obligations between parties, but only for crimes that are covered by that treaty. For instance, article 46(1) of the UN Convention against Corruption obliges states parties to "afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences covered by this Convention."[21]

Multilateral treaties and regional schemes usually do not supplant, but instead sit alongside, any bilateral treaties or relationships that particular states may have. For example, in an investigation of a corruption offence, a state may be able to make an MLA request on the basis of reciprocity, a bilateral treaty, a regional scheme, or the UN Convention against Corruption. The requesting state will select which legal basis to use depending on its own (or the requested state's) practical requirements or preferences. This combination of bilateral, regional, and multilateral arrangements provides a far-reaching web of MLA relationships. Where there is the political will to assist one another, a supporting legal framework can often be found.

Mutual legal assistance requires a significant level of trust between states because it often requires one state (the requested state) to use compulsory legal process on persons within that state, which can have serious consequences for that individual's liberty, property, or privacy.[22] For this reason, both the requesting and requested states usually have multiple steps and levels of authorization to make or receive an MLAT request, and the process can be quite bureaucratic and formalistic.[23]

Mutual legal assistance treaties commonly require each party to establish a central authority to handle all incoming and outgoing requests for assistance.

---

[19] See, e.g., OAS, General Assembly, *Inter-American Convention on Mutual Assistance in Criminal Matters*, (1992), online: <www.oas.org/juridico/english/treaties/a-55.html>; Association of Southeast Asian Nations, *Treaty on Mutual Legal Assistance in Criminal Matters* (2004), online: <agreement.asean.org/media/download/20131230232144.pdf>; Council of Europe, PA, *European Convention on Mutual Assistance in Criminal Matters*, 1959 C.E.T.S. 30 (1959), online: <conventions.coe.int/Treaty/en/Treaties/Html/030.htm>.

[20] See, e.g., *UNTOC*, *supra* note 10, *UNCAC*, *supra* note 10, *Drugs Convention*, *supra* note 10.

[21] *UNCAC*, *supra* note 10, art. 46(1)

[22] See Westmoreland, "Sharing Evidence," *supra* note 12.

[23] The many steps involved in an MLAT request are explained in section III below.

Central authorities are usually located within the government's justice department or foreign ministry.[24] The agreements themselves do not specify the end-to-end process. Instead, this is governed by a mixture of national laws, laws covering international cooperation, and laws relating to what is being requested. The MLA process is therefore determined by a combination of domestic law, and bilateral and multilateral treaties. MLA is legally robust because it is the only process that ties together the laws of both the requesting and requested states.

II. JURISDICTION: WHOSE LAWS CONTROL ACCESS TO USER DATA?

Access to user data can easily involve three or more different states and it is important to be clear about which state's laws apply to which aspects of the process of sharing user data. An email provider might be headquartered in State X, the law enforcement officer and the user might be in State Y, and the actual data might be stored in State Z.

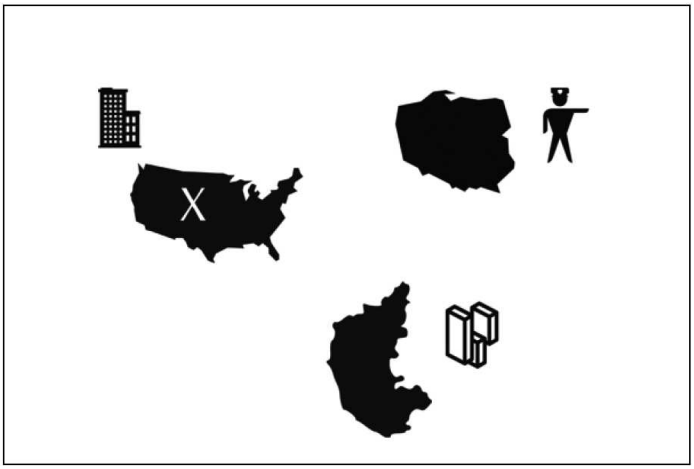

Figure 2

This example could easily become more complicated if the user were in a different state from the law enforcement officer or if copies of the data were hosted in multiple locations. In the context of cloud computing, it is also common for data to be hosted by a third party unrelated to the service provider,

---

[24] United Nations Office on Drugs and Crime, *Revised Manuals on the Model Treaty on Extradition and on the Model Treaty on Mutual Assistance in Criminal Matters*, (Vienna: UNODC, 2006) at 83, online: <www.unodc.org/pdf/model_treaty_extradition_revised_manual.pdf>.

which adds yet another layer of complexity. It is therefore unsurprising that it can be difficult to determine which state's laws govern data access in international cases. This is an unsettled area of the law, and state practice is rapidly evolving as an increasing number of cases are coming before the courts.[25] This section will provide an overview of the legal issues in determining jurisdiction when requesting online records. The next section will explain how the law is currently being applied in practice with respect to US-based Internet companies.

As an issue in international law, jurisdiction means a state's right to regulate the conduct of matters that are not exclusively of domestic concern.[26] The concept of jurisdiction can be broken down into three aspects, which broadly mirror the arms of government: prescriptive (exercised by the legislature); enforcement (exercised by the executive); and adjudicative (exercised by the judiciary). In the context of online user records, prescriptive jurisdiction means the ability to create laws controlling when and on what terms governments can access user data held by private companies. Adjudicative jurisdiction means which courts can hear disputes about the application of these laws. Enforcement jurisdiction means the power for officers to enforce the laws through compulsory process (e.g., executing search warrants, or arresting or imprisoning individuals). It is this third aspect of jurisdiction that is most important in the context of accessing online records because government agencies need to use search warrants to compulsorily access online data.

A state enjoys plenary power with respect to all three types of jurisdiction for matters and individuals *within its own territory*. However, legislative jurisdiction can go beyond a state's territory. There are four main bases that a state can use to legislate concerning crimes occurring outside its territory:

(1) nationality (for conduct committed by a national or resident of that state);
(2) the protective principle (for conduct such as espionage or counterfeiting that would prejudice the state's vital interests);
(3) universal jurisdiction (for conduct that constitutes the crime of piracy, genocide, crimes against humanity, war crimes or torture, which customary international law recognizes as having extraterritorial jurisdiction); and
(4) passive personality (for conduct committed against a victim from that state).[27]

---

[25] See, e.g., *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 15 F.Supp.3d 466 (S.D.N.Y., 2014) [*Microsoft Ireland*].

