EMORY | LAW

Emory Law Journal

Volume 66
Issue 3 *The 2016 Randolph W. Thrower Symposium — Redefined National Security Threats: Tensions and Legal Implications*

Article 5

2017

How Both the EU and the U.S. Are "Stricter" Than Each Other for the Privacy of Government Requests for Information

Peter Swire Swire

DeBrae Kennedy-Mayo

HOW BOTH THE EU AND THE U.S. ARE "STRICTER" THAN EACH OTHER FOR THE PRIVACY OF GOVERNMENT REQUESTS FOR INFORMATION

Peter Swire[*]
DeBrae Kennedy-Mayo[**]

Law enforcement access to personal data presents a paradox at the heart of debates between the European Union (EU) and the United States about privacy protections. On the one hand, the comprehensive privacy regime in the EU contains many requirements that do not apply in the United States—the EU is "stricter" than the United States in applying requirements that do not exist in the latter. On the other hand, the United States also sets requirements that do not exist in the EU, such as the Fourth Amendment requirement that a warrant be signed by a judge upon a finding of probable cause. Thus, both are stricter in important ways when setting standards for law enforcement access to personal data. The fact that both sides are stricter in significant respects is important to two distinct topics: how to reform the system of Mutual Legal Assistance (MLA), and whether the United States provides "adequate" protection for personal data under EU law, and thus is an appropriate destination for data flows from the EU.

The relative strictness of standards for law enforcement access is central to understanding current obstacles to reforming the MLA system, the mechanism for sharing law enforcement evidence held in one country for use in criminal investigations in a different country. Our research team has been writing a series of articles about MLA reform.[1] The topic has become increasingly important in

---

[*] Peter Swire is the Huang Professor of Law and Ethics at the Georgia Institute of Technology's Scheller College of Business, and Senior Counsel at Alston & Bird, LLP. For comments on earlier versions of this work, the authors thank Deven Desai, Daniel Felz, James Harvey, Justin Hemmings, Amie Stepanovich, Suzanne Vergnolle, and Jesse Woo. This article is current as of November 27, 2016.

[**] DeBrae Kennedy-Mayo is a research associate faculty member at the Georgia Institute of Technology's Scheller College of Business. J.D. Emory Law School.

[1] Peter Swire, Justin D. Hemmings & Suzanne Vergnolle, *A Mutual Legal Assistance Case Study: The United States and France*, WIS. INT'L L.J. (forthcoming 2017); Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, N.Y.U. ANN. SURV. AM. L. (forthcoming 2017) (manuscript at 3) [hereinafter Swire & Hemmings, *Mutual Legal Assistance*], http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728478; Peter Swire & Justin Hemmings, *Stakeholders in Reform of the Global System for Mutual Legal Assistance* (Georgia Tech. Scheller College of

recent years—globalized communications mean that e-mails, social network data, and other evidence for criminal investigations are often held in a different country. In the course of studying obstacles to effective reform, we have come to believe that the fact that both the EU and the United States provide stricter privacy protections is salient but little understood—each side is reluctant to compromise on a new approach to the extent that there would be a weakening of some specific safeguards that currently exist in their respective jurisdictions. We hope that a fuller understanding of the relative strictness of both sides will enable a more fruitful discussion of possible paths to MLA reform.

The relative strictness of both the EU and the United States is also important to a second topic, the current litigation and debates about whether the United States provides "adequate" protection of privacy, and thus is a lawful destination for flows of personal data from the EU.[2] Under the EU Data Protection Directive, which went into effect in 1998,[3] transfers of personal data from EU Member States to other countries, such as the United States, are generally permitted only if the recipient jurisdiction has "adequate" protections.[4] From its negotiation in 2000 until 2015, a major legal basis for such transfers was the EU/U.S. Safe Harbor, under which participating companies could lawfully send personal data to the United States.[5] In 2015, the European Court of Justice struck down the Safe Harbor for lacking adequacy in *Schrems v. Data Protection Commissioner*.[6] A related transfer mechanism, the standard contract clause, is now facing a similar legal challenge in Ireland, and the Irish Data Protection Commissioner has preliminarily found the challenge to be "well founded."[7] In

Business, Working Paper No. 2015-32, 2015) [hereinafter Swire & Hemmings, *Stakeholders in Reform*], http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2696163.

[2] *See, e.g.*, Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. I-627.

[3] European Commission, *Analysis and Impact Study on the Implementation of Directive EC 95/46 in Member States*, at 1, http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf (last visited Oct. 19, 2016).

[4] Directive 95/46/EC, of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 25, 26, 1995 O.J. (L 281) 31, 33.

[5] Mark Scott, *Data Transfer Pact Between U.S. and Europe Is Ruled Invalid*, N.Y. TIMES (Oct. 6, 2015), http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html; *see also* Commission Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, No. 2000/520, 2000 O.J. (L 215) 7, 10.

[6] *Schrems*, 2015 E.C.R. at 1.

[7] At the time of this writing, the *Schrems* case is before the Irish High Court. Swire has been engaged as an independent expert in the case, by Facebook, to discuss, among other things, the U.S. surveillance and privacy law issues. Under Irish court rules, Swire is required to provide his independent opinion, and not testify as an advocate for the party that selected him. Rule 57 of the Rules of Procedure of the Superior Courts of Ireland:

addition, the EU has recently approved two instruments that will go into full effect in 2018 and strengthen existing privacy protections: the General Data Protection Regulation (GDPR),[8] which applies predominantly to private-sector processing of personal information, and a new Police and Criminal Justice Directive that governs law enforcement access to personal data.[9] Both the GDPR and law enforcement directive have similar "adequacy" requirements for transfers of personal data.[10] An accurate assessment of the adequacy of U.S. law enforcement access to information is thus vital to multiple aspects of current EU data protection law.

Part I of this Article provides background for both MLA reform and the current adequacy debates. Part II highlights ways that the EU's comprehensive data protection regime creates privacy protections, including for law enforcement access, that are stricter than those applied to the United States. Part III highlights ways the United States has stricter rules governing law enforcement and other government access to information. We introduce the term "plus factors" as a way to highlight how specific provisions of U.S. law and practice provide greater protection than the EU approach. Some of these plus factors are structural, such as the assurances of lawfulness provided by over two centuries of the U.S. independent judiciary and operation of a written constitution of checks and balances. Other plus factors are more specific, such as the probable cause standard and specific provisions of statutes, such as the Electronic Communications Privacy Act (ECPA), which provide higher standards for access to some categories of information than is required in the EU. Part IV focuses on the implications for MLA reform. Based on our study of both the EU and U.S. systems, we believe there are generally effective rule-of-law protections against excessive law enforcement surveillance in both the U.S.

"(1) It is the duty of an expert to assist the Court as to matters within his or her field of expertise. This duty overrides any obligation to any party paying the fee of the expert." Rules of the Superior Courts (Conduct of Trials) 2016, SI 254/2016 (Ir.) r. 57(a).

[8] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1; *Reform of EU Data Protection Rules*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/reform/index_en.htm (last visited Oct. 19, 2016).

[9] Directive 2016/680, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89.

[10] Regulation 2016/679, *supra* note 8, art. 45, at 61 ("A transfer of personal data to a third country . . . may take place where . . . the international organisation in question ensures an adequate level of protection."); *id.* at 19–20 ("The third country should offer guarantees ensuring an adequate level of protection . . . .").

and EU Member States. We therefore conclude that these generally effective safeguards provide a promising basis for MLA reform, even where details of the systems differ and specific safeguards on one side do not have precise counterparts on the other.

I. BACKGROUND ON MUTUAL LEGAL ASSISTANCE REFORM AND THE CURRENT ADEQUACY DEBATES

The first section of this Part describes our ongoing research project into MLA reform and explains the distinctive task of this Article in relation to our previous work. It also describes the new urgency of MLA reform, in light of the Second Circuit's 2016 decision in *Microsoft v. United States* (*Microsoft Ireland*),[11] and the 2016 announcement of proposed legislation to reform the MLA process between the United States and United Kingdom. The second section then provides background on current data protection controversies between the EU and the United States both for new EU legal instruments and in ongoing litigation that quite possibly will reach the European Court of Justice.

A. Why Mutual Legal Assistance Matters Now: The Research Project

This Article is part of a larger research project examining the current state of international MLA and builds upon those previous articles. This section first highlights key findings from our team's previous work on MLA. It next describes the 2016 *Microsoft Ireland* case and the 2016 proposal for a new U.S./U.K. framework for MLA. It concludes by outlining what this Article adds to the overall MLA reform debate.

1. Previous Research Findings

A simple example shows how the globalization of data is affecting even routine criminal investigations. Consider a burglary that takes place in Paris with a French suspect and a French victim. In investigating the crime, French law enforcement find that the suspect was using a U.S.-based e-mail service, and the e-mails can only be retrieved from the relevant e-mail server located in the United States. Under the current regime, to access the e-mails, French law enforcement would need to file a MLAT request with the U.S. Department of Justice (DOJ).[12] The request would need to show "probable cause" of a crime—

[11] 829 F.3d 197 (2d Cir. 2016).

[12] Swire, Hemmings & Vergnolle, *supra* note1 (manuscript at 35).

the U.S. legal standard[13]—despite the crime having no connection to the United States (other than the physical location of an e-mail server). This example shows how MLA issues increasingly arise for routine criminal investigations. The need for MLA requests is even more pervasive for cybercrime, drug smuggling, money laundering, and other categories of crime where the criminal activity itself often crosses borders.

The first article in the research project introduces the international MLA regime,[14] explaining the origins of MLATs and how electronic evidence requests have come to overwhelm these systems.[15] One important source of current challenges is how the increased use of encryption has made many local wiretaps ineffective, pressing law enforcement to seek evidence by alternate means.[16] The article examines the risks of failing to adequately reform the system.[17] It provides a number of potential administrative reforms that could reduce the current average response time of ten months for MLA requests to the United States. The article stresses an innovative way to avoid reliance going forward on mutual legal assistance *treaties*; instead, reform may be more achievable and effective through mutual legal assistance *statutes*.[18] The article is thus entitled, *Mutual Legal Assistance in an Era of Global Communications: The Analogy to the Visa Waiver Program*.[19] The Visa Waiver Program (VWP) was a response to the globalization of travel—for the thirty-eight countries that participate today, individuals can travel to and from the United States without the need for an individualized visa interview.[20] Similarly, a new MLA statute can respond to the globalization of evidence—countries that meet strict standards would use a streamlined system to share evidence for criminal investigations. Since the article was written, the United States and the United Kingdom have announced one such proposal for an MLA statute,[21] consistent in structure with the VWP model supported by our research.

---

13 *Id.* (manuscript at 3).

14 Swire & Hemmings, *Mutual Legal Assistance*, *supra* note1 (manuscript at 3–12).

15 *See id.* (manuscript at 6–16).

16 *See id.* (manuscript at 22–25).

17 *See id.* (manuscript at 27–31).

18 *See id.* (manuscript at 43–45).

19 *Id.* (manuscript at 1).

20 *Id.* (manuscript at 48).

21 Devlin Barrett & Jay Greene, *U.S. to Allow Foreigners to Serve Warrants on U.S. Internet Firms*, WALL ST. J. (July 15, 2016, 8:00 PM), http://www.wsj.com/articles/obama-administration-negotiating-international-data-sharing-agreements-1468619305.

The second article identifies the various stakeholders in this international MLA regime, and their respective incentives and goals for reform.[22] That article, *Stakeholders in Reform of the Global System for Mutual Legal Assistance*, looks to the interests of the U.S. government, non-U.S. governments, technology companies, and public interest groups both in the United States and abroad.[23] The article seeks to accurately describe the interests of these stakeholders to better inform the debate for MLA reform. It identifies major goals of the various actors, notably: (1) effective law enforcement access to evidence; (2) ensuring that such access is achieved consistent with privacy and civil liberty goals; (3) avoiding data localization, which might otherwise result where local law enforcement insists on data being stored locally; and (4) preventing a greater role for the International Telecommunications Union or other institutions that might seek to impose top-down controls, risking splintering of the global Internet.[24]

We have written two articles that examine in detail how the French and U.S. systems compare for MLA purposes. The first, *Understanding the French Criminal Justice System as a Tool for Reforming International Legal Cooperation and Cross-Border Data Requests*,[25] focuses on the procedural differences between the two approaches. For example, the U.S. system clearly separates the judicial and prosecutorial roles, while the French investigating magistrate in many ways combines these roles.[26] The second, *A Mutual Legal Assistance Case Study: The United States and France*,[27] focuses on the substantive standards that apply before law enforcement can gain access to electronic evidence. One important contrast is that the U.S. Electronic Communications Privacy Act (ECPA) and other laws set forth detailed and differing standards for judicial approval of different categories of electronic evidence,[28] while the French approach delegates considerable discretion to the investigating magistrate to decide what evidence should be gathered.[29] This comparison of the French and U.S. legal systems, in turn, informs this Article's

---

[22] Swire & Hemmings, *Stakeholders in Reform*, *supra* note 1.

[23] *Id.* at 1–16.

[24] *Id.*

[25] Suzanne Vergnolle, *Understanding the French Criminal Justice System as a Tool for Reforming International Legal Cooperation and Cross-Border Data Requests*, *in* DATA PROTECTION, PRIVACY, AND EUROPEAN REGULATION IN THE DIGITAL AGE (Tobias Bräutigam & Samuli Miettinen eds., 2016).

[26] *Id.* (manuscript at 6–7).

[27] Swire, Hemmings & Vergnolle, *supra* note1.

[28] *Id.* (manuscript at 7–20).

[29] *Id.* (manuscript at 20–34).

broader comparison of EU and U.S. rules governing law enforcement access to information.

2. The Microsoft Ireland *Case and the Proposed U.S./U.K. MLA Agreement*

In July 2016, the U.S. Court of Appeals for the Second Circuit ruled in *Microsoft Ireland* that the Stored Communications Act did not apply "extraterritorially," meaning that a search warrant issued to a company to seize the contents of an e-mail account did not require that company to provide electronic evidence that was stored outside of the United States.[30] This interpretation, that a search warrant could not compel production of electronic evidence held by a U.S. company outside the United States, surprised some commentators.[31] The government had contended that search warrants could apply similarly to subpoenas from the federal government.[32] In cases such as *Bank of Nova Scotia*, the government had successfully used subpoenas to require companies to produce all financial or other data held by the company, regardless of where in the world the information was stored.[33]

Until the *Microsoft Ireland* case (so called because the evidence at issue was housed by Microsoft in Ireland), the United States had received far more MLA requests than it had requested from other countries.[34] Leading e-mail and social network services have been based in the United States, so the U.S. government could rely on the existence of U.S. headquarters to gain evidence in law enforcement investigations. By contrast, other governments have had to meet the requirements of U.S. law, such as ECPA, to gain access to e-mail, social network, or other electronic evidence held by these companies. Other countries aside from the United States have thus needed to use the MLA process, and so had to meet probable cause or other U.S.-defined standards for gaining the evidence. In the wake of *Microsoft Ireland*, the U.S. government appears to have a far greater reason to support MLA reform—to gain evidence from Ireland and other countries where relevant data is stored.

Even before the *Microsoft Ireland* decision, the DOJ was exploring legislation, consistent with the VWP model, to streamline MLA requests. In

---

30 829 F.3d 197, 220 (2d Cir. 2016).

31 Jennifer Granick, *The Microsoft Ireland Case and the Future of Digital Privacy*, JUST SECURITY BLOG (July 18, 2016, 12:46 PM), https://www.justsecurity.org/32076/microsoft-ireland-case-future-digital-privacy/.

32 *Microsoft*, 829 F.3d at 220–21.

33 740 F.2d 817, 826–29 (11th Cir. 1984).

34 Telephone Interviews with Anonymous Department of Justice and National Security Council Officials (Mar.–Apr. 2015).

February 2016, the United Kingdom and the United States announced the outline of an agreement that would act as an alternative to the MLAT process in place.[35] As drafted, it would enable U.K. officials in some circumstances to send direct requests to U.S. companies for data held in the United States, both for stored data and for real-time wiretaps or other access to communications for investigation.[36] Further details of the proposed legislation emerged soon after the *Microsoft Ireland* decision.[37] The proposal would amend portions of the wiretap laws, the Stored Communications Act, and the Pen/Trap Statute.[38] It would allow the United States to enter into reciprocal agreements with other countries to enhance the DOJ's ability to obtain electronic evidence abroad.[39] The proposal, as presently drafted, attempts to carve out those individuals and situations of greatest Fourth Amendment concern—data pertaining to a U.S. citizen or legal permanent resident (wherever they are located) and persons located within the United States, regardless of their nationality. In response to the proposal, some U.S. civil society groups have expressed serious reservations.[40] Professors Jennifer Daskal and Andrew Woods have provided a cautiously optimistic review of the proposed approach, if sufficient privacy and civil liberties safeguards are included.[41]

---

[35] Ellen Nakashima & Andrea Peterson, *The British Want to Come to America—with Wiretap Orders and Search Warrants*, WASH. POST (Feb. 4, 2016), https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america—with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html.

[36] *Id.*

[37] Letter from Peter J. Kadzik, Assistant Attorney General, U.S. Dep't of Justice, to Joseph R. Biden, President of the United States Senate (July 15, 2016), https://www.aclu.org/sites/default/files/field_document/doj_legislative_proposal.pdf.

[38] *Id.*

[39] Jonathan B. New, Patrick T. Campbell & David M. McMillan, *DOJ Responds to 'Microsoft Ireland' Decision with Proposed Legislation and Bilateral Agreements Allowing Cross-Border Data Searches*, BAKERHOSTETLER (July 29, 2016), https://www.bakerlaw.com/mobile/alerts/doj-responds-to-microsoft-ireland-decision-with-proposed-legislation-and-bilateral-agreements-allowing-cross-border-data-searches.

[40] They argue that the new agreement between the United States and the United Kingdom concerning mutual legal assistance, "if finalized and approved, would 'lower the human rights protections for accessing private information of Internet users and give the U.K. unprecedented new authority to act extraterritorially without adequate oversight.'" Eric Geller, *British Police Want to Be Able to Serve Warrants Directly to U.S. Tech Companies*, DAILY DOT (Feb. 5, 2016, 4:57 PM), http://www.dailydot.com/layer8/uk-wiretaps-warrants-us-companies-negotiations. "This deal as reported would not require the U.K. to heighten its standards to meet ours in the U.S., or even to meet the basic requirements of human rights law . . . ." *Id.*

[41] Jennifer Daskal, *A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right*, JUST SECURITY BLOG (Feb. 8, 2016, 8:10 AM), https://www.justsecurity.org/29203/british-searches-america-tremendoUS-opportunity/; *see also* Jennifer Daskal & Andrew K. Woods, *Cross-Border Data Requests: A Proposed Framework*, JUST SECURITY BLOG (Nov. 24, 2015, 8:03 AM), https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/.

The negotiations between the United States and the United Kingdom highlight the growing importance of MLA reform in the wake of *Microsoft Ireland*, and the interest of the U.S. government in providing accelerated data sharing mechanisms, at least for its close allies. We are pleased to see the U.S. government taking steps to address MLA reform, and Swire has met with the DOJ and other government officials to provide our questions and concerns about the draft agreement. We are cautiously supportive of the VWP approach, if appropriate civil liberties safeguards are included in the final drafting.

3. The Role of This Article for MLA Reform Debates

Swire has been convinced of the increasing importance of MLA issues at least since his participation in President Obama's Review Group on Intelligence and Communications Technology in 2013, which supported a number of MLA reforms.[42] As part of efforts to further MLA reform, our research team has chaired and participated in a variety of stakeholder meetings on the topic. This Article reflects five statements that we have come to believe in the course of our efforts:

1. Both the United States and the EU are stricter in some respects in the limits that they set on government access to evidence for law enforcement purposes.

2. Participants in the debates often have a weak understanding of the relative strengths and weaknesses of the U.S. and EU legal systems in this area. Some EU participants are skeptical that effective privacy safeguards exist at all in the United States. Some U.S participants are skeptical of non-U.S. legal systems, especially with respect to the probable cause standard and First Amendment protections.

3. Stakeholders in both the United States and EU are noticeably reluctant to agree to any weakening of specific, familiar safeguards that exist in their own legal system.

4. Although each side is stricter in some respects and less strict in others, we believe that there are generally effective rule-of-law protections

[42] LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY (Dec. 12, 2013) [hereinafter REVIEW GROUP REPORT], https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

against excessive law enforcement surveillance in both the U.S. and EU Member States.

5. These generally effective safeguards provide a promising basis for MLA reform along the lines of the VWP model, even where details of the systems differ and specific safeguards on one side do not have precise counterparts on the other.

This Article provides research and discussion to support these five statements. By providing details about the relative strictness of the two systems, the Article seeks to correct misunderstandings and provide a more informed basis for further discussions of possible reform. Part IV of this Article also examines likely consequences if MLA reform is blocked. As will be discussed, in the absence of reform, we are likely to see diminution in privacy and civil liberties protections, increased pressure for counter-productive data localization proposals, and increased pressure for countries to deploy extraterritorial methods for gaining access to evidence.

B. The Importance of the Relative Strictness of Protections to Broader EU/U.S. Data Protection Issues

Along with MLA reform, studying the relative strictness of the EU and United States is important to a second topic: the current litigation and debates about whether the United States provides "adequate" protection of privacy and thus is a lawful destination for flows of personal data from the EU.

Under the EU Data Protection Directive, which went into effect in 1998, transfers of personal data from EU Member States to other countries such as the United States are generally permitted only if the recipient jurisdiction has "adequate" protections.[43] From the time it was negotiated in 2000 until 2015, a major legal basis for such transfers was the EU/U.S. Safe Harbor, under which participating companies could lawfully send personal data to the United States.[44] In 2015, the European Court of Justice struck down the Safe Harbor for lacking adequacy in *Schrems v. Data Protection Commissioner*.[45] One of the concerns expressed by the European Court of Justice was that U.S. government

[43] Directive 95/46/EC, *supra* note 4, at 36–37.

[44] *See* MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RESEARCH SERV., R44257, US-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD (2016); Commission Decision, *supra* note 5 (determining that Safe Harbor provided adequate protection for the transfer of data to the United States).

[45] Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 1, 26.

surveillance was so pervasive that the data of EU citizens was not safe once it was in the United States.[46] A related transfer mechanism, standard contract clauses, is now facing a similar legal challenge in Ireland, and the Irish Data Protection Commissioner has preliminarily found the challenge to be "well-founded."[47]

The issue of whether the United States has "adequate" protections also arises under two instruments that go into full effect in 2018 and strengthen existing privacy protections. The GDPR[48] applies predominantly to private-sector processing of personal information,[49] and a new Directive governs law enforcement access to personal data.[50] An accurate assessment of the adequacy of U.S. law enforcement access to information is thus vital to multiple aspects of current EU data protection law.

Going forward, the crux of the concern is that if the European legal regime makes a firm finding that the United States lacks an adequate legal order, then transfers of personal data may be essentially blocked. Such a blockage would affect large portions of trans-Atlantic commerce and communication. In light of the high stakes, it is important to develop an accurate and detailed understanding of the relative strengths and weaknesses of both the U.S. and EU systems for

---

[46] *Id.* at 23.

[47] Mary Carolan, *Data Protection Groups Seek to Join Key High Court Case*, IRISH TIMES (July 17, 2016, 1:07 PM), http://www.irishtimes.com/news/crime-and-law/courts/high-court/data-protection-groups-seek-to-join-key-high-court-case-1.2688868; Explanatory Memorandum from the Data Prot. Comm'r on Update on Litigation Involving Facebook and Maximilian Schrems (Sept. 28, 2016), https://www.dataprotection.ie/docs/28-9-2016-Explanatory-memo-on-litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm; *see also* Jedidiah Bracy, *Model Clauses in Jeopardy with Irish DPA Referral to CJEU*, IAPP (May 25, 2016), https://iapp.org/news/a/model-clauses-in-jeopardy-with-irish-dpa-referral-to-cjeu/; Mary Carolan, *Schrems and Facebook Privacy Case: Next Round Set for February*, IRISH TIMES (July 25, 2016, 4:55 PM), http://www.irishtimes.com/business/technology/schrems-and-facebook-privacy-case-next-round-set-for-february-1.2733961; Julia Fioretti & Conor Humphries, *Irish Privacy Watchdog Refers Facebook's U.S. Data Transfers to EU Court*, REUTERS (May 25, 2016, 12:41 PM), http://www.reuters.com/article/US-eu-privacy-facebook-idUSKCN0YG2DL; Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, at 3 n.5 (Georgia Inst. of Tech. Scheller College of Bus. Res. Paper No. 36, 2015) [hereinafter *US Surveillance Law*], http://ssrn.com/abstract=2709619. This document was submitted as a White Paper to the Belgian Privacy Authority at its request for its Forum on "The Consequences of the Judgment in the *Schrems* Case."

[48] Regulation 2016/679, *supra* note 8; *see also* Jan Dhont, Delphine Charlot & Jon Filipek, *The EU General Data Protection Regulation—Europe Adopts Single Set of Privacy Rules*, ALSTON & BIRD: PRIVACY & SECURITY BLOG (Dec. 16, 2015), http://www.alstonprivacy.com/the-eu-general-data-protection-regulation-europe-adopts-single-set-of-privacy-rules/.

[49] Regulation 2016/679, *supra* note 8, at 3. In addition to applying to private-sector processing of information, the GDPR applies to non-national security and non-law enforcement processing by public agencies. *See* Dhont, Charlot & Filipek, *supra* note 48.

[50] Directive 2016/680, *supra* note 9.

regulating government access to personal data. The next two Parts take up this task.

II. WAYS IN WHICH THE EU IS MORE PRIVACY PROTECTIVE THAN THE UNITED STATES

Since promulgation of its Data Protection Directive in 1995, the EU has taken a comprehensive approach to privacy protection, with an emphasis on business access to information. Part A summarizes main components of the EU approach. Part B then briefly discusses three recent areas where the United States has agreed to privacy changes to bring the two systems more closely together: the Judicial Redress Act, Umbrella Agreement, and Privacy Shield.

A. EU Privacy Approach

In the EU, privacy protections for data include a comprehensive approach, the Data Protection Directive, and, in the near future, the GDPR. In 2015, the *Schrems* case struck down the Safe Harbor between the EU and the United States.[51] A pending case in Ireland, which could then be appealed to the European Court of Justice, is expected to determine whether standard contract clauses will continue to be a legitimate basis for data transfers between the EU and the United States. Legal challenges have also been filed against the Privacy Shield.[52]

1. The EU Takes a Comprehensive and Fundamental Rights Approach to Privacy and Data Protection

"Europe has seen the gradual spread of privacy legislation since the German state of Hesse enacted the first data protection statute in 1970."[53] Since the 1990s, European data protection laws generally had four features:

1) "typically they apply to both public and private sectors;"[54]

---

[51] *Schrems*, 2015 E.C.R. at 1, 26.