[26] Teresa Scassa & Robert J. Currie, "New First Principles? Assessing the Internet's Challenges to Jurisdiction" (2011) 42:4 Geo. J. Intl L. 1017 at 1021, citing , 42 Geo. J. Int'l L. 1017, 1020 (2011) citing F.A. Mann, "The Doctrine of Jurisdiction in International Law" (1964) 111 Rec des Cours 1 at 9.

[27] International Bar Association, *Report of the Task Force on Extraterritorial Jurisdiction* (2009) at 11, online: < www.ibanet.org > . See also *Restatement (Third) of the Foreign Relations Law of the United States* § 432(2) (1987).

These multiple bases for extraterritorial legislative jurisdiction mean that it is not uncommon for there to be concurrent jurisdiction, with multiple states having legislation governing a situation. Various norms have evolved to settle situations where there is a conflict of laws.[28]

Unlike legislative jurisdiction, enforcement jurisdiction is usually bound by a state's territory. Absent special circumstances or express permission, a state cannot enforce its own laws in another state's territory.[29] As the International Bar Association *Report of the Task Force on Extraterritorial Jurisdiction* states: "a state cannot investigate a crime, arrest a suspect, or enforce its judgment or judicial processes in another state's territory without the latter state's permission."[30] The different territorial bounds of legislative and enforcement jurisdiction can create a situation where a state has legislation governing a person's actions outside its territory but is unable to enforce that law (at least while the person is outside of its territory).

Applied to the online records example above, this means that State Y may have laws about when a law enforcement agent is able to seek records from a company or individual in another state and what rights the user has for how that information is handled. States X and Z could each have laws about how companies handle personal information and when they can hand over user data. There is therefore concurrent legislative jurisdiction about how user data is stored and shared by companies, and accessed and used by government officers. If parties provide user data on a voluntary basis, it could be governed by the laws of States X, Y, and Z. However, if a government officer seeks to *compel* the production of that data, this usually requires the exercise of a search warrant. This can usually only be exercised within the officer's territorial state.

The key question for compulsorily obtaining user data then becomes: where does the search and seizure occur? Several possibilities exist:

- Where the data servers are located;
- Where the Internet company receives copies of the records after retrieval from the data servers; or
- Where the law enforcement officer looks at the records.

At the moment, the law is unsettled and there is no clear answer to this question. Applying precedents based on physical property to electronic data is difficult. Physical property is usually searched before it is seized. Cases involving electronic data turn this scenario on its head because police officers usually seize computer data first (either by seizing the device or by obtaining it from the Internet company), and then take it off-site to search it. Electronic property is also unusual in that it may be copied infinitely without compromising the original data, and multiple copies are often created in the ordinary course of

---

[28] Scassa & Currie, *supra* note 26 at 1020, 1026.

[29] *The Case of the S.S. "Lotus" (France v. Turkey)*, (1927) P.C.I.J. (Ser. A) No. 10.

[30] International Bar Association, *supra* note 27 at 10.

use.[31] Companies or users can therefore hand over data without necessarily forfeiting the original copy.

The US courts are currently grappling with the correct way of analyzing search and seizure in the context of access to user data.[32] Microsoft Corporation is challenging a US search warrant over user data that the company stores in Ireland. Microsoft argues that the search warrant seeks to access data that is stored outside of the United States and is therefore beyond the scope of the US search warrant. Effectively, this is arguing that the search or seizure occurs in Ireland and is therefore beyond US enforcement jurisdiction. The federal magistrate did not dwell on the issue of where the search and seizure occurred. He referred in passing to Orin Kerr's opinion in a 2005 article that the search occurs at the time that officers observe the information, not at the time it is copied. However, in 2010 Kerr rejected his previous position and instead argued that in most cases it is the act of copying the data that constitutes a seizure under the Fourth Amendment. He explains:

> [A] government request to an ISP to make a copy of a suspect's remotely stored files and to hold it while the government obtains a warrant would also constitute a seizure. In such a case, the government uses a private actor as its agent, and it so happens that this agent might need to copy the target's files for back-up purposes of its own. The government's action, however, changes the path of the communication of contents that would have occurred in the ordinary course of business. Generating the copy freezes the scene at the government's request, preserving evidence for government use. Generating such a copy should also be a seizure.[33]

Other commentators adopt different reasoning, but agree with Kerr's conclusion that it is the copying that constitutes a seizure.[34]

Even if it is accepted that it is the act of copying that constitutes the seizure, this is only part of the answer. The question then shifts to where the copying actually occurs—is it where the parent company is based when it sends the request for the data and receives the response (i.e., State X, in our example); or is it the host's location when it retrieves that data (State Z)? Arguments could be made for either position.[35]

---

[31] Orin S. Kerr, "Fourth Amendment Seizures of Computer Data"(2010) 119:4 Yale L.J. 700 at 702.

[32] *Microsoft Ireland*, *supra* note 25.

[33] Kerr, *supra* note 31 at 722 [footnotes omitted].

[34] Paul Ohm, "The Fourth Amendment Right to Delete" (2005) 119 Harv L. Rev. Forum; Susan W. Brenner & Barbara A. Frederiksen, "Computer Searches and Seizures: Some Unresolved Issues" (2001-2002) 8 Mich Telecomm & Tech L. Rev. 39.

[35] For an excellent discussion of the *Microsoft Ireland* case and the ways in which data challenges traditional notions of jurisdiction, see Jennifer Daskal, "The Un-Territoriality of Data," Yale L.J. [forthcoming in 2015/2016], online: SSRN <ssrn.com/abstract=2578229>.

Yet another layer of complication occurs when an Internet provider's terms of service specify the jurisdiction where it will accept legal process. If the user and provider both agree to be bound by State Z's laws, does this impact on the ability to use a search warrant obtained under the laws of State X (i.e., where the headquarters are located)? Does consent change the analysis of whether enforcement jurisdiction is being invoked when copying data from servers located in another state? Article 32(b) of the *Budapest Convention* partially answers this by suggesting that a state can:

> [W]ithout the authorisation of another Party. . .access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.[36]

However, there is not a definitive answer about whether the "person who has the lawful authority" is limited to the user or could include the Internet provider.[37] Moreover, the Council of Europe has also suggested that "general agreement by a person to terms and conditions of an online service used might not constitute explicit consent even if these terms and conditions indicate that data may be shared with criminal justice authorities in cases of abuse."[38] A detailed consideration of this issue is beyond the scope of this article. However, it is worth highlighting the added layer of complexity that consent and terms of service can bring to the issue of jurisdiction.

In light of this uncertainty, the following section will outline the way in which the law is currently being applied by most companies and governments seeking to access records from US-based Internet companies that accept US jurisdiction.

III. US LAW IN PRACTICE: WHAT PROCESS DO YOU NEED TO USE TO OBTAIN USER DATA?

By virtue of the fact that US Internet providers dominate the global market, an issue that is inherently global in theory becomes decidedly US-focused in practice. Many of the large, US-based Internet companies (including Google, Twitter, and LinkedIn) will only accept jurisdiction in California, where their headquarters are located. This position is reflected in these companies' terms of service[39] and their guides for law enforcement.[40] In practice, this means that a

---

[36] *Budapest Convention*, *supra* note 11, art. 32(b)

[37] *Ibid.*

[38] Council of Europe, Cybercrime Convention Committee, *T-CY Guidance Note #3 Transborder Access to Data (Article 32)* (Strasbourg: Council of Europe, 2014) at 7, online: <www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297REV_GN3_transborder_V13.pdf>.

[39] See, e.g., Twitter, "Terms of Service," s. 12(B), online: <https://twitter.com/tos>; Google, "Google Terms of Service," online: <www.google.com/intl/en/policies/terms>.

law enforcement officer in State Y must follow US law in order to access Gmail records.

However, there is currently a major divergence in the approach of some of the US-based Internet companies. Microsoft, Yahoo, and Apple have established legal entities in other regions of the world where their international users reside and will only accept local legal process with respect to these users. Microsoft has recently been defending this position, refusing to accept US legal process seeking access to user content that is stored in Ireland.[41]

Public backlash against US government access to non-US persons' data, and data localization movements in countries such as Brazil, Russia, and India are creating pressure to locate data on servers outside the US and to use local jurisdiction. Depending on the outcome of the *Microsoft Ireland* case, this may mean that US law becomes less dominant in determining law enforcement access to online user data. However, at the moment, it is still US law and policy that shapes much of the day-to-day sharing of online data. This section will first briefly outline the law governing access by US law enforcement to online data, and will then explain how this law applies to international law enforcement access.

(a) Access to Online Records by US Domestic Law Enforcement

The *Electronic Communications Privacy Act of 1986* (*ECPA*)[42] governs disclosure and access to online communications. Within this, the *Stored Communications Act* (*SCA*)[43] regulates access to stored information (real-time or prospective access is beyond the scope of this article). The *SCA* covers emails held by electronic communication services (ECS) and contents of communications transmitted for remote storage and processing by remote computing services (RCS). This categorization as an ECS provider or RCS provider is an outdated dichotomy. Today's multifunction email, cloud storage, and social media providers blur these boundaries beyond recognition. This adds a layer of uncertainty and confusion about precisely which protections apply to certain types of user data. This section will not explore the many criticisms and detailed analyses of *ECPA*.[44] Instead, it will briefly outline how the *SCA* is

---

[40] See, e.g., Twitter, "Guidelines for Law Enforcement" (2015), online: https://support.twitter.com/articles/41949-guidelines-for-law-enforcement [Twitter, "Guidelines"]; LinkedIn, "LinkedIn Law Enforcement Data Request Guidelines" (2015), online: *https://help.linkedin.com/app/answers/detail/a_id/16880* > .

[41] See *Microsoft Ireland*, *supra* note 25.

[42] *Electronic Communications Privacy Act of 1986*, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.) [*ECPA*].

[43] 18 U.S.C. § 2701-2712 (2006) [*SCA*].

[44] See, e.g., Digital Due Process, "About the Issue" (2010), online: < digitaldueprocess.org > , which is a coalition of privacy advocates, companies, and think tanks calling for *ECPA* reform. See also, Orin S. Kerr "The Next Generation Communications Privacy Act" (2014) 162:2 U. Pa. L. Rev. 373 [Kerr, "NGCPA"].

currently applied in practice in order to explain how it interacts with international governments' access to online records in the United States.

(i) Access to Non-Content

Under the law of the United States, an Internet company cannot *voluntarily* disclose customers' non-content records to any government entity unless a statutory exception applies.[45] These statutory exceptions include emergencies "involving danger of death or serious physical injury to any person [and] requires disclosure without delay" or reports to the National Center for Missing and Exploited Children.[46]

The ways in which government agencies can *compel* an Internet company to disclose non-content information depends on what type of non-content information is being sought. Government officials can request the information via administrative subpoena, court order, or search warrant as outlined in Figure 3 below. One noticeable gap is that the *SCA* probably does not cover stored information about a user's search queries. It is likely that this highly sensitive content receives no statutory protection.[47]

	Voluntarily disclose	Subpoena without notice	Subpoena with notice	2703(d) court order	Search warrant
Basic subscriber, session, and billing information	Emergencies, NCMEC	Yes	Yes	Yes	Yes
Other transactional and account records	Emergencies, NCMEC			Yes	Yes
Content of stored files	Emergencies, NCMEC				Yes

Figure 3: Legal process required for US government agencies to obtain online records for domestic law enforcement

(ii) Access to Content

There is a similar starting point for disclosure of content as there is for non-content information; an Internet company can only *voluntarily* disclose user data content if it falls within a statutory exception. These are similar to the situations of emergency and child exploitation established for non-content disclosure.[48]

---

[45] *SCA*, *supra* note 43, § 2702(a)(3).

[46] *Ibid*, § 2702(c)(4).

[47] Kerr, "NGCPA," *supra* note 44 at 396-397.

[48] *SCA*, *supra* note 44, § 2702(b)(8).

Under the *SCA*, the ways in which the government can compel an Internet company to disclose content depends on whether it is held by an ECS or RCS, whether it is 180 days old, and whether the user has retrieved the information. In practice, these distinctions have largely been superseded by the pivotal decision of *United U.S. v. Warshak*.[49] The *Warshak* Court held that the Fourth Amendment of the United States Constitution applies because users have a reasonable expectation of privacy in the content of their emails. This means that an Internet company can only be *compelled* to disclose online content in response to a search warrant that meets the standard of "probable cause."[50] While there is still some uncertainty about the application of the Fourth Amendment, the major Internet companies have taken the stance that they will only release content in response to a search warrant. In 2013, the US Department of Justice told Congress that they also followed the ruling in *Warshak*.[51] Thus, in practice, US law enforcement can generally only access user content if they obtain a search warrant or in the case of an emergency.

(b) Access by Foreign Law Enforcement Officers

In many respects, the way in which the *SCA* covers requests from foreign governments is largely a matter of chance rather than good design. The *SCA* refers to "governmental entit[ies]."—defined in 18 U.S.C. 2711(4) to mean "a department or agency of the United States or any State or political subdivision thereof." Foreign governments are therefore not "governmental entit[ies]" for the purposes of the *SCA*. This definition has important implications for foreign government access to both content and non-content information.