[52] Natasha Lomas, *EU-US Privacy Shield Data Transfer Deal Faces Legal Challenge*, TECHCRUNCH (Oct. 27, 2016), https://techcrunch.com/2016/10/27/eu-us-privacy-shield-data-transfer-deal-faces-legal-challenge/; Peter Sayer, *A Second Privacy Shield Legal Challenge Increases Threat to EU-US Data Flows*, COMPUTERWORLD (Nov. 3, 2016, 5:17 AM), http://www.computerworld.com/article/3138405/data-privacy/a-second-privacy-shield-legal-challenge-increases-threat-to-eu-us-data-flows.html.

[53] PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 22 (1998).

[54] FRED H. CATE, PRIVACY IN THE INFORMATION AGE 32–33 (1997).

2) "they apply to a wide range of activities, including data collection, storage, use, and dissemination;"[55]

3) "they impose affirmative obligations (often including registration with national authorities) of anyone wishing to engage in any of these activities; and"[56]

4) "they have few, if any, sectoral limitations—they apply without regard to the subject of the data."[57]

As a matter of fundamental rights, these concepts were incorporated into Article 8 of the European Convention of Human Rights, which provides: "Everyone has the right to respect for his private and family life, his home and his correspondence."[58] Article 8 contains limitations that are "necessary in a democratic society" for purposes such as "the interests of national security" and "the prevention of disorder or crime."[59] The seminal document of the European Union, the 2009 Lisbon Treaty, explicitly applies these protections to personal data in Article 16: "Everyone has the right to the protection of personal data concerning them."[60] Article 7 of the Charter of Fundamental Rights of the European Union echoes the protection of private and family life,[61] and Article 8 protects personal data.[62] According to Article 52 of the Charter, any limitation to the rights must be subject to the principle of proportionality and only made if necessary to "genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."[63]

2. Data Protection Directive

The Data Protection Directive, promulgated in 1995 and in effect since 1998, provides the legal structure for data protection in the EU.[64] The Directive

---

55 *Id.*

56 *Id.*

57 *Id.* at 33.

58 Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, http://www.echr.coe.int/Documents/Convention_ENG.pdf.

59 *Id.*

60 *See* Consolidated Version of the Treaty on the Functioning of the European Union, art. 16, Oct. 26, 2012, 2012 O.J. (C 326) 47 [hereinafter TFEU].

61 Charter of Fundamental Rights of the European Union, art. 7, 2012 O.J. (C 326) 391, 397.

62 *Id.* art. 8.

63 *Id.* art. 52(1).

64 Prior to the adoption of TFEU, the Economic Community adopted data protection rules under the 1995 Economic Community Treaty's clause that allowed for the harmonization of internal markets. *See* Treaty Establishing the European Community, art. 95, Nov. 10, 1997, O.J. (C 340) 173 (as in effect 1995) (now TFEU art. 100(a)).

imposes requirements on any person who collects or processes data pertaining to individuals. These requirements include protections related to:

- *Fairness and lawfulness:* The processing of the data is required to be fair and lawful for a legitimate purpose. The data may not be kept longer than necessary.[65]

- *Purpose limitation:* Data must be collected for a specific purpose.[66] Once obtained, the data cannot be additionally processed in a way that is incompatible with the purpose initiating the collection of the data.[67]

- *Proportionality:* The means employed to process the data must be reasonably likely to achieve the stated objectives. The adverse consequences of the processing must be justified in light of the importance of the stated objective.[68]

- *Processing:* To obtain data about a particular person, the individual[69] whose data is involved must unambiguously consent to the collection or another legitimate basis for the collection must exist.[70] Once obtained, the data cannot be additionally processed in a way that is incompatible with the purpose initiating the collection of the data.[71]

- *Transparency:* The holder of the data should keep the data subjects informed about how their data is being used, both in instances when the data is obtained directly from the individual and when it is obtained indirectly.[72]

- *Notice:* The holder of the data must inform the Data Protection Authority before carrying out any automated processing of personal information.[73]

---

65 Directive 95/46/EC, *supra* note 4, art. 6(1)(a)–(b), (e).

66 *Id.* art. 6(1)(b).

67 *Id.* Exceptions exist such as for processing data for "historical, statistical, or scientific purposes" provided that appropriate safeguards are in place for the data processing. *Id.*

68 *Id.* art. 6(1)(c)

69 Individuals are referred to as "data subjects." *Id.* art. 2(a).

70 *Id.* art. 7. These bases include performance of a contract to which the individual is a party; a legal obligation of the controller; protection of a "vital interest" of the individual; part of an action carried out for the "public interest;" or purposes carried out by the controller or a third party for a "legitimate interest." *Id.*

71 *Id.*

72 *See id.* art. 11–12.

73 *Id.* art. 18(1).

- *Access:* An individual has a right to learn whether data have been collected regarding the person, whether those data have been processed, and to whom the data have been made available.[74]

- *Rectification, Erasure, and Blocking:* An individual has the right to "rectification," "erasure," and "blocking" of data that were not handled in accordance with the law, as well as to ensure notification of these actions to the third parties who gained access to this data.[75]

- *Automated decisions:* The individual has a right to prevent automated decisions about the individual from being made.[76]

- *Sensitive data:* Stricter rules govern the processing of sensitive data that reveal racial or ethnic origin, political opinions, trade-union membership, religious beliefs, or data concerning health or sex life.[77]

- *Right to Object:* The individual's right to object to the processing of her data is a central component of the European legal framework and encompasses the concept that an individual has a right to informational self-determination.[78]

Under the Data Protection Directive, Member States may place restrictions on these rights "when such a restriction constitutes a necessary measure[] to safeguard" national security, defense, public security, the investigation or prosecution of criminal offenses, or an important economic interest of the Member State.[79]

Under the E-Privacy Directive of 2002, Member States are required to ensure the confidentiality of communications.[80] The Directive particularly prohibits "listening, tapping, storage or other kinds of interception or surveillance."[81] Exceptions apply when "necessary, appropriate and proportionate . . . within a democratic society to safeguard national security (i.e. State security), defence,

---

74 Directive 95/46/EC, *supra* note 4, art. 12.

75 *Id.*

76 *See id.* art. 15. The right does not extend to automated processing, but is limited to automated decisions. *Id.*

77 *See id.* art. 8. GDPR further tightens these restrictions. *See* Dhont, Charlot & Filipek, *supra* note 48.

78 Directive 95/46/EC, *supra* note 4, at art. 14.

79 *Id.* art. 13.

80 Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), art. 5(1), 2002 O.J. (L 201) 37, 43.

81 *Id.*

public security, and the prevention, investigation, detection and prosecution of criminal offenses."[82]

To ensure protection of these rights, each Member State must establish a Data Protection Authority (DPA), with powers including: (1) the power to investigate; (2) the power to intervene, including the power to order blocking, erasure, or destruction of data; and (3) the power to engage in legal proceedings when rules or regulations are violated.[83] The Data Protection Directive created the Article 29 Working Party, comprised of representatives of DPAs, to provide guidance on data protection issues.[84]

The Data Protection Directive sets out a number of legal bases for international data transfers.[85] Under Article 25, personal data can be transferred to a non-EU country if that country ensures an adequate level of protection.[86] Due to its lack of comprehensive privacy legislation, the United States has not qualified for a finding that it generally provides adequate protections.[87] Article 26 authorizes other legal bases for international data transfers, including standard contract clauses, binding corporate rules, and, until it was struck down, the Safe Harbor agreement.[88]

3. GDPR and Police and Criminal Justice Authorities Directive

In 2016, the EU completed the GDPR, which takes effect in 2018 and will replace the Data Protection Directive.[89] Key new provisions of the GDPR address: (1) notification of security breaches; (2) new requirements for processors (contractors who act on behalf of data controllers); (3) liability for damages; (4) designation of data protection officers; (5) international data transfers; (6) accountability obligations; (7) cross-border processing; and (8)

---

[82] *Id.* art. 15.

[83] Directive 95/46/EC, *supra* note 4, art. 28; *see also* Charter, *supra* note 61, art. 8(3); TFEU, *supra* note 60, art. 16(3) ("Compliance with these rules shall be subject to the control of independent authorities.").

[84] Directive 95/46/EC, *supra* note 4, art. 29.

[85] CHRISTOPHER KUNER, EUROPEAN DATA PRIVACY LAW AND ONLINE BUSINESS 124 (2003).

[86] SWIRE & LITAN, *supra* note 53, at 24.

[87] Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 1.

[88] European Commission, *Model Contracts for the Transfer of Personal Data to Third Countries*, EUROPA, http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last updated Nov. 24, 2016).

[89] European Commission, *Reform of EU Data Protection Rules*, EUROPA, http://ec.europa.eu/Justice/data-protection/reform/index_en.htm (last updated Nov. 24, 2016).

sanctions of up to four percent of worldwide revenues.[90] The GDPR provides extensions of individual rights, including the right to be forgotten, the right to data portability, and implementation of principles of data protection by design and data protection by default.[91]

Along with the GDPR, the EU in 2016 promulgated the Police and Criminal Justice Authorities Directive, which will apply to the processing of personal data for law enforcement purposes.[92] This Directive does not directly govern the actions of the Member States the way the GDPR does,[93]and the European Data Protection Supervisor in 2012 criticized an earlier, but similar, version of the Directive for not providing sufficient protections.[94] Article 35 of the Directive contains an adequacy requirement similar in structure to the Data Protection Directive and GDPR.[95] This Directive also takes full effect in 2018.[96]

4. Schrems v. Data Protection Commissioner *Litigation*

As discussed above, the European Court of Justice in October 2015 struck down the EU/U.S. Safe Harbor as lacking adequate protections for the personal data of EU citizens when data is transferred to the United States.[97] This decision in the litigation between Austrian privacy advocate Max Schrems and Facebook Ireland led to the negotiations of the EU/U.S. Privacy Shield, finalized in 2016. Follow-on litigation continues in Ireland, where the Data Protection Commissioner has made an initial finding that similar concerns about adequacy apply to standard contract clauses—an important alternative method for transferring personal data out of the EU to countries that lack a general adequacy finding. The case has been referred for trial by the Irish High Court, scheduled for February 2017.[98]

---

[90] Dhont, Charlot & Filipek, *supra* note 48; *Guidance: What to Expect and When*, ICO., https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/ (last visited Oct. 25, 2016) (discussing the potential future effect of the GDPR on the U.K. after Brexit).

[91] VĚRA JOUROVÁ, HOW DOES THE DATA PROTECTION REFORM STRENGTHEN CITIZENS' RIGHTS? (2016).

[92] *See* Directive 2016/680, *supra* note 9.

[93] *Id.*

[94] Peter Hustinx, then European Data Protection Supervisor, said he was "seriously disappointed with the proposed Directive . . . in the law enforcement area." European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Data Protection Reform Package* 4 (Mar. 7, 2012), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf.

[95] *See* Directive 2016/680, *supra* note 9, art. 35, at 120.

[96] *Id.* art. 63, at 130.

[97] Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 1, 26.

[98] *See* Carolan, *supra* note 47.

B. U.S.-EU Negotiations About Increasing U.S. Privacy Protections

As part of ongoing negotiations between the EU and United States, the United States has agreed to a number of privacy protections, especially in the wake of the European Court of Justice's *Schrems* decision. We briefly examine three reforms, which address EU concerns that U.S. privacy protections—including law enforcement access to data—have not been sufficiently strict: (1) the Judicial Redress Act; (2) the "Umbrella Agreement" for law enforcement sharing and use; and (3) the Privacy Shield.

1. Judicial Redress Act

One longstanding EU privacy concern has been that the U.S. Privacy Act of 1974 provided judicial remedies for U.S. persons (U.S. citizens and legal permanent residents) but not to others, such as EU citizens who lived outside of the United States.[99] The Privacy Act has provided U.S. persons with the right to bring claims against the federal government for damages due to inappropriate disclosure by the government of information that it held, in addition to rights to access and correct individuals' government records.[100] In February 2016, the United States enacted the Judicial Redress Act, which can extend privacy protections and remedies available under the Privacy Act to persons from qualifying countries outside of the United States.[101]

2. Umbrella Agreement

In June 2016, the United States and the EU concluded negotiation of the "Umbrella Agreement," providing a data protection framework for personal data exchanged between the United States and the EU for the prevention, detection, investigation, and prosecution of crimes for law enforcement purposes.[102] The

---

[99] European Commission Memorandum MEMO/15/5612, Questions and Answers on the EU-US Data Protection "Umbrella Agreement" (Sept. 8, 2015) [hereinafter European Commission Memorandum]; Mary Ellen Callahan, Nancy Libin & Lindsey Bowen, *Will the Judicial Redress Act Address Europeans' Privacy Concerns?*, JENNER & BLOCK (Mar. 2, 2016), https://jenner.com/system/assets/publications/14908/original/MEC_Libin_Bowen_IAPP_March_2016.pdf?1457973439.

[100] 5 U.S.C. § 552a(g)(1) (2012).

[101] Judicial Redress Act of 2015, H.R. 1428, 114th Cong. (2016) (enacted). The language of the law extends the protections to qualifying non-U.S. individuals of covered countries. *Id.* at § 2. Covered countries are designated by the agreement of the Attorney General, Secretary of State, Secretary of Treasury, and Secretary of Homeland Security. *Id.* § 2(d). At the time of this writing in late 2016, no countries have yet qualified.