(i) Non-Content

Because foreign governments are not "governmental entit[ies]" under the *SCA*, the prohibitions on disclosing non-content records to governmental entities do not apply to disclosure to foreign governments. This means that an Internet company is not compelled and can choose whether to voluntarily disclose non-content data to foreign law enforcement officers.

Different companies adopt different policies on this issue. For example, Google acknowledges that "[o]n a voluntary basis, we may provide user data in response to valid legal process from non-U.S. government agencies, if those requests are consistent with international norms, U.S. law, Google's policies and the law of the requesting country."[52] LinkedIn,[53] Twitter,[54] and Facebook[55] take a similar approach. Dropbox previously required that all data requests go

---

[49] *U.S. v. Warshak*, 631 F.3d 266 (6th Cir., 2010) [*Warshak*].

[50] U.S. Const. amend IV.

[51] Ira S. Rubinstein, Gregory T. Nojeim & Ronald D. Lee, "Systematic Government Access to Personal Data: A Comparative Analysis" (2014) 4:2 Intl Data Privacy L. 96 at 110.

[52] Google, "Transparency," *supra* note 2 at "Requests for Information about our Users: Legal Process".

through the US judicial system, but changed their policy in 2013 to allow voluntary disclosure.[56] LinkedIn states that they "generally" require that requests come through MLA or a letter rogatory.[57] Twitter also states that they respond to requests that properly come through MLA or letter rogatory.[58]

(ii) Content

Foreign governments must rely on the assistance of the US government to obtain a search warrant. This is because the *SCA* only provides avenues for "governmental entit[ies]" (i.e., not foreign governments) to obtain a search warrant and, as discussed above, most Internet companies now require a search warrant before handing over any user content. In practice, this means that foreign governments must go through either police-to-police cooperation or mutual legal assistance to access user content in the United States.

Where the matter being investigated or prosecuted can be characterized as a US offence as well as a foreign offence, a US law enforcement agency can open their own investigation and obtain the data using a search warrant under the *SCA*. They can then share that data with their foreign counterparts using law enforcement cooperation. Some crime types, such as online child pornography, where the sharing of images is prolific and often global, have an inherently international aspect and can often be characterized as both a US offence and a foreign offence. They therefore lend themselves to this type of information sharing.

Where the US law enforcement agency either will not or cannot obtain or share the information, a foreign law enforcement agency must make a request through MLA. This effectively requests the US Department of Justice to work with the US agency to obtain US legal process on behalf of the foreign government.

Section 18 U.S.C §3512 enables federal courts to compel testimony or production in response to a request under an MLAT or letter rogatory. This is the section that enables US governmental entities to obtain search warrants in response to an MLA request. US law enforcement can then seek a warrant under rule 41 of the *Federal Rules of Criminal Procedure*.[59]

All requests for MLA come through the US central authority. While most US MLATs specify the Attorney General as the central authority, in practice, the

---

53 LinkedIn, *supra* note 40.

54 Twitter, "Guidelines," *supra* note 40.

55 Facebook, "Information for Law Enforcement Authorities," online: < https://www.facebook.com/safety/groups/law/guidelines > .

56 Dropbox, "2014 Transparency Report" (2014), online: < https://www.dropbox.com/transparency > .

57 LinkedIn, *supra* note 40.

58 Twitter, "Guidelines," *supra* note 40.

59 Fed. R. Crim. P. 41.

Attorney General's power has been delegated to the Office of International Affairs (OIA) within the Department of Justice.[60] Figure 4 shows the process for requesting online records from the United States through mutual legal assistance.

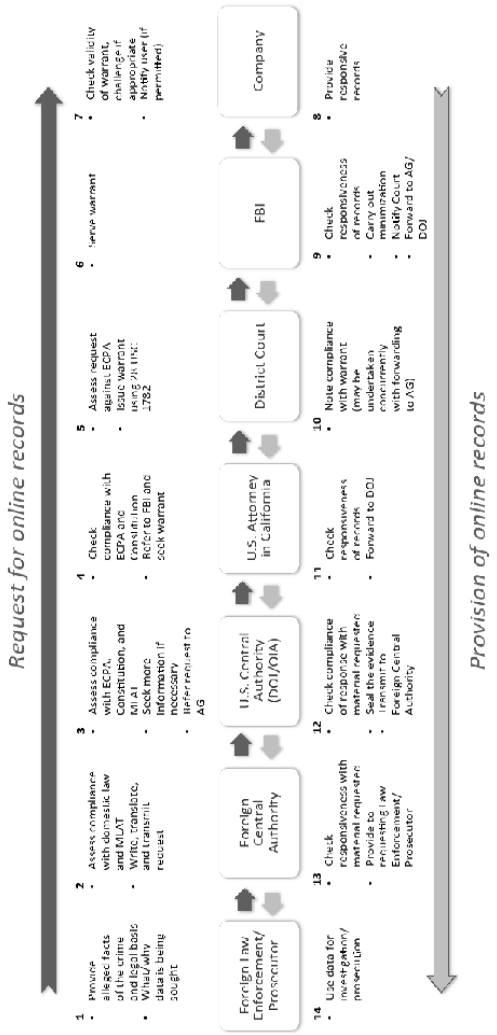

Figure 4: Process for obtaining user data from an Internet company in California

---

[60] U.S., Department of Justice, "Office of International Affairs (OIA): FAQs," online: < www.justice.gov/criminal-oia > .

MLA requests are typically initiated by prosecutors or investigators, who liaise with their central authority to draft the request in a form that meets the requirements of the domestic law and the MLAT. The central authority presents a formal, written request to the US central authority. The OIA assesses the request against US law and the MLAT, and seeks any further explanation from the requesting state if necessary. One area that can be particularly problematic for foreign countries is ensuring that the request explicitly articulates how it meets the standard of "probable cause"[61] because this is a uniquely US standard of evidence.

The OIA then refers the request to the relevant US district attorney (in the case of online matters, this is usually the Northern District of California in San Francisco). The district attorney's office works with the small team of FBI officers in charge of managing requests to the Californian Internet companies to obtain a search warrant from the district court. After assessing whether US legal requirements have been met (particularly whether probable cause has been established), the court issues the search warrant and it is served on the Internet company. At this stage, the search warrant has usually been stripped of its supporting affidavits, which means that it appears similar to a domestic search warrant. Unless there are other indications, such as a reference in the document to the originating country or the Internet company has had direct contact with the originating country, the company may not realize that it is an international request.[62] The Internet company can consider whether there are grounds on which to challenge the search warrant before handing over the records. Sometimes these records may need to be provided in a particular manner, so that they meet any requirements of the domestic law of the requesting state.[63] The records are then transmitted back through the district attorney's office to the OIA. The OIA seals the records and formally presents the MLAT response to the requesting state's central authority, who forwards them to the relevant investigator or prosecutor.