[102] Council of Europe Press Release 305/16, Enhanced Data Protection Rights for EU Citizens in Law Enforcement Cooperation: EU and U.S. Sign "Umbrella Agreement" (June 2, 2016).

agreement specifically includes terrorism within the crimes it covers.[103] With regard to the framework, the Umbrella Agreement focuses on the following: (1) limiting the usage of data to that related to addressing criminal activity; (2) restricting onward transfer of the data to instances where prior consent is obtained from the country that initially provided the data; (3) requiring retention periods for the data obtained to be made public; and (4) providing the individual to whom the data refers the right to access and rectify inaccuracies.[104] The Umbrella Agreement does not authorize data transfers, but does provide agreed upon safeguards for data shared for law enforcement purposes, addressing prior EU concerns about the lack of agreed upon safeguards.[105]

3. Privacy Shield

In July 2016, the European Commission adopted the EU-U.S. Privacy Shield. The agreement sets forth commitments that qualify for adequacy by U.S. companies, detailed explanations of U.S. laws, and commitments by U.S. authorities. U.S. companies wishing to import personal data from Europe under the Privacy Shield accept obligations on how that data can be used, and those commitments are legally binding and enforceable.[106] The U.S. government, through the DOJ and the Office of the Director of National Intelligence, assures that access for law enforcement and national security purposes is subject to safeguards and oversight mechanisms, with the addition of an ombudsman who will follow up on complaints and inquiries by EU individuals.[107] EU individuals who believe that their data have been misused will have several avenues of

---

[103] Press Release, Department of Justice, Joint EU-U.S. Press Statement Following the EU-U.S. Justice and Home Affairs Ministerial Meeting (June 2, 2016); European Commission Memorandum, *supra* note 99. National security surveillance programs that involve data transfers are specifically excluded from the Umbrella Agreement. Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, art. 3, 10, 16, https://epic.org/privacy/intl/data-agreement/Umbrella-Agreement-EU-Release.pdf.

[104] *Transatlantic Data Flows: Restoring Trust Through Strong Safeguards*, at 13, COM (2016) 117 final (Feb. 29, 2016) [hereinafter *Transatlantic Data Flows*].

[105] *Id.* at 8.

[106] *Id.* at 9. Lothar Determann has asserted that the EU should consider making the reach of the Privacy Shield "bidirectional" with the "more effective, specific and up-to-date US privacy laws" applying in Europe. Lothar Determann, *Adequacy of Data Protection in the USA: Myths and Facts*, 6 INT'L DATA PRIVACY L. 244, 250 (2016). His contention is that data protection laws in continental Europe have "a 45-year history and always contemplated damages, fines, and even imprisonment. But in practice there are only a few and only recent examples of actual enforcement of data protection laws in Europe." *Id.* at 245.

[107] *See Transatlantic Data Flows*, *supra* note 104, at 9.

redress, including cost-free alternative dispute resolution.[108] Companies transferring human resources data from Europe will be subject to the decisions of the relevant EU DPA.[109] The DPA will be provided a formal procedure to refer complaints to the U.S. Department of Commerce or the U.S. Federal Trade Commission. The Privacy Shield is scheduled to undergo annual joint reviews by the European Commission and the U.S. Department of Commerce.[110] European regulators have announced they will not challenge the Privacy Shield at least until its first annual review, scheduled for 2017.[111]

In sum, the comprehensive EU privacy laws provide numerous protections that are not explicitly included in U.S. law; nonetheless scholars such as Kenneth Bamberger and Deirdre Mulligan have found that U.S. corporate practice "on the ground" compares favorably to EU practice, and often provides more effective privacy protections than found in many EU countries.[112] In addition, in ways that narrow the legal gaps between the EU and United States, recent intensive negotiations between EU and U.S. officials have led to significant U.S. reforms to address EU concerns, notably for issues of government collection and use of data under the Judicial Redress Act, the Umbrella Agreement, and the Privacy Shield.

III. "PLUS FACTORS": WAYS IN WHICH U.S. LAW IS MORE PRIVACY PROTECTIVE THAN EU LAW

The United States has a complex legal regime that protects privacy in numerous ways relevant to government access to personal information. The discussion here highlights what we call "plus factors"—ways in which U.S. privacy protections reasonably can be considered at least as strict or stricter than EU privacy protections. For purposes of MLA reform, these plus factors are important because, as discussed in Part IV, the stricter U.S. provisions can create obstacles to reform due to U.S. stakeholders' reluctance to weaken the standards. For other purposes, such as EU assessment of the lawfulness of transferring personal data to the United States, the plus factors are also significant. In

---

108 European Commission Press Release IP/16/2461, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016).

109 *See Transatlantic Data Flows*, *supra* note 104, at 10.

110 *Id.*

111 Aaron Souppouris, *EU Will Watch Privacy Shield for a Year Before Challenging*, ENGADGET (July 27, 2016), https://www.engadget.com/2016/07/27/eu-data-protection-privacy-shield-annual-review/.

112 *See* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 173–74 (2015).

assessing the overall adequacy of U.S. safeguards, we believe it is rational to give credit for ways in which the U.S. system provides equivalent or greater protection. If adequacy determinations omit the privacy-protective effects of the plus factors, then the determination may find lack of adequacy based on relatively minor omissions from the European list of privacy protections, without giving corresponding weight to significant privacy protections that apply in the United States but not the EU.

The discussion here focuses on two types of plus factors: (1) structural protections in U.S. law against excessive surveillance and (2) limits on government access to information for law enforcement purposes. We also briefly discuss legal limits on foreign intelligence investigations, but do not give a complete account of those because MLA predominantly applies to law enforcement rather than intelligence investigations.[113]

A. Structural Protections Against Excessive Surveillance

Numerous safeguards concerning government access to information arise from the structure of government in the United States, as a constitutional democracy under the rule of law. In 2015 testimony for the Belgian Privacy Commission, Swire provided an extensive discussion for a European audience of how these safeguards operate.[114] Although often taken for granted by U.S. lawyers, many relevant features of U.S. law are different than European civil law systems, or even from common law jurisdictions such as the United Kingdom that lack centuries of a written constitution interpreted by an independent judiciary that is binding on the legislative and executive branches.

The architecture of the U.S. government is designed to restrain the power of government and to ensure individual rights and freedoms, including privacy

---

[113] MLATs address sharing of information for law enforcement purposes. The EU-U.S. MLAT, as with other MLATs such as U.S.-France, explicitly state that they do not apply to foreign intelligence investigations. Mutual Legal Assistance Treaty Between the United States of America and the European Union, EU-U.S., June 25, 2003, T.I.A.S. No. 10-201.1, art. 1, http://www.state.gov/documents/organization/180815.pdf; Mutual Legal Assistance Treaty Between the United States of America and France, Fr.-U.S., Dec. 10, 1998, T.I.A.S. No. 13010, art. 1, http://www.state.gov/documents/organization/121413.pdf. Nonetheless, some criminal investigations overlap with foreign intelligence investigations, so that evidence shared for the former may be used for foreign intelligence purposes; for example, an anti-terrorism investigation may qualify as "law enforcement," such as investigation into a terrorist attack, but also gather evidence for national security purposes such as combatting the terrorist group abroad.

[114] PETER SWIRE FOR THE BELGIAN PRIVACY AUTHORITY, US SURVEILLANCE LAW, SAFE HARBOR, AND REFORMS SINCE 2013 (2015), https://fpf.org/wp-content/uploads/2015/12/Schrems-White-Paper-12-18-2015.pdf.

rights such as limits on searches and seizures. These structural protections include: (1) a time-tested system of checks and balances; (2) judicial independence; (3) constitutional protections of individual rights; and (4) democratic accountability.

1. A Time-Tested System of Checks and Balances

The U.S. Constitution created a time-tested system of checks and balances among the three branches of government. The separation of powers among the legislative, executive, and judicial branches matches the views of Montesquieu in his 1748 treatise on "The Spirit of Laws"—divided power among the three branches protects "liberty" and guards against "tyrannical" uses of power.[115] The U.S. Constitution provides detailed checks and balances among the three branches, as set forth in Article I (legislative branch), Article II (executive branch), and Article III (judicial branch).

Compared to EU Member States, the U.S. Constitution has been in continuous operation since 1790, far longer than most Member States. In contrast to some recently admitted Member States, where there have been questions about the effective protection of constitutional rights and the rule of law,[116] the U.S. constitutional system of checks and balances has been enduring and remains in vigorous effect today.

2. Judicial Independence

The judiciary is a separate branch of government in the United States, established by Article III of the Constitution.[117] Federal judges are nominated by the President and confirmed by the Senate.[118] The independence of federal

---

[115] MONTESQUIEU, COMPLETE WORKS VOL. I BOOK XI 199 (London 1777) ("When legislative and executive powers are united in the same person, or in the same body of magistrates, there can be no liberty; because apprehensions may arise, lest the same monarch or senate should enact tyrannical laws, to execute them in a tyrannical manner. Again, there is no liberty if the judiciary power be not separated from the legislative and executive. Were it joined with the legislative, the life and liberty of the subject would be exposed to arbitrary controul; for the judge would be then the legislator. Were it joined to the executive power, the judge might behave with violence and oppression. There would be an end of every thing, were the same man, or the same body, whether of the nobles or of the people, to exercise those three powers, that of enacting laws, that of executing the public resolutions, and of trying the causes of individuals.").

[116] European Commission Press Release IP/16/2643, Rule of Law: Commission Issues Recommendation to Poland (July 27, 2016); European Commission Press Release IP/13/327, The European Commission Reiterates Its Serious Concerns over the Fourth Amendment to the Constitution of Hungary (Apr. 12, 2013).

[117] U.S. CONST. art. III, § 1.

[118] *Id.* art. II, § 2.

judges is provided in the Constitution—appointments are for the lifetime of the judge, with removal only by impeachment, and with a guarantee of no diminution of salary.[119]

European data protection law emphasizes the importance of an independent decision-maker to protect privacy rights.[120] The precise guarantees of judicial independence in EU Member States vary considerably.[121] The lifetime tenure and protection against diminution of salary provides a strong guarantee of the independence of U.S. federal judges.

Since the 1803 Supreme Court case of *Marbury v. Madison*, the judicial branch has the authority to engage in judicial review.[122] Judges have the legal power to strike down a statute that is contrary to the Constitution. For executive actions, judges have the legal power to issue binding orders to prevent the executive branch from violating either the U.S. Constitution or applicable statutes.

3. Constitutional Protections of Individual Rights

The U.S. Constitution enumerates a set of rights that protect the individual against government action. As just mentioned, U.S. judges have the power of judicial review. This power serves as a systemic check against abuse—a judge may strike down an entire statute or government program as unconstitutional. In addition, these rights protect individuals against unconstitutional action in a criminal prosecution—defendants can argue, for instance, that there was a

---

[119] *Id.* art. III, § 1 ("The judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish. The Judges, both of the supreme and inferior Courts, shall hold their Offices during good Behaviour, and shall, at stated Times, receive for their Services, a Compensation, which shall not be diminished during their Continuance in Office.").

[120] As the Article 29 Data Protection Working Party stated in its Privacy Shield Opinion: "The WP29 recalls that ideally, as has also been stated by the CJEU and the ECtHR, [surveillance] oversight should be in the hands of a judge in order to guarantee the independence and impartiality of the procedure." Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, at 41, 16/EN WP 238 (Apr. 13, 2016), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf; *see* EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, SURVEILLANCE BY INTELLIGENCE SERVICES: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU: MAPPING MEMBER STATES' LEGAL FRAMEWORKS 52 t.4 (2015) [hereinafter FRA REPORT], http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services.

[121] *See generally* European Commission for the Efficiency of Justice, Study on the Functioning of Judicial Systems in the EU Member States, CEPEJ (2014)4final (Mar. 14, 2014), http://ec.europa.eu/justice/effective-justice/files/cepj_study_scoreboard_2014_en.pdf.

[122] 5 U.S. (1 Cranch) 137, 177 (1803).

violation of their rights under the Fourth Amendment (search and seizure) or First Amendment (free speech).

For government access to personal data, the Fourth Amendment plays a particularly important role.[123] It 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.[124]

As discussed in Swire's 2015 testimony, the jurisprudence concerning the Fourth Amendment has responded to changing technology. Federal courts in recent years have issued a string of Fourth Amendment rulings to protect privacy, such as *Riley v. California*[125] (warrant needed to search cell phones), *United States v. Jones*[126] (warrant needed for GPS attached to a car), *Kyllo v. United States*[127] (warrant needed for high-technology search of home conducted from the street), and *United States v. Warshak*[128] (warrant needed to access e-

---

[123] In our view, there has been some confusion about the way that the Fourth Amendment applies to non-U.S. persons, in the wake of *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). Briefly, the Fourth Amendment applies to searches and seizures that take place within the U.S. (such as on data transferred to the U.S.), and to searches against U.S. persons (U.S. citizens as well as permanent residents) that take place outside of the U.S. For foreign intelligence collected in the U.S., such as personal data transferred from the EU by a company, the Fourth Amendment continues to apply because all searches must meet the overall Fourth Amendment test that they be "reasonable." *See In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (holding that foreign intelligence searches must satisfy Fourth Amendment reasonableness standards). The EU Commission has recognized this rule: "While the Fourth Amendment right does not extend to non-U.S. persons that are not resident in the United States, the latter nevertheless benefit indirectly from its protections, given that the personal data are held by U.S. companies with the effect that law enforcement authorities in any event have to seek judicial authorisation (or at least respect the reasonableness requirement)." European Commission, *Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield*, C(2016) 4176 final, ¶ 127 (July 7, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL. For data that the U.S. government collects in the United States, statutory protections apply in addition to the Fourth Amendment, such as the Wiretap Act, 18 U.S.C. §§ 2510–2522, and the Stored Communications Act, 18 U.S.C. §§ 2701–2712.

[124] U.S. CONST. amend. IV.

[125] 134 S. Ct. 2473 (2014).

[126] 132 S. Ct. 945 (2012); *see also* David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders*, 14 INT'L J. CONST. L. 220, 230–33 (2016) (discussing the application of *Jones* to warrants based on length of the search).

[127] 533 U.S. 27 (2001).

[128] 631 F.3d 266 (6th Cir. 2010). Despite the fact that the *Warshak* case is not a U.S. Supreme Court decision, the case has had significant impact. *See* Tamar R. Gubins, Warshak v. United States*: The* Katz *for Electronic Communication*, 23 BERKELEY TECH. L.J. 723, 741–52 (2008); Erin E. Wright, *The Right to Privacy*

mail). We further discuss the probable cause requirement and other aspects of Fourth Amendment protection below, in connection with specific law enforcement and intelligence rules.

Other constitutional protections for information about a person's information include:

- First Amendment—This amendment protects free speech, assembly, and association, providing a wide range of protections against government interference with freedom of thought and expression. With regards to privacy, the First Amendment protects a range of anonymous speech,[129] and protects the right of individuals to gather or communicate privately.[130]
- Third Amendment—Because soldiers had been quartered in homes during colonial times, the Founders specifically outlawed this practice under the Constitution. This protection supports the privacy of one's home.[131]
- Fifth Amendment—The prohibition on compelled self-incrimination protects the privacy of an individual's thoughts. In the context of electronic evidence, this provision of the U.S. Constitution has been used to restrain the government from requiring an accused person from providing passwords and encryption keys.[132]

These constitutional rights, enforced by independent judges, provide systemic protections against overreach by the other branches of government.

4. Democratic Accountability

As part of the longer U.S. history of skepticism of excessive government power, two examples illustrate the willingness of the elected branches to set limits on government surveillance. When excessive surveillance became known,

---

in Electronic Communications: Current Fourth Amendment and Statutory Protection in the Wake of Warshak v. United States, I/S: J.L. & POL'Y INFO. SOC'Y 531, 543–52 (2007–08).

[129] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).

[130] Givhan v. W. Line Consol. School Distr., 439 U.S. 410, 415–16 (1979) (holding that a public employee cannot be fired based on the content of private communications); Nat'l Ass'n for Advancement of Colored People v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460 (1958) (holding that the First Amendment guarantee of free association included a right to private, anonymous membership in an organization).

[131] U.S. CONST. amend. III.

[132] *Id.* amend. V; *see also In re* Grand Jury, 670 F.3d 1335, 1349 (11th Cir. 2012); United States v. Kirschner, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010).

the democratically-elected branches responded with new and significant safeguards.

The Watergate scandal under President Nixon was followed by a host of significant government reforms, including the Privacy Act of 1974, major expansion of the Freedom of Information Act in 1974, and the Foreign Intelligence Surveillance Act of 1978.[133] Following the Edward Snowden revelations that began in 2013, the U.S. government undertook over two dozen significant surveillance reforms, including two notable statutes. The USA FREEDOM Act of 2015 created multiple new limits on foreign intelligence surveillance, and Congress also enacted the Judicial Redress Act in 2016.[134] These legislative and executive safeguards are evidence of an ongoing political culture in the United States that sets limits on surveillance powers, complementing the protection afforded by the Constitution and the independent judiciary.[135]

B. Protections to Ensure Limits on Law Enforcement Investigations

Consistent with constitutional requirements, the U.S. system provides numerous limits on law enforcement investigations. Plus factors, where the limits are at least as strict as EU practice and often stricter, include: (1) oversight of searches by independent judicial officers; (2) probable cause of a crime as a relatively strict requirement for both physical and digital searches; (3) even stricter requirements for government use of telephone wiretaps and other real-time interception; (4) the exclusionary rule, preventing prosecutors' use of evidence that was illegally obtained, is supplemented by civil suits; (5) other legal standards that are relatively strict for government access in many non-search situations, such as the judge-supervised "reasonable and articulable suspicion" standard under ECPA; (6) transparency requirements, such as notice to the service provider of the legal basis for a request; (7) lack of data retention requirements for Internet communications; and (8) lack of limits on use of strong encryption.

---

133 *See* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1325–26 (2004).

134 Judicial Redress Act of 2016, Pub. L. No. 114-126, 130 Stat. 282 (2016), https://www.congress.gov/bill/114th-congress/house-bill/1428/text.

135 Swire, *US Surveillance Law*, *supra* note 47, at 32. This document was submitted as a White Paper to the Belgian Privacy Authority at its request for its Forum on "The Consequences of the Judgment in the *Schrems* Case."

1. Oversight of Searches by Independent Judicial Officers

Standard practice in the United States is that search warrants are issued by a judge, who is a member of the judiciary, separate from the executive branch.[136] Under the usual MLA process, a federal prosecutor appears before a federal judge. After review by the DOJ, the prosecutor provides evidence from the requesting country, asking the judge to issue an order requiring production of the evidence. Federal judges have strong legal guarantees of independence—Article III of the U.S. Constitution guarantees that federal judges have lifetime tenure and cannot have their salaries reduced.[137]

This review by an independent judge, separate from the executive branch, is far from universal under European legal systems. Approximately half of the Member States lack a review by an independent judge when the government seeks to engage in surveillance.[138] As discussed in the comparative case study of U.S. and French criminal procedure by Swire, Hemmings, and Vergnolle, French public prosecutors typically combine the prosecutorial and judicial roles when determining what evidence to gather for a criminal prosecution.[139]

2. Probable Cause of a Crime as a Relatively Strict Requirement for Both Physical and Digital Searches

Most important for surveillance issues, the Fourth Amendment limits the government's ability to conduct searches and seizures, and warrants can issue only with independent review by a judge. The Fourth Amendment governs more than simply a person's home or body; its protections apply specifically to

---

[136] The U.S. Department of Justice's manual explains how to obtain electronic evidence in criminal investigations. *See* DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 1–56 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

[137] U.S. CONST. art. III. More specifically, the constitutional text provides that federal judges retain their positions during "good behavior," which means in practice they have lifetime tenure except in extraordinary circumstances, notably when Congress impeaches the individual judge. *See* Walter F. Pratt, *Judicial Disability and the Good Behavior Clause*, 85 YALE L.J. 706, 712 (1976).

[138] FRA REPORT, *supra* note 120, at 51–52. Even in the United Kingdom, which shares a common law history with the United States, the independent judiciary plays a far smaller role in overseeing criminal investigations than in the United States. *See* Regulation of Investigatory Powers Act 2000, § 5 (Eng.). The FRA Report identifies five Member States that engage in the collection of signals intelligence (collection that, at least in the initial stage, targets large flows of data and not an individual). None of these Member States—France, Germany, the Netherlands, Sweden, and the United Kingdom—has a judicial body involved in the approval of signal intelligence. FRA REPORT, *supra* note 120, at 55 t.5.

[139] Swire, Hemmings & Vergnolle, *supra* note 1 (manuscript at 22).

communications, covering a person's "papers and effects."[140] In criminal prosecutions, the law enforcement officer must determine whether the Fourth Amendment requires a warrant to conduct a search, or whether it is an instance where a lesser requirement will satisfy the reasonableness requirement of the Fourth Amendment.[141] If law enforcement officers are incorrect in their assessment, the evidence collected may be excluded from evidence in a criminal trial.

The search warrant is issued by a neutral magistrate, a judge, only after a showing of probable cause that there is incriminating evidence in the place to be searched.[142] Probable cause that a crime has been committed must be established by the law enforcement officer by "reasonably trustworthy information" that is sufficient to cause a reasonably prudent person to believe that an offense has been or is being committed or that evidence will be found in the place that is to be searched.[143] In the warrant, the law enforcement officer is required to list, with specificity, the items to be searched and seized.[144]

Based on our MLA research, the probable cause standard is different than the legal rules in other countries, and generally considered stricter than non-U.S. practice before the government can access evidence. For instance, formal investigations under the French system provide the investigating magistrate with broad powers to order the search of any place where one can discover objects or data.[145]

3. Even Stricter Requirements for Government Use of Telephone Wiretaps and Other Real-Time Interception

In U.S. law, the real-time interception of electronic data is recognized as holding heightened privacy risks, and consequently an order authorizing such interception must meet a stricter standard of proof. Wiretaps are understood as

---

[140] U.S. CONST. amend. IV.

[141] In this context, the search is considered to be reasonable if law enforcement obtained a valid warrant before the search was conducted. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 352 (5th ed. 2015).

[142] *See* Johnson v. United States, 333 U.S. 10, 13–14 (1948).

[143] *See* Brinegar v. United States, 338 U.S. 160, 171 (1949).

[144] *See* Horton v. California, 496 U.S. 128, 144 (1990) (Brennan, J., dissenting); *see also* DEP'T OF JUSTICE, *supra* note 136, at 63.

[145] Swire, Hemmings & Vergnolle, *supra* note 1 (manuscript at 22).

requiring "probable cause plus," with requirements before the courts permit real-time interception.[146]

1. An interception order requires "a particular description" of both the "nature and location of the facilities from which or the place where the communication is to be intercepted" and "the type of communications sought."[147]
2. The application for an interception order must explain "whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or be too dangerous."[148] Failure to exhaust alternate, less-intrusive means of obtaining the same information can result in the denial of an application for an interception order.[149]
3. The application must specify the period of time during which the interception will take place, or a reason why the applicant has probable cause to believe no termination date should be set because additional covered communications will continue to occur.[150] Minimization rules apply so non-relevant communications are not authorized by the wiretap.[151]
4. There are multiple rounds of review within the DOJ before a wiretap request can go to a judge—magistrates on their own motion cannot approve a wiretap.[152]

The judge must make a determination in favor of the government on all of these factors to issue an order permitting the interception.[153] Once the order is approved, the government is responsible for complying with minimization procedures. Specifically, the order is to be executed as soon as possible, is to be conducted in such a way as to minimize the incidental collection of

---

146 18 U.S.C. § 2518(2) (2012). The Wire Tap Act is "codified at Title I of ECPA." SOLOVE & SCHWARTZ, *supra* note 141, at 353.

147 § 2518(1)(b) (2012).

148 § 2518(1)(c).

149 *Id.*

150 § 2518(1)(d).

151 § 2518(5); *see, e.g.*, United States v. Rivera, 527 F.3d 891, 904–05 (9th Cir. 2008), (describing the government's minimization efforts).

152 § 2518(1); *see also* 18 U.S.C. § 2510(9) (defining an approving judge as "(a) a judge of a United States district court or a United States court of appeals; and (b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications").

153 § 2518(3). If the request is denied, the court must notify the individual who was the target of the request within ninety days of the denial. § 2518(8)(d).

communications not subject to the order, and is to be terminated once the communication authorized under the order is obtained.[154] Within ninety days of the termination of the order, the individual who was searched must be notified by the court of the existence of the order.[155]

These probable-cause-plus requirements for wiretaps are stricter than practice in other countries. For instance, the United Kingdom has requested access to real-time interceptions in the proposed MLA reform package with the United States under merely the rules that apply to other electronic evidence.[156]

4. The Exclusionary Rule, Preventing Prosecutors' Use of Evidence That Was Illegally Obtained, Is Supplemented by Civil Suits

U.S. criminal law provides individual remedies to address evidence obtained during a search that was illegally conducted. In a criminal trial in the United States, the courts enforce constitutional rights by excluding evidence that the government obtains illegally.[157] In addition, the courts bar evidence that is "the fruit of the poisonous tree"—additional evidence similarly cannot be used in court if it is derived from an illegal search.[158] Since the 1960s, this "exclusionary rule" has served as an important practical motivation for police officers to follow the rules for searches and seizures.

With regard to civil remedies, an individual who has been the subject of a search that violated the Fourth Amendment can file a lawsuit suit seeking monetary damages.[159] When the law enforcement officials conducting the search are state or local employees, the individual files a civil rights suit pursuant to 42 U.S.C. § 1983.[160] In a § 1983 claim, the plaintiff can recover compensatory damages and reasonable attorney's fees. The courts have permitted suits by U.S.

---

154 § 2518(5).

155 § 2518(8)(d)(1).

156 Devlin Barrett & Jay Greene, *U.S. to Allow Foreigners to Serve Warrants on U.S. Internet Firms*, WALL ST. J. (July 15, 2016, 8:00 PM), http://www.wsj.com/articles/obama-administration-negotiating-international-data-sharing-agreements-1468619305.

157 Mapp v. Ohio, 367 U.S. 643, 657 (1961). For details on the exclusionary rule, see JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE VOL. 1: INVESTIGATION 347–92 (5th ed. 2010). In addition to exclusion from evidence under the Fourth Amendment, certain statutes, such as the Wiretap Act, provide for exclusion of evidence for violation of the statutory requirements. *See* 18 U.S.C. § 2518(10)(a).

158 Wong Sun v. United States, 371 U.S. 471, 487–88 (1963).

159 SOLOVE & SCHWARTZ, *supra* note 141, at 354.

160 42 U.S.C. § 1983 (2012). In addition to § 1983 claims, certain federal statutes provide for a basis for a civil suit. *See* 18 U.S.C. § 2511(4)(a) (2012); The Stored Communications Act, 18 U.S.C. § 2701(b) (2012).

citizens and non-U.S. citizens living in the United States.[161] The U.S. exclusionary rule, backed up by the "fruit of the poisonous tree" doctrine and civil remedies, provides clear individual remedies against illegal searches.