---

[61] The Fourth Amendment to the United States Constitution (U.S. Const. amend IV) states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

[62] Interestingly, this means that industry transparency reports may include MLAT-related requests for user records under the heading of "US requests" because they are not formally notified of the original source of the request.

[63] This is commonly allowed for in MLATs—e.g., *UN Model Treaty*, *supra* note 18, art. 6 states that "[t]o the extent consistent with its law and practice, the requested State shall carry out the request in the manner specified by the requesting State."

IV. PROBLEMS WITH THE CURRENT SYSTEM

The increasing number of calls to reform the system of sharing online records for criminal matters often refer to "the MLAT problem." This reflects a tendency to focus on MLAT as the primary means of sharing online evidence. However, this MLAT focus risks overlooking the fact that MLA is only one part of a broader web of international cooperation.

While there are no publicly available statistics on the number of MLAT requests, companies clearly receive fewer MLAT requests than direct requests from foreign governments. For this reason, any analysis of the problems and proposals for reform must consider the entire spectrum of international legal cooperation, not just MLA. This section briefly outlines some of the major problems with the broader system as it currently operates.

(a) Delay

One problem that affects all stakeholders is the inordinate amount of time that requests can take to complete. As noted above, MLAT requests take many months to complete. Delays in obtaining information can jeopardize law enforcement officers' ability to identify or prosecute criminals, which has obvious consequences for victims of crime and for the general public. Perhaps less obvious is the way in which delays with the MLAT system can encourage law enforcement and law-makers to adopt alternative strategies, with sometimes undesirable consequences.

Users and privacy groups are concerned that dissatisfaction with the MLAT system encourages the use of alternative mechanisms such as directly approaching Internet providers or using law enforcement cooperation. These methods are perceived as having fewer checks and balances because they do not necessarily require judicial scrutiny and are not controlled by international treaties or public agreements. In November 2014, a coalition of civil society groups wrote to members of Congress to encourage them to increase funding of the MLAT system based on the idea that MLATs "contain human rights and due process protections that may be lacking in informal assistance requests and letters rogatory."[64]

US Internet providers and the US government are fearful that delays in the MLAT process encourages the balkanization of the Internet. As the President's Review Group stated,

> Non-US governments seeking such records [via MLAT] can face a frustrating delay in conducting legitimate investigations. These delays provide a rationale for new laws that require e-mail and other records

---

[64] Letter from Access, Center for Democracy & Technology, Advocacy for Principled Action in Government, American Library Association, New America's Open Technology Institute, PEN America Center, to Members of Congress, (18 November 2014) at 1, online: < https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/11/MLAT-coalition-letter.pdf > .

> to be held in the other country, thus contributing to the harmful trend of localization laws.[65]

Data localization undermines the free flow of information across borders that enable fast and innovative online products, particularly those utilizing cloud-based technologies.

(b) Legal Uncertainty

As can be seen from the preceding sections, there are uncertainties or gaps in the law on critical issues, such as:

- jurisdiction;
- what constitutes "content"; and
- when to provide "non-content" to foreign law enforcement.

Legal uncertainty makes navigating the system and predicting how it will apply to a particular case very difficult, which is a significant problem for all stakeholders.

For providers, the uncertainty generates additional workload in considering and challenging incoming requests for data, many of which may not meet US legal requirements. It also creates business risk by placing companies in a position where they exercise a large amount of discretion as to whether to hand over data. In some cases, the companies' decisions have extremely serious consequences for users or victims of crime. Handing over the data could enable foreign police to prevent a crime from occurring. However, it could also unnecessarily invade a user's privacy, or even enable a nefarious government to persecute a human rights activist. In light of Edward Snowden's revelations about government access to user data with cooperation from Internet companies, US providers are particularly sensitive to voluntary schemes for access to metadata and subscriber information, and would like to show consistency to their users by only acceding to requests with an explicit legal underpinning.[66]

When companies insist on requiring that data requests go through the MLA process, company employees based in-country may find themselves threatened with legal action by local governments. This occurred in 2012 and 2013 for Twitter in France,[67] for several providers in India,[68] and for Google in Brazil.[69]

---

[65] President's Review Group on Intelligence and Communications Technologies, *supra* note 4 at 227.

[66] Brad Smith, "Time for an International Convention on Government Access to Data" The Huffington Post (22 January 2014), online: <www.huffingtonpost.com/brad-smith/time-for-an-international-convention-on-government-access-to-data_b_4644130.html>.

[67] Somini Sengupta, "Twitter Yields to Pressure in Hate Case in France" *The New York Times* (21 July 2013), online: <www.nytimes.com>.

[68] "Centre not co-operating in complaint against websites: Court" *Zee News* (5 December 2012), online: <zeenews.india.com>.

[69] "Google executive in Brazil detained after failure to remove YouTube video" The Guardian (27 September 2012), online: <www.theguardian.com>.

This kind of threat can impede the business growth strategies for companies in international markets because they do not want to expose local employees to retribution from their governments.

For law enforcement officers, the lack of certainty means that they cannot reliably predict whether they will be able to obtain a particular type of information from a given provider in a specific case. The time wasted in making fruitless requests or seeking records through the incorrect channel not only wastes resources, but also delays the apprehension and prosecution of criminals.

The lack of predictability and consistency also adversely impacts users in ways that concern privacy advocates. When the law is unclear, it is very difficult for everyday citizens to make informed decisions about how to manage sensitive personal data. Without clear standards and precedents it is also difficult to challenge government or company decisions if users feel that their data has been mishandled.

(c) Lack of Information about the System

The uncertainty in the current laws and practices is compounded by the lack of quality information available to law enforcement, legal practitioners, and civil society. This causes confusion and delays when requests are made through inappropriate channels or with inadequate supporting information. It can also impede investigations because lack of support and information may deter law enforcement officers from seeking information that could assist in identifying and prosecuting an offender.

(d) Costs

As the number of requests for international communications data rises, this creates a significant burden on governments' central authorities, who are responsible for processing both incoming and outgoing requests. Despite this increased burden, few countries have increased the resources provided to central authorities. MLATs generally specify that, except in exceptional circumstances, the costs of responding to requests must be borne by the requested state.[70]

The dominance of US Internet companies means that the US government receives a particularly large number of requests for online records. Recommendation 34 of the December 2013 *Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* is to

> Increase resources to the office in the Department of Justice that handles MLAT requests. The Office of International Affairs (OIA) in the Department of Justice has had flat or reduced funding over time, despite the large increase in the international electronic communications that are the subject of most MLAT requests.[71]

---

[70] *UN Model Treaty*, *supra* note 18, art. 20.

Providing adequate funding will likely continue to be a challenge as the number of requests increases each year.

Companies also feel this burden. For instance, for the second half of 2009, Google received 12,539 requests for user data from foreign governments. By the second half of 2014, that number had increased to 20,189.[72] It seems clear that the number of these requests is likely to continue to grow. Providers are able to recover from the requesting entity "a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information."[73] However, this only applies to requests through the MLAT system. Given that foreign agencies are not "governmental entit[ies]," there is no statutory obligation on these agencies to reimburse the cost to companies of complying with direct requests. Whether the companies can recover costs depends on the domestic laws and policies of the requesting state.

(e) Burden of Bureaucracy

As Figure 4 shows, steps in the MLA system are duplicated by separate agencies within each state, and then mirrored by the other state's agencies. As the system is currently designed, this process is part of the assurance between governments that appropriate authorizations have been obtained. The centralized process is also an important part of the chain of evidence because it constitutes the US government's assurance that they have obtained and provided the information. However, it also adds significantly to the expense and delays in the system. As requests for online information continue to grow, it is questionable whether this highly bureaucratic process is scalable.

(f) Sovereignty and Ownership of Data

Governments may feel a sense of frustration when they are unable to obtain communications data involving their own citizens under their own national laws, especially where these laws have robust human rights safeguards. In many cases, the duplication of processes in the requesting and requested states arguably does no more to protect the privacy of the user, instead frustrating the investigative or judicial process in the country requiring the information.

Having US law as the gatekeeper for all requests for data from US-based providers also limits the ability of foreign citizens or governments to protect their citizens and challenge the way in which foreign companies handle their data. This has been raised as a concern in the *Microsoft Ireland* case, where the data protection regime in Ireland could be seen as stronger than in the United States.[74] Minister for EU Affairs and Data Protection Dara Murphy said:

---

[71] President's Review Group on Intelligence and Communications Technologies, *supra* note 4 at 227-228 [emphasis omitted].

[72] Google, "Transparency," *supra* note 2.

[73] *SCA*, *supra* note 43, § 2706(a).

> "[T]he possible implications of this ruling are very serious for Ireland and the European Union as compliance with the warrant may result in Microsoft, and any other US companies with operations in the EU which are served with such warrants in the future, being in breach of the Irish Data Protection Acts and the EU Data Protection Directive. This would create significant legal uncertainty for Irish and EU consumers and companies regarding the protection of their data which, in this digital age, is everyone's most valuable asset."[75]

Governments' concerns about ensuring that companies that are doing business in their jurisdiction comply with the laws of their jurisdiction can be used to justify data localization laws, thus undermining the global nature of the Internet.[76]

(g) Lack of Feedback about Requests and Outcomes

There is currently no systematic communication between Internet companies, the various agencies within the requesting state, and the various bodies within the requested state about the status of a request for assistance. This means that law enforcement or prosecutors in the requesting state often cannot monitor the progress of their request after it has entered into the "black hole" of the MLAT system. The lack of information also removes a possible incentive for these actors to perform their part of the process quickly because there is no attribution of responsibility for delays.

(h) Transparency

Non-governmental organizations who focus on representing the privacy rights of the users are frustrated by the lack of transparency in the current system.[77] Despite increased transparency reporting by many providers, this only provides part of the picture because providers are not informed if a search warrant is based on a request made through MLAT. In order to have the full picture, governments must also provide transparency reports. While some governments provide statistics on MLAT requests,[78] the US government does not. As discussed below, the proposed *Law Enforcement Access to Data Stored*

---

74 Irish Government News Service, News Release, "Murphy expresses serious concern over implications of U.S. Court ruling for Irish and EU Data Protection law," (4 September 2014), online: < www.merrionstreet.ie/en > .

75 *Ibid.*

76 See, e.g., Jonah Force Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders" (2014) Hague Institute for Global Justice, online: SSRN < papers.ssrn.com/sol3/papers.cfm?abstract_id = 2430275 > .

77 Access Policy Team, "MLAT: a Four-Letter Word in Need of Reform" (9 January 2014), *Access Now* (blog), online: < https://www.accessnow.org/blog/2014/01/09/mlat-a-four-letter-word-in-need-of-reform > .

78 See, e.g., Austl., Commonwealth, *Attorney-General's Department Annual Report, 2013-*

Abroad Act calls for mandatory regular reporting of details about MLAT requests for online records.[79]

(i) Human Rights Protections

There is very little in the way of enforceable human rights safeguards in any of the methods of sharing user data internationally. As noted above, when US companies provide non-content user data directly to foreign governments, there are no legal safeguards under US law. Many companies have internal policies about the due diligence they undertake and the factors they consider. Some of these are made public in the form of law enforcement guidelines.[80] However, adherence to these policies is voluntary, and the contents and implementation of these policies can vary from company to company.[81]

The existence and the scope of any human rights protections in how online user data can be shared through law enforcement cooperation depends largely on the domestic legislation in the requesting and the requested states. International organizations, including INTERPOL and EUROPOL, are becoming increasingly sensitive to how personal data is accessed, used, and retained and have established structures and processes to ensure adherence to international data protection standards (particularly those established in the European Union). To this end, INTERPOL and EUROPOL have established independent oversight and inspection bodies, comprising the data protection inspectors and other independent members from member states.[82]

The MLAT process picks up any domestic legal protections over data access in both the requesting state and the requested state. Depending on the terms of the MLA relationship, there may also be additional, treaty-derived safeguards. Bilateral MLATs can vary widely depending on the negotiating parties, but the

---

2014 (Barton, ACT: 2014) at 188, online: <www.ag.gov.au/Publications/Annual-Reports/13-14/Documents/AGDAnnualReport.pdf>.

79 U.S., Bill S 2871, *Law Enforcement Access to Data Stored Abroad Act*, 113th Cong., 2013-2014, § 4(A)(2), online: <www.hatch.senate.gov/public/_cache/files/1f3692d5-f41f-4c73-acf2-063c61da366f/LEADS%20Act,%20September%2018,%202014.pdf>.