The adversarial system in the United States makes this remedy quite different than the laws in many European countries. For example, in the French system, a search needs to be necessary to establish the "truth," and any evidence "necessary to establish the truth" can be presented to the bodies investigating and ultimately prosecuting the crime.[162]

5. *Other Legal Standards that Are Relatively Strict for Government Access in Many Non-Search Situations, Such As the Judge-Supervised "Reasonable and Articulable Suspicion" Standard Under ECPA*

ECPA defines categories of information that retain the requirement of judicial approval but require less than a probable cause showing. Location information and many e-mails have historically been available to the government when a judge has been satisfied that reasonable suspicion exists to believe that the data are relevant to an ongoing criminal investigation based on "specific and articulable facts" presented by the government.[163] This requirement of reasonable and articulable suspicion means that the government must meet the touchstone of the Fourth Amendment's requirement for reasonableness, but does not require a search warrant because the level of intrusion is considered lower than that in a full search.[164]

---

[161] The text of § 1983 states that an aggrieved person is "any citizen of the United States or other person within the jurisdiction thereof." 42 U.S.C. § 1983 (2012); *see* Plyler v. Doe, 457 U.S. 202, 210 (1982) ("Aliens . . . have long been recognized as 'persons' guaranteed due process of law by the Fifth and Fourteenth Amendments."); Graham v. Richardson, 403 U.S. 365, 378 (1971) ("[A]liens . . . have a right to enter and abide in any State . . . 'on an equality of legal privileges with all citizens under non-discriminatory laws.'" (quoting Takahashi v. Fish & Game Comm'n, 334 U.S. 410, 420 (1948))); MARTIN A. SCHWARTZ, SECTION 1983 LITIGATION 27 (3d ed. 2014). Because § 1983 claims do not extend to instances where the law enforcement officials conducting the search were federal officers, the U.S. Supreme Court recognized an implied remedy known as a *Bivens* claim, so named for the 1971 case where the claim was first discussed. Bivens v. Six Unknown Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 397 (1971); *see also* SCHWARTZ, *supra*, at 7–11. Generally, the same legal principles and procedures apply in a *Bivens* claim as in a § 1983 claim. *Id.* at 10.

[162] For a full comparison of these concepts of French and U.S. laws, see Swire, Hemmings & Vergnolle, *supra* note 1.

[163] 18 U.S.C. § 2703(d) (2012).

[164] The standard derives from *Terry v. Ohio*, 392 U.S. 1 (1968), which established the reasonable and articulable suspicion test for brief police stops of individuals. For one discussion of the relative role of *Terry*, probable cause, and other standards, see CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 21–47 (2007).

More recently, federal appellate courts have interpreted ECPA to say that requests under § 2703(b) for content of communications, including e-mails, require a probable cause warrant.[165] Some magistrates have placed even further limitations on obtaining content, such as the length of time the content can be retained and limits on searching within a computer for all the files in that computer.[166]

Compared with the approaches in France and other EU countries, the U.S. analysis is similar to that provided for the probable cause standard. Once again, an independent judge in the United States must make the decision whether the legal standard has been met for the government to access the evidence, in contrast for instance to the French approach where the investigating magistrate can generally seek access to all evidence deemed helpful to the investigation.

6. Transparency Requirements, Such As Notice to the Service Provider of the Legal Basis for a Request

U.S. law and practice is to have clear notice in the judge's order to produce evidence of the legal basis for the order, for instance by citing the specific statutory provision under which the order is issued.[167] This notice enables the recipient of the order to research the lawful basis to help determine whether there are reasons to challenge the order. By contrast, our interviews with companies that receive requests for electronic evidence is that many EU and other jurisdictions lack this information about the legal basis for the evidence request.

7. Lack of Data Retention Rules for Internet Communications

Data retention requirements have been a prominent feature of European debates about how to achieve privacy protection consistent with law enforcement and national security goals. In 2006, the EU promulgated a Data

---

[165] *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding the Fourth Amendment prevents law enforcement from obtaining stored e-mail communications without a warrant based on probable cause); *United States v. Ali*, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012), ("[I]ndividuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider." (quoting United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011))).

[166] *See* United States v. Ganias, 755 F.3d 125, 134, 137–39 (2d Cir. 2014) ("Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools."); *see also In re* Black iPhone 4, 27 F. Supp. 3d 74, 78 (D.D.C. 2014) (holding the government "must be more discriminating when determining what it wishes to seize, and it must make clear that it intends to seize *only* the records and content that are enumerated and relevant to its present investigation").

[167] *See* 18 U.S.C. § 2703(b); FED. R. CRIM. P. 41(d)–(e); DEP'T OF JUSTICE, *supra* note 136, at 127–34.

Retention Directive, which required publicly available electronic communications services to retain records for an extended period of time, for purposes of fighting serious crime.[168] For instance, for e-mail and other electronic communications, the communications services were required to retain "the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication."[169] In *Digital Rights Ireland v. Minister of Communications*,[170] the European Court of Justice struck down that Directive due to privacy concerns related to excessive access to the retained data and lack of assurances that the records would be destroyed at the end of the retention period.[171] In the wake of that judgment, a number of EU Member States reinstated modified data retention requirements for telephone and Internet communications.[172]

By contrast, the United States does not require data retention for e-mail or other Internet communications. Internet data retention bills have been introduced in Congress, but have not come close to passage.[173] The Federal Communications Commission has issued rules concerning retention of telephone records for up to eighteen months.[174] Those rules apply only to telephone toll records, which are a diminishing portion of all communications as users increasingly rely on non-telephone Internet communications and often have unlimited phone calls, so toll records are no longer required for billing purposes.[175]

In light of the significant privacy concerns explained in *Digital Rights Ireland*, the presence of data retention rules in the EU and their general absence in the United States support the view that the absence of such rules is a

---

168 Directive 2006/24/EC, of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54.

169 *Id.* art. 5(1)(b)(2)(ii).

170 Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd. v. Minister of Communications, 2014 EUR-Lex 62012CJ0293 (Apr. 8, 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CC0293&from=EN.

171 *Id.* ¶71.

172 Federico Fabrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States*, 28 HARV. HUM. RTS. J. 65, 88 (2015).

173 *See Resources on Data Retention*, CTR. FOR DEMOCRACY & TECH. (Sept. 26, 2012), https://cdt.org/insight/resources-on-data-retention (collecting materials on the issue).

174 47 C.F.R. § 42.6 (2016).

175 *Id.*

significant plus factor for the United States in comparing the privacy regimes that apply to both law enforcement and foreign intelligence investigations.

8. Lack of Limits on Use of Strong Encryption

As of November 2016, there have been calls for new limits on strong encryption in a growing number of EU countries, including a joint press conference by the Interior Ministers of France and Germany.[176] In the United Kingdom, in addition to relatively strict rules relating to encryption in the Regulation of Investigatory Powers Act of 2000,[177] authority to limit end-to-end encryption is included in the Investigatory Powers Bill, which was enacted in 2016.[178] In our view and the view of many other experts, such limits on the use of strong encryption pose serious threats to user privacy.[179]

Debates about the use of strong encryption have also occurred recently in the United States, most prominently expressed by FBI Director James Comey in the controversy about encryption of the Apple iPhone.[180] The United States historically permitted use of strong encryption within the country but limited exports of strong encryption through export control laws. The bulk of these export controls were eliminated in 1999.[181] Based on Swire's extensive experience with encryption policy in the United States, we believe legislation limiting the use of strong encryption has a fairly low likelihood of passage.[182]

---

[176] Natasha Lomas, *Encryption Under Fire in Europe as France and Germany Call for Decrypt Law*, TECHCRUNCH (Aug. 24, 2016), https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/.

[177] *See* Bert-Jaap Koops, *Crypto Law Survey, Overview per Country, Version 27.0*, CRYPTOLAW (Feb. 2013), http://www.cryptolaw.org/cls2.htm.

[178] Cara McGoogan, *What Is the Investigatory Powers Bill and What Does It Mean for My Privacy?*, TELEGRAPH (Nov. 29, 2016, 6:29 PM), http://www.telegraph.co.uk/technology/2016/11/29/investigatory-powers-bill-does-mean-privacy.

[179] *See, e.g.*, Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary, 114th Cong. (2015) (testimony of Peter Swire); HAROLD ABELSON ET AL., KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS (2015), http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[180] Lev Grossman, *Inside Apple CEO Tim Cook's Fight with the FBI*, TIME (Mar. 17, 2016), http://time.com/4262480/tim-cook-apple-fbi-2/.

[181] Press Briefing by Deputy National Security advisor Jim Steinberg, Attorney General Janet Reno, Deputy Secretary of Defense John Hamre, Under Secretary of Commerce Bill Reinsch, and Chief Counselor for Privacy at OMB Peter Swire, White House, Office of the Press Sec'y (Sept. 16, 1999), http://www.peterswire.net/archive/privarchives/Press%20briefing%20Sept.%2016%201999.html.

[182] In 1999, Swire chaired the White House Working Group on Encryption when the United States repealed most of the export controls on export of strong encryption. *See id.* Swire has since written extensively on

Meanwhile, a number of EU Member States retain stricter laws governing encryption than the United States, including France and Hungary.[183] Indeed, U.S.-based technology companies have taken a global position of leadership on use of strong encryption, bolstering the likelihood that encryption-enabled privacy protections will continue to develop in the United States.

C. Protections to Ensure Limits on Foreign Intelligence Investigations

MLA requests typically are for evidence used in law enforcement investigations rather than for national security or foreign intelligence investigations.[184] Swire has written extensively in the past on the system of U.S. foreign intelligence law,[185] and also plans in a separate forum to do a more detailed comparison of U.S. and EU access for foreign intelligence purposes.[186] In this Article, we therefore address the U.S. rules governing foreign intelligence investigations in summary form.

Especially in light of the extensive U.S. surveillance reforms since 2013, independent researchers, including Professor Ian Brown of Oxford University, have written that:

> the legal framework for foreign intelligence collection in the US, as enhanced by the Presidential Policy Directive of January 2014, contains much clearer rules on the authorisation and limits on the

encryption law and policy. *See, e.g.*, Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416 (2012).

[183] Swire, Hemmings & Vergnolle, *supra* note 1 (manuscript at 29–30); *Freedom of the Net 2016, Hungary Country Profile*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-net/2016/hungary (last visited Jan. 30, 2017); *see also* Glyn Moody, *Proposed Hungarian Law Would Allow Government to Suspend Key Human Rights Whenever There is a 'Terror Threat Situation'*, TechDirt (Feb. 4, 2016, 11:23 PM), https://www.techdirt.com/articles/20160203/09004533506/proposed-hungarian-law-would-allow-government-to-suspend-key-human-rights-whenever-there-is-terror-threat-situation.shtml.

[184] There is some overlap between criminal and foreign intelligence surveillance investigations, such as where a government seeks to jail a potential terrorist for criminal activities. Also, the line between law enforcement and national security or foreign intelligence investigations is not necessarily the same in each jurisdiction. Nonetheless, MLA requests focus on law enforcement investigations, so comparison of the safeguards for criminal prosecutions is thus central to MLA reform efforts. DEP'T OF JUSTICE CRIMINAL DIVISION, PERFORMANCE BUDGET FY 2017 PRESIDENT'S BUDGET 22–30 (2016), https://www.Justice.gov/jmd/file/820926/download.

[185] Swire, *supra* note 47, at 23–43 (discussing reforms to U.S. surveillance law since 2013); REVIEW GROUP REPORT, *supra* note 42, at 53–57 (history of U.S. foreign intelligence regime); Swire, *supra* note 133.

[186] Swire has submitted testimony as an independent legal expert in *Schrems v. Data Protection Comm'r*, on U.S. and EU legal rules for surveillance.

> collection, use, sharing and oversight of data relating to foreign nationals than the equivalent laws of almost all EU Member States.[187]

The U.S. legal framework, among others, contains the following safeguards in connection with foreign intelligence surveillance:

1) The Foreign Intelligence Surveillance Act of 1978 (FISA) creates a comprehensive legal system for foreign intelligence surveillance. Independent federal judges play the central role in overseeing government surveillance requests, and those judges have access in the Foreign Intelligence Surveillance Court (FISC) to the classified information necessary for assessing government requests.[188]
2) Under FISA and the Fourth Amendment, judges retain their power to oversee all electronic surveillance conducted within the United States. A search is generally either (a) conducted in the criminal context, in which case a judge must approve a warrant showing probable cause of a crime; or (b) conducted in the foreign intelligence context, in which case the Foreign Intelligence Surveillance Court must authorize the surveillance pursuant to FISA and subject to the reasonableness requirements of the Fourth Amendment. These are the principle ways that an electronic communications search is carried out lawfully within the United States.[189]

---

[187] IAN BROWN ET AL., TOWARDS MULTILATERAL STANDARDS FOR FOREIGN SURVEILLANCE REFORM 3 (2015), https://cihr.eu/wp-content/uploads/2015/01/Brown_et_al_Towards_Multilateral_2015.pdf. For a detailed comparison of U.S. and EU surveillance law practices, similarly concluding that U.S. protections are generally greater, see JACQUES BOURGEOIS ET AL., ESSENTIALLY EQUIVALENT: A COMPARISON OF THE LEGAL ORDERS FOR PRIVACY AND DATA PROTECTION IN THE EUROPEAN UNION AND UNITED STATES (Jan. 25, 2016), http://datamatters.sidley.com/wp-content/uploads/2016/01/Essentially-Equivalent-Final-01-25-16-9AM3.pdf.

[188] 50 U.S.C. §§ 1801–1885(c) (2012).

[189] When these searches occur under a mandatory order, they generally follow either the foreign intelligence or law enforcement regime. 50 U.S.C. § 1802(a) permits a limited collection for a period of a year or less at the direction of the President and with the approval of the Attorney General, for (1) the collection of communications exclusively between or among foreign powers; and (2) the collection of technical intelligence, which does not include spoken communications of individuals, from property under the control of a foreign power. 50 U.S.C. § 1802(a).

Some government access to information does not rise to the level of a "search" under the Fourth Amendment. For instance, under what is called the "third party doctrine," government access to telephone metadata held by a "third party" (the phone company) is permitted constitutionally without a judge-approved warrant. Smith v. Maryland, 442 U.S. 735, 741–46 (1979). In response, the ECPA of 1986 created statutory protections for telephone metadata, requiring a judicial order by statute rather than it being required by the Constitution. *See* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 264–65 (2016).