80 For a list of major companies' law enforcement guidelines see Nate Cardozo, Cindy Cohn, Parker Higgins, Kurt Ospahl & Rainey Reitman, *Who Has Your Back? The Electronic Frontier Foundation's Fourth Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data* (Electronic Frontier Foundation, 2014), online: <www.eff.org/who-has-your-back-2014>.

81 See Kate Westmoreland, "Are Some Companies 'Yes Men' when Foreign Governments Ask for User Data?" (30 May 2014), *Stanford Center for Internet and Society* (blog), online: .

82 See, e.g., EUROPOL, "Management & Control) (EUROPOL, 2015), online: <https://www.europol.europa.eu/content/page/management-147>; INTERPOL, "Structure and Governance: Commission for the Control of INTERPOL's Files" (INTERPOL), online: <www.interpol.int/About-INTERPOL/Structure-and-governance/Commission-for-the-Control-of-INTERPOL's-Files>.

UN Model Treaty gives an indication of the types of provisions that commonly appear in bilateral MLATs. Article 4 of the *UN Model Treaty* sets out discretionary grounds upon which a requested state can refuse to provide assistance. These include where the request "if granted, would prejudice its sovereignty, security, public order. . .or other essential public interest."[83] This could potentially include a requested state's human rights obligations. Other relevant grounds for refusal include:

- Where "[t]here are substantial grounds for believing that the request. . .has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions"[84]; and
- Where the individual would be subject to the death penalty.[85]

Many MLATs only facilitate assistance if there is "dual criminality." This means that the conduct constituting the offence amounts to a crime under the laws of both the requesting state (if it were committed in that state's jurisdiction) and the requested state. It is important to note that dual criminality and all of the grounds for refusal are commonly discretionary, meaning that there are still very few *mandatory* safeguards.[86] Moreover, there are likely no obligations under international human rights law owed by a state that provides user data to another state, even if that state is known to have a bad human rights track record.[87]

With so many criticisms of the current system, it comes as no surprise that there are multiple domestic and international reform efforts underway.

V. REFORM EFFORTS AND THE WAY FORWARD

There has recently been a surge of interest in MLATs, and growing consensus about the need for reform. While the need for reform may be clear, it is not clear what form it should take. This section will briefly outline some of the major groups involved in reform efforts and the initiatives that they are undertaking.

(a) Inter-Governmental Initiatives

The UN Office on Drugs and Crime is the UN agency responsible for international legal cooperation in criminal matters, including mutual legal assistance. Some of UNODC's reform activities include establishing regional networks of central authorities to improve cooperation and coordination.

---

83 *UN Model Treaty*, *supra* note 18, art. 4(1)(a).

84 *Ibid*, art. 4(1)(c).

85 *Ibid* at 147, n. 6.

86 See Westmoreland, "Sharing Evidence," *supra* note 12.

87 *Ibid*.

UNODC has also developed an MLA request-writing tool to assist governments in drafting MLA requests, which they are currently updating.[88] Unfortunately, this request-writing tool is only available to governments, not to civil society or private practitioners. This secrecy seems overly cautious, and misses an opportunity not only to demonstrate transparency but also to benefit from broader external input.

UNODC performs the secretariat function for some of the major multilateral criminal treaties with MLA provisions, including the *United Nations Convention against Transnational Organized Crime* (*UNTOC*) and the *United Nations Convention against Corruption*. The UNODC also coordinates the United Nations Commission on Crime Prevention and Criminal Justice (the Crime Commission), which comprises all 147 states parties to *UNTOC*. The Crime Commission has recently called for input from member states on whether the model bilateral MLAT should be updated.[89] However, this is likely to be a difficult and contentious project. Previous proposals from states wishing to draft a new, multilateral, comprehensive MLA and law enforcement cooperation treaty have been rejected by the majority of states.[90]

INTERPOL increasingly facilitates the sharing of information, including electronic data, through a network of liaison officers and shared databases. INTERPOL's new Global Complex for Innovation is located in Singapore. It focuses on "cutting-edge" research and development, with one of its three core components being "[d]igital [s]ecurity." As part of this component, INTERPOL is working to develop "practical solutions in collaboration with police, research laboratories, academia and the public and private sectors."[91]

(b) Governmental Initiatives

As well as working together through international organizations, individual states are undertaking reform initiatives. Public concern in response to Edward Snowden's revelations has meant that much of the international spotlight has been on the US government. In response, on 12 August 2013, President Obama established the President's Review Group on Intelligence and Communications

---

[88] United Nations Office on Drugs and Crime, *Mutual Legal Assistance Request Writer Tool* (2015), online: <https://www.unodc.org/mla/introduction.html>.

[89] Commission on Crime Prevention and Criminal Justice, *Report on the Twenty-Third Session*, UNESCOR, 2014, Supp. No. 10, U.N. Doc. E/CN.15/2014/20, online: <https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_23/E2014_30e_V1403808.pdf>.

[90] For example, the issue was discussed but ultimately rejected at the 2010 UN Congress on Crime Prevention and Criminal Justice. See Congress on Crime Prevention and Criminal Justice, *Draft Salvador Declaration: Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World*, U.N. Doc. A/CONF.213/L.5 (2010).

[91] INTERPOL, "The INTERPOL Global Complex for Innovation" (INTERPOL), online: <www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation>.

Technology.[92] The Review Group's final report included in recommendation 34 that the US government should streamline the process for lawful international requests to obtain electronic communications through the MLAT process. Specifically, the review group suggested:

- increasing resources to the OIA within the DOJ;
- creating an online submission form for MLATs;
- streamlining the number of steps in the process;
- streamlining the provision of information back to the requesting state; and
- promoting the use of MLATs globally.[93]

On 18 September 2014, Senators Orrin Hatch, Chris Coons, and Dean Heller introduced the *Law Enforcement Access to Data Stored Abroad Act*.[94] This Bill seeks to restrict US law enforcement's ability to use US legal process to access data that is stored abroad. It is based on the premise that law enforcement should use the MLAT process for trans-border data requests. Section 4 of the Bill outlines reforms to the MLAT process, including creating an online request form, and requiring the US Department of Justice to publish statistics about requests and the time taken to process them.

The British government has also been active in this area. In July 2014, the British Prime Minister announced his intention to appoint a Special Envoy on intelligence and law enforcement data sharing. In September 2014, he appointed a former senior diplomat, Sir Nigel Sheinwald, to this role.[95] The terms of reference for the role include: improving relationships with Internet companies; improving the way in which MLATs, law enforcement cooperation, and direct requests for user data are managed; and considering new international arrangements for data sharing.[96]

(c) Industry Initiatives

Individual companies have been working separately on ways to streamline their processes for handling user data requests but at the same time distance themselves from allegations of being too cooperative with government. Many of the big US-based Internet providers are part of the Reform Government Surveillance initiative, which focuses on five key reforms.[97] One of these reforms is "[a]voiding [c]onflicts [a]mong [g]overnments," and it calls on governments to

---

92 U.S., Office of the Director of National Intelligence, *The Review Group* (ODNI), online: < http://www.dni.gov/index.php/intelligence-community/review-group > .