3) Perhaps the most dramatic change in U.S. surveillance statutes since 2013 concerns reforms of § 215 of the USA PATRIOT Act, which provided the government with broad powers to obtain "documents[] and other items."[190] After the September 11 attacks, § 215 was used as a basis for collecting metadata on large numbers of phone calls made in the United States. The USA FREEDOM Act abolished bulk collection under § 215 and two other similar statutory authorities. These limits on collection apply to both U.S. and non-U.S. persons. A far narrower authority now exists, based on individualized selectors associated with terrorism and judicial review of each proposed selector.[191]
4) Section 702 of FISA applies to collections that take place within the United States, and only authorizes access to the communications of targeted individuals, for listed foreign intelligence purposes.[192] Misunderstanding about the PRISM program under § 702 traces to the original and since-revised Washington Post story, which stated that "[t]he National Security Agency and the FBI are tapping *directly* into the central servers of nine leading U.S. Internet companies" to extract a range of information.[193] This statement was incorrect. In practice, PRISM operates under a judicially-approved and judicially-supervised directive, pursuant to which the government sends a request to a U.S.-based provider for collection of targeted "selectors," such as an e-mail address.
5) There have also been concerns about Upstream as a mass collection program. In fact, the U.S. government receives communications under both Upstream and PRISM based on targeted selectors, with actions under each program subject to FISC review. Concerning scale, a declassified FISC opinion found that over 90% of the Internet communications obtained by the NSA in 2011 under § 702 actually resulted from PRISM, with less than 10% coming from Upstream.[194]

---

[190] *See* USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (2001).

[191] These reforms are codified at 50 U.S.C. § 1861. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268, 269–76.

[192] Section 702 is codified at 50 U.S.C. § 1881a.

[193] *See* Barton Gellman & Laura Poitras, *U.S. British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013) (emphasis added), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.ad91d2af80a0. The story was revised to explain that a leaked document said that there was direct access; in fact, the leaked document was misleading or incorrect; § 702 does not authorize direct access.

[194] *See* [Caption Redacted], No. [Redacted], 2011 WL 10945618, at *9–11 (F.I.S.C. Oct. 3, 2011).

The U.S. intelligence community now releases an annual Statistical Transparency Report,[195] with the statistics subject to oversight from Congress, Inspector Generals, the FISC, the Privacy and Civil Liberties Oversight Board, and others.[196] For 2015, there were 94,368 "targets" under the § 702 programs, each of whom was targeted based on a finding of foreign intelligence purpose.[197] That is a tiny fraction of U.S., European, or global Internet users. Rather than having mass or unrestrained surveillance, the documented statistics show the low likelihood of communications being acquired for ordinary citizens.[198]

6) There is a comprehensive oversight system for foreign intelligence, including Senate and House intelligence committees, agency inspectors general, privacy offices in executive agencies, and the independent Privacy and Civil Liberties Oversight Board. Each of these institutions gains access to the classified information needed to provide oversight.[199]

---

[195] Transparency reports have been released for every year since 2013. Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities—Annual Statistics for Calendar Year 2015*, IC ON THE RECORD (May 2, 2016), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015; Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities—Annual Statistics for Calendar Year 2014*, IC ON THE RECORD (Apr. 22, 2015), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014; Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities—Annual Statistics for Calendar Year 2013*, IC ON THE RECORD (June 26, 2014), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.

[196] For a listing of the multiple oversight entities, see REVIEW GROUP REPORT, *supra* note 42, at 269.

[197] The statistical reports define "target" in detail, and my assessment is that the number of individuals targeted is lower than the reported number.

[198] The 2016 Statistical Transparency Report reiterates the targeted nature of the surveillance: "Section 702 only permits the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information." Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities—Annual Statistics for Calendar Year 2015*, IC ON THE RECORD (May 2, 2016), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015.

[199] *See generally* U.S. SENATE SELECT COMMITTEE ON INTELLIGENCE, http://www.intelligence.senate.gov/; U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMMITTEE ON INTELLIGENCE, http://intelligence.house.gov/; IC INSPECTOR GENERAL, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, https://www.dni.gov/index.php/about/leadership/inspector-general; Exec. Order No. 13719, Establishment of the Federal Privacy Council, 81 Fed. Reg. 7685–89 (Feb. 12, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-02-12/html/2016-03141.htm; *The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act)*, JUSTICE INFORMATION SHARING, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1283 (last visited Dec. 13, 2016) (describing the independence of the Privacy and Civil Liberties Oversight Board (PCLOB)). For recent PCLOB reports, see PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf; PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE

7) There are numerous transparency safeguards in the U.S. foreign intelligence system, including: federal agency reports on the number and type of surveillance orders; company transparency reports on such orders; provisions in the USA-FREEDOM Act that require transparency of new legal decisions by the FISC; and new policies for transparency to the extent possible of FISC opinions.[200]
8) The Executive Branch has multiple safeguards in place to supplement legislative safeguards, including Presidential Policy Directive 28, which recognizes the privacy interest of non-U.S. persons and includes other privacy protections for foreign intelligence activities.[201]

With respect to U.S. safeguards for government access to information for U.S. foreign intelligence and law enforcement investigations, there are important plus factors that have often not been recognized in MLA reform debates and discussions about the adequacy of protections when data are transferred from the EU to the United States.

IV. IMPLICATIONS FOR MLA REFORM WHEN BOTH THE UNITED STATES AND THE EU ARE STRICTER ON PRIVACY IN IMPORTANT RESPECTS

Part II of this Article highlighted ways that the EU is more privacy protective, including for issues of government access to data. Notable examples are the comprehensive privacy laws for data held by the private sector, in the GDPR, and by law enforcement in the 2016 Directive. Part III highlighted ways that the United States is more privacy protective. The most prominent legal example is the probable cause standard as judged by an independent magistrate, but the plus factors discussion showed multiple respects in which the privacy rules limiting U.S. government access are stricter.

This Part analyzes the implications for MLA since both the EU and the United States are stricter about privacy in important, yet different, respects. This Part first examines the implications of our description on those who advocate for privacy, notably civil society groups and privacy regulators. Based on both

PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014), https://www.pclob.gov/library/702-Report.pdf.

[200] USA FREEDOM Act of 2015, Pub. L. No. 114-23, §§ 603, 604, 129 Stat. 268, 295–97 (2015); *see also* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities—Annual Statistics for Calendar Year 2013*, IC ON THE RECORD (June 26, 2014), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.

[201] Press Release, Office of the Press Sec'y, Presidential Policy Directive PPD-28, Signals Intelligence Activities (Jan. 17, 2014), https://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf.

theory and our experience in working with these supporters of stricter privacy protections, the relative strengths of both the United States and the EU create important obstacles to MLA reform, in ways that have not been well appreciated to date.

The discussion next turns to three models for the future of MLA, especially in the wake of the 2016 Second Circuit decision in *Microsoft Ireland*, which set important new limits on U.S. government access to e-mails held in overseas servers. We call the three models: (1) MLA status quo; (2) extraterritoriality; and (3) Visa Waiver Program (VWP). We assess the ability of each model both to protect privacy and civil liberties, and to fulfill legitimate law enforcement requests. We conclude that a well-designed VWP is the best available approach.

Although we believe a well-designed VWP is the most promising option for privacy protection, enacting such a statute would likely require legislation that has weaker privacy provisions in some respects than the status quo in either in the United States or the EU. It is understandably a difficult decision for privacy supporters to accept compromise on these provisions, such as permitting access to some records in the United States, without a showing of probable cause. Yet, we conclude, overall privacy protection is likely to be greater with such a compromise, as part of a well-designed VWP, than with other approaches.

A. The Effects on Privacy Supporters of Both the United States and the EU Being Stricter in Important Respects

We turn now to a discussion of the challenges that MLA reform poses to privacy supporters, such as civil society groups and data protection officials. Any significant streamlining of the MLA process would likely require some of the recipient country's rules to be relaxed. For instance, an EU request may succeed without going before a U.S. judge to prove probable cause. A U.S. request may mean that personal data goes to the U.S. without being subject to every requirement of European data protection law. Or law enforcement information might go to the United States without the Member State Data Protection Agency having direct access to the records held by U.S. law enforcement.

We argue below that overall privacy is likely to be enhanced via well-designed MLA reform that follows the VWP model. Nonetheless, based both on theory and our experience in deliberations on these issues, the relaxation of specific current requirements can be quite difficult for privacy supporters to accept.

1. Difficulties in Compromising on Stricter U.S. Privacy Provisions

The longstanding and, in our view, admirable efforts of the Digital Due Process Coalition illustrate this point. Since 2010, the Digital Due Process Coalition has enlisted a wide range of support both from civil society and from leading technology companies for a set of principles about how to update ECPA. Notably, the principles require having a search warrant based on probable cause for government access to "communications that are not readily accessible to the public," and for "location information regarding a mobile communications device."[202] This reform effort has made considerable progress, notably with passage by the House of Representatives in April 2016 of H.R. 699, the Email Privacy Act, which would amend ECPA in ways broadly consistent with the principles of the Digital Due Process Coalition.[203]

There is a painful tension, however, between this potential codification of the probable cause standard for U.S. government access and the fact that probable cause is "an exacting, privacy-protective standard that most countries in Europe and elsewhere in the world do not follow."[204] To the extent that MLA reform would streamline some access for EU countries, and those countries do not agree to amend their laws to meet the probable cause standard, it would require some modification of the U.S. probable cause standard, precisely at the moment when achievement of the Digital Due Process Coalition's goals appear within sight.

U.S. privacy supporters thus have a number of reasons for caution in supporting any MLA reform that modifies the probable cause standard. First, allowing non-U.S. governments access with less than probable cause goes against the simple principle that probable cause is appropriate for any government access. Second, procedurally, MLA reform proposals might muddy the waters and make it more complex and difficult to achieve final passage of the Email Privacy Act. Third, as a psychological matter, it can be difficult for privacy supporters to agree to any weakening of the probable cause standard when they have worked for years to establish that standard, even if they agree

---

202 *Our Principles*, DIG. DUE PROCESS (2010), http://digitalddueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163.

203 Sophia Cope, *House Advances Email Privacy Act, Setting the Stage for Vital Privacy Reform*, ELEC. FRONTIER FOUND. (Apr. 27, 2016), https://www.eff.org/deeplinks/2016/04/hoUse-advances-email-privacy-act-setting-stage-vital-privacy-reform.

204 Ian Brown, Vivek Krishnamurthy & Peter Swire, *Reforming Mutual Legal Assistance Needs Engagement Beyond the U.S.*, LAWFARE (Mar. 1, 2016, 7:38 AM), https://www.lawfareblog.com/reforming-mutual-legal-assistance-needs-engagement-beyond-US.

that it is a different context when governments other than the United States gain access to information about non-U.S. persons.

We have seen these concerns of privacy supporters arise in the deliberations of the Working Group on Cross-Border Data Requests. This Working Group, consisting of civil society groups, academics, and technology companies, met beginning in late 2015 to discuss MLA reform, with discussions chaired by (alphabetically) Jennifer Daskal, Jim Dempsey, Greg Nojeim, Peter Swire, and Andrew Woods.[205] After initial discussions, Jennifer Daskal and Andrew Woods posted one version of a proposed framework for what MLA reform principles could look like.[206] The structure of the proposed framework was consistent with the VWP model—a statutory reform to ECPA that would apply to countries with sufficiently strong legal safeguards, and which would provide the United States with reciprocal access to evidence held in other participating countries.

The framework focused on what we sometimes called "the easy case" for MLA reform,

> where the requesting entity makes an adequate showing of three things: (i) the requesting government has a legitimate interest in the criminal activity being investigated; (ii) the target is located outside the United States; and (iii) the target is not a US person (defined to include US citizens and legal permanent residents).[207]

In terms familiar to conflict of laws experts,[208] the interests of the requesting government (such as an EU government) are potentially quite strong in these circumstances (a crime, the target outside of the United States, and the target is not a U.S. person), while the interests of the United States are relatively weak (the evidence is held in the United States or is held by a U.S.-based company).

As discussed in our 2015 article about stakeholders in MLA reform, there is a significant congruence between the interests of civil society and technology companies—both have strong reasons to support effective privacy protections for the companies' users out of a sincere desire to protect privacy and as good business for global companies who wish to assure non-U.S. customers that data will be carefully protected.[209] In light of this congruence, as one participant in

---

[205] Our research project at Georgia Tech. provided financial support for meetings of the Working Group, as did a variety of civil society groups and companies.

[206] Daskal & Woods, *supra* note 41.

[207] *Id.*

[208] JAMES A.R. NAFZIGER, CONFLICT OF LAWS: A NORTHWEST PERSPECTIVE 94 (1985).

[209] Swire & Hemmings, *Stakeholders in Reform*, *supra* note 1, at 10–14.

the discussions of the Working Group, Swire was initially optimistic about reaching a consensus document, either in a relatively detailed format that was discussed initially, or in a more high-level set of principles that was discussed as the U.S./U.K. agreement was nearing announcement in April, 2016.

After considerable efforts to reach agreement, the Working Group was unable to reach consensus. In Swire's view, one important reason for the lack of consensus was the understandable reluctance of civil society groups to agree to text that was weaker than existing U.S. protections. For instance, the published November version of the proposed framework would allow access with "a strong factual basis" (not "probable cause") to believe a crime was committed.[210] For clear reasons, the proposal did not require a finding of probable cause by a neutral magistrate—most countries even in Europe do not follow that U.S. practice, so a probable cause requirement would render the framework unworkable in almost all instances. Civil society groups expressed concerns about the lack of possible new safeguards as well as possible weakening of other safeguards, such as the current practice of the DOJ performing a First Amendment review before turning over evidence to the requesting country.[211]

This recent experience with the Working Group on Cross-Border Data Requests shows how the existence of stricter privacy protections in the United States creates difficulties for MLA reform. The authors' view is that MLA reform is likely to be more privacy protective in the long run than the status quo, because the status quo of protections is likely to be weakened due to localization and other effects. It is difficult, however, for privacy supporters to agree publicly to weakening specific safeguards that have long been the subject of their support in litigation, legislation, and public advocacy.