93 President's Review Group on Intelligence and Communications Technologies, *supra* note 4 at 227-229.

94 Bill S 2871, *supra* note 79.

95 U.K., Cabinet Office, Press Release, "Sir Nigel Sheinwald appointed Special Envoy on intelligence and law enforcement data sharing" (19 September 2014), online: < https://www.gov.uk > .

96 *Ibid.*

97 Participants are AOL, Apple, Dropbox, Evernote, Facebook, Google, LinkedIn,

create "a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions, such as improved mutual legal assistance treaty—or 'MLAT'—processes."[98] US-based Internet providers have been issuing increasingly detailed transparency reports to rebuild user trust, particularly in the wake of Edward Snowden's disclosures.[99]

Microsoft has been vocal in its calls for reform of the way in which countries access online data. These calls began with general counsel, Brad Smith, stating that there should be a new multilateral MLA convention.[100] As the *Microsoft Ireland* case has progressed, Smith has been increasingly vociferous.[101] A significant number of Internet companies, telecommunications providers, and industry groups, including Apple, Verizon, Amazon, AT&T, and the Chamber of Commerce of the United States of America have submitted amicus curiae briefs in the *Microsoft Ireland* case, all of which criticize the US government's attempt to access data located abroad by using a US search warrant.[102]

(d) Civil Society Initiatives

The Global Network Initiative (GNI) is:

> [A] multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics dedicated to protecting and advancing freedom of expression and privacy in the Information and Communications Technology (ICT) sector.[103]

The GNI commissioned a report on reforming the MLA process as it applies to requests for online records. The report outlines three main areas of reform:

Microsoft, Twitter, and Yahoo. Reform Government Surveillance, online: <https://www.reformgovernmentsurveillance.com>.

98 *Ibid.*

99 See, e.g., U.S., *Written Testimony of Richard Salgado: Senate Judiciary Subcommittee on Privacy, Technology and the Law: Hearing on 'The Surveillance Transparency Act of 2013'"* 113th Cong. (Washington, D.C.: 2013), online: <www.judiciary.senate.gov/imo/media/doc/11-13-13SalgadoTestimony.pdf>.

100 Smith, *supra* note 66.

101 See Digital Constitution, online: <digitalconstitution.com> for a Microsoft-curated collection of relevant posts and media articles.

102 See, e.g., *Microsoft Corporation v. United States*, No. 14-2985 (2nd Cir., 2014) (Brief for Verizon Communications et al. as Amici Curiae Supporting Appellant); *Microsoft Corporation v. United States*, No. 14-2985 (2nd Cir., 2014) (Brief for AT&T Corporation et al. as Amici Curiae Supporting Appellant); *Microsoft Corporation v. United States*, No. 14-2985 (2nd Cir., 2014) (Brief for Apple Inc. as Amicus Curiae Supporting Appellant).

103 Global Network Initiative, "Data Beyond Borders: Mutual Legal Assistance in the Internet Age," by Andrew K. Woods (Global Network Initiative, 2015) at ii, online: <https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf>.

development of electronic MLA systems; training of international government officials (especially law enforcement officers); and increased staffing for officials who are responsible for responding to MLA requests.[104]

Another civil society initiative is the Necessary and Proportionate Principles. These are 13 principles that are "intended to explain how existing human rights standards and international law applies to the new capabilities and risks of digital surveillance."[105] They have been endorsed by hundreds of organizations from around the world. The Principles include safeguards for international cooperation—that is, "where the laws of more than one state could apply to Communications Surveillance, the available standard with the higher level of protection for individuals is applied." It encourages the requirement of dual criminality and also states that "[m]utual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness."[106]

Yet another notable initiative is the Internet and Jurisdiction Project, which is a not-for-profit project that brings together states, industry, international organizations, civil society, and the technical community. These stakeholders meet regularly to discuss ways to create due process frameworks that accommodate different legal systems.[107] This is a broad initiative which covers all kinds of cross-border legal processes and could have some relevance to cross-border requests in criminal matters.

CONCLUSION

International access to user data for criminal matters from US-based companies is governed by a patchwork of domestic and US laws and policies. As technology has evolved, different patches and workarounds have been developed. This has resulted in a system that is confusing and uncertain, lacks a logical underpinning, and does not meet the needs of users, business, government, or rights advocates.

This article has outlined the existing system in the belief that the first step towards reform is to make sure that there is a clear understanding of the status quo. Too often, it is as though each stakeholder group is describing a different part of the elephant without understanding its relationship to the whole.[108] Any reform efforts need to understand the relationship between each of the different

---

[104] *Ibid.*

[105] International Principles on the Application of Human Rights to Communications Surveillance, "Signatories" (2014), online: < https://en.necessaryandproportionate.org/signatories > .

[106] *Ibid.*

[107] Internet & Jurisdiction Project, "About," online: < www.internetjurisdiction.net > .

[108] Gail Kent, "Sharing Investigation Specific Data with Law Enforcement: An International Approach" (2014) Stanford Public Law Working Paper, online: SSRN < papers.ssrn.com/so13/papers.dfm?abstract_id = 2472413 > .

types of international cooperation and the needs of each of the stakeholders. To this end, advocates for reform should not focus solely on MLAT, but instead need to acknowledge the role of law enforcement cooperation and direct requests to providers.

Comprehensive reform of this issue will require overcoming some of the most difficult and intractable areas of legal policy. The US Congress has shown little ability or inclination to tackle reform of *ECPA*. Despite seemingly broad industry, public, and political support for the notion that government authorities must obtain a search warrant in order to access user content, Congress still has not amended *ECPA* to codify this position. It does not seem likely that Congress will be any faster in addressing the problems with applying *ECPA* to the international context. Moreover, a comprehensive solution to international data sharing issues requires engagement and agreement not only from the US Congress, but also from international governments.

However, there is clearly a growing awareness of the need for the laws to change. The involvement of so many representatives from the Internet industry, journalist groups, privacy organizations, and civil rights advocates in the *Microsoft Ireland* case shows the level of interest and financial investment in this issue. The challenge now is to translate this interest into meaningful and workable change.