2. Difficulties in Compromising on Stricter EU Privacy Protections

Along with these obstacles to weakening any U.S. privacy protections that are stricter than EU protections, there are also obstacles from the European side to accepting any MLA reform that omits European safeguards.

---

210 Daskal & Woods, *supra* note 41.

211 Greg Nojeim of the Center for Democracy and Technology proposed stricter standards for government access to metadata as an example of one such possible new safeguard to offset weakening due to relaxation of the probable cause or other standards. Greg Nojeim, *MLAT Reform Proposal: Protecting Metadata*, LAWFARE (Dec. 10, 2015, 2:43 PM), https://www.lawfareblog.com/mlat-reform-proposal-protecting-metadata.

An initial obstacle to acceptance of reform in Europe is the widespread skepticism of the effectiveness of U.S. privacy protections. Based on Swire's work on EU data protection issues for two decades,[212] one source of the skepticism is the lack of an overarching, comprehensive privacy law in the United States that corresponds to the Data Protection Directive or General Data Protection Regulation.[213] The U.S. system of privacy protection arises from a complex set of constitutional, statutory, administrative, and common law protections. In the words of the Article 29 Data Protection Working Party, an EU-level group of national privacy regulators, "the framework of statutes, procedures and policies is fragmented," with the consequence that the Working Party concluded in 2016 that it could not assess the level of protection for data accessed by law enforcement authorities.[214]

The skepticism of U.S. government practices clearly became greater after the Snowden revelations that began in 2013. In October 2015, the European Court of Justice in the *Schrems* case struck down the EU/U.S. Safe Harbor agreement for providing inadequate protection of personal data transferred from the EU to the United States.[215] The Advocate General's opinion in that case stated that the United States practiced "mass and indiscriminate surveillance," and relied for this conclusion in part on a 2013 report from the EU Commission.[216] Swire has written in detail concluding that multiple such assertions are over-stated and notably do not reflect the over two dozen surveillance reforms that the United States has made since 2013.[217] Despite growing recognition of the depth and breadth of the privacy safeguards that apply to U.S. intelligence activities, our view is that skepticism about the effectiveness of these safeguards remains widespread in Europe.

Apart from any mistaken skepticism about U.S. safeguards, EU law places important limits on the extent to which the EU can transfer personal data to other

---

212 Swire began work in 1996 for the project that became SWIRE & LITAN, *supra* note 53.

213 *Accord Hearing on Examining the EU Safe Harbor Decision and Impact for Transatlantic Data Flows, Joint Hearing Before H.R. Energy & Commerce Subcomm. on Commerce, Mfg., and Trade and Commc'ns and Tech.*, 114th Cong. 11 (2015) (testimony of Marc Rotenberg, President of EPIC), https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf (discussing concerns by other nations over the U.S. sectoral approach to privacy regulation).

214 Article 29 Data Protection Working Party, *supra* note 120, at 53.

215 Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 1, 26.

216 Opinion of Advocate General Bot, Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 EUR-Lex 62014CC0362 (Sept. 23, 2015).

217 Swire, *US Surveillance Law*, *supra* note 47; Peter Swire, *Don't Strike Down the Safe Harbor Based on Inaccurate Views of U.S. Intelligence Law*, IAPP (Oct. 5, 2015), https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law.

jurisdictions for MLA purposes. The EU Data Protection Directive has long permitted transfers to third countries, subject to limited exceptions, only where there is adequate protection of personal data.[218] The court in *Schrems* gave an apparently strict interpretation to this requirement, saying that the legal standard for transfers was "essential equivalence" to EU legal protections.[219] To the extent MLA reform offers less than "essential equivalence," then that reform would risk being overturned by the European courts.[220]

To show adequacy or essential equivalence, data protection officials have often underscored the need for a comprehensive system of protections that match the extensive list of EU protections. One example comes from the opinion in May 2016 of the European Data Protection Supervisor, concerning the draft Privacy Shield agreement. The opinion provided a section on "[i]ntegrating *all* main data protection principles," as well as a section on "[l]imiting derogations" (i.e., exceptions).[221] The opinion listed concerns about implementation of a number of specific principles, and concluded "the Privacy Shield should therefore be amended to better integrate *all* main EU data protection principles."[222] The analysis did not discuss the role of the sorts of plus factors of stricter safeguards discussed in Part III. To the extent there was any deviation from the EU list, the opinion appears to be quite skeptical about whether the legal requirements are met. In terms of MLA reform, there is thus uncertainty about the extent to which such reform could deviate from the numerous details of EU data protection law.

B. Implications for MLA Reform

We next analyze three main options for MLA reform, as informed by the discussion about how both the United States and the EU sometimes have stricter privacy rules for law enforcement access to data. In brief, the three options are:

---

[218] Directive 95/46/EC, *supra* note 4, art. 25–26, 45–46.

[219] *Schrems*, 2015 E.C.R. 1 at 21-22, 25. For an analysis of how "essential equivalence" applies to U.S. safeguards, see Swire, *US Surveillance Law*, *supra* note 47, at 3–9.

[220] A new Directive took effect in May 2016, and Member States are supposed to pass implementing legislation by May 2018, "on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties." Directive 2016/680, *supra* note 9. Articles 35, 36, and 37 of the Directive establish an adequacy regime similar to the 1998 Data Protection Directive, and this Directive will thus play an important role governing law enforcement data requests going forward. *Id.* art. 35–37.

[221] EUROPEAN DATA PROTECTION SUPERVISOR, 4/2016 OPINION ON THE EU-U.S. DRAFT PRIVACY SHIELD AGREEMENT 7 (May 30, 2016) (emphasis added), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf.

[222] *Id.* (emphasis added).

1) *MLA status quo*, where the *Microsoft Ireland* rule applies. In this approach, there are significant limits on the ability of EU countries to gain access to data held in the United States, due to the relatively strict rules of the Fourth Amendment and ECPA. There are also significant limits on the ability of the United States to use a warrant to get data held in Ireland or other countries.
2) *Widespread extra-territoriality*, where governments require companies doing business in their jurisdiction to produce records available to that company anywhere in the world. This option emphasizes the ability of a government to exert pressure on a company that has any assets or employees in the jurisdiction. One can think of this approach as the *Bank of Nova Scotia* model, where bank regulators insist on access to records held by the bank outside of the country. The Second Circuit in *Microsoft Ireland* found that Congress had not previously expressed its intent to give extra-territorial effect for warrants, but Congress could overcome that finding with a new statute explicitly providing for extra-territorial reach.
3) *Visa Waiver Program model*, where countries such as the United States and EU Member States negotiate agreements, similar in structure to the proposed U.S./U.K. agreement, that provide streamlined access to the requesting country when sufficient privacy and related safeguards are in place.

The analysis here focuses on which approach will best protect privacy over time. It also discusses other goals our previous work on MLA reform has highlighted, especially providing law enforcement legitimate access to evidence and promoting a well-functioning Internet, such as by discouraging balkanization and data localization proposals.

The MLA status quo approach, at least initially, might seem to protect privacy more strictly than the other approaches. For EU requests to the United States, data would be produced only where the requesting country meets its own rules, and then also satisfies the often laborious process to get an MLAT court order in the United States. For U.S. requests to the EU, after *Microsoft Ireland*, the United States would apparently need to go through a similar process, deciding to make the request in the United States, and then needing to get cooperation from Ireland or another country to actually produce the data.

We believe that long-run incentives, however, would undermine the privacy protections of the MLA status quo approach. One factual finding of our MLA

research program, after all, is the strong trend toward globalization of data and criminal evidence, such as e-mails, social network communications, web surfing, and myriad other kinds of potentially relevant evidence.[223] Another factual finding is how the spread of effective encryption increasingly blocks the effectiveness of local wiretaps.[224] As these trends continue, the delays in the MLA status quo will become politically more difficult to tolerate.

Countries that object to the MLA status quo can gain faster access to evidence in two main ways. First, the country can pass data localization requirements, so that the evidence resides in that jurisdiction. Russia has this type of law in effect, as part of the overall Russian system for surveilling its domestic communications,[225] and a growing array of other countries have passed or proposed localization laws.[226] Localization laws, along with other negative consequences for the operation of the Internet,[227] have clearly negative privacy effects for data held by U.S.-based companies—data are available in the localizing country, and are no longer subject to the Fourth Amendment and ECPA protections of the current MLA process. Second, the country can enact extra-territorial requirements, with the negative privacy consequences of the second of our three models.

The widespread extra-territoriality model clearly has negative effects for privacy. The main feature of an extra-territoriality approach is that it is

---

223 The trend toward data being held in countries outside of the requesting jurisdiction is indicated by research such as Jonathan Mayer, *The Web Is Flat*, WEB POLICY (Oct. 30, 2013), http://webpolicy.org/2013/10/30/the-web-is-flat/ (study showing pervasive flow of web browsing data outside of the United States for U.S. individuals using U.S.-based websites).

224 Swire, Hemmings & Vergnolle, *supra* note 1 (manuscript at 38–39).

225 The lack of surveillance safeguards in Russia has been documented in detail by the European Court of Human Rights in the 2015 *Zakharov* case. *See* Zakharov v. Russia, 2015 Eur. Ct. H.R. 69 (2015), http://hudoc.echr.coe.int/eng#{"itemid":["001-159324"]}; *see also* James Slater, *As Russia Insulates Itself from Human Rights Bodies, State Surveillance Decision Looms*, GLOBALVOICES (Dec. 17, 2015, 11:03 PM), https://advox.globalvoices.org/2015/12/18/as-russia-insulates-itself-from-human-rights-bodies-state-surveillance-decision-looms/; Andrei Soldatov & Irina Borogan, *Russia's Surveillance State*, WORLD POLICY INST., http://www.worldpolicy.org/journal/fall2013/Russia-surveillance (last visited Nov. 10, 2016); Pierluigi Paganini, *New Powers for the Russian Surveillance System SORM-2*, SECURITY AFFAIRS (Aug. 18, 2014), http://securityaffairs.co/wordpress/27611/digital-id/new-powers-sorm-2.html; PRIVACY INT'L, PRIVACY INTERESTS: MONITORING CENTRAL ASIA (Nov. 2014), https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf.

226 REVIEW GROUP REPORT, *supra* note 42, at 215; Neha Mishra, *Data Localization Laws in a Digital World: Data Protection or Data Protectionism?*, PUBLIC SPHERE, 2016, at 135, 139; Alexander Plaum, *The Impact of Forced Data Localisation on Fundamental Rights*, ACCESS NOW (June 4, 2014), https://www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/.

227 *See* REVIEW GROUP REPORT, *supra* note 42, at 214–16.

unilateral—the country seeking the records decides what level of legal process and privacy protection to offer. Compared to the MLA status quo, that means that requests made to U.S.-based companies will no longer have to meet the current Fourth Amendment and ECPA requirements. More generally, widespread use of extra-territoriality leads to a "race to the bottom" for privacy, where the country with the fewest legal protections gains easiest access to the evidence.[228] Compared to the MLA status quo, where U.S. legal protections help set a global norm for when access is appropriate, widespread extra-territoriality would undermine the ability of the United States and other rule-of-law nations to set international norms for privacy and civil liberties protections.

Supporting the MLA status quo thus quite likely leads to a degradation of privacy protections, as countries gain access to evidence by a combination of data localization and extra-territoriality measures.

The disadvantages of the MLA status quo, along with the advantages to legitimate law enforcement access from a streamlined process, have led the United States to support revisions to MLA, notably through the VWP model. As we began advocating to the U.S. government and other stakeholders in early 2015,[229] we support amending ECPA to allow streamlined access where the requesting country agrees to a series of effective privacy and civil liberties safeguards. The proposed U.S./U.K. MLA Agreement contains many of the types of safeguards we have discussed previously in writing and in stakeholder meetings, although we have reservations about some items, such as whether a foreign government can constitutionally intercept real-time communications in the United States without U.S. judicial oversight.[230]

---

[228] Companies can avoid doing business entirely in a jurisdiction if the legal regime there becomes too objectionable. The possibility of companies doing so provides some constraint on a country's decision to demand access to records, especially for smaller markets where a global company can more readily decide to abstain from doing business. For larger markets, companies face a bigger loss if they decide to avoid the jurisdiction entirely.

[229] We set forth the argument for the VWP analogy in a series of conferences in the first half of 2015, at NYU Law School, the Privacy Law Scholars Conference, and the Berkman Center of Harvard Law School.

[230] As discussed in Part III, the U.S. courts have historically required more than a probable cause showing for real-time wiretaps, and have also applied Fourth Amendment constitutional protections to wiretaps that take place on U.S. territory. The proposed U.S./U.K. agreement, by contrast, would enable U.K. access not only to stored communications (where we support streamlined access), but also to real-time interceptions. We believe there is a strong likelihood that U.S. courts would find real-time interceptions by a government, carried out in the United States to be protected by the Fourth Amendment and thus not authorized by the U.S./U.K. agreement. Professors Daskal and Woods have argued that the stricter protections for real-time interceptions are no longer justified due to changing technology. *See* Jennifer Daskal & Andrew Keane Woods, *Congress Should Embrace the DOJ's Cross-Border Data Fix*, JUST SECURITY BLOG (Aug. 1, 2016, 8:03 AM), https://www.justsecurity.org/32213/congress-embrace-dojs-cross-border-data-fix/; *see also* Jennifer Daskal, *A New UK-US Data Sharing*

Not only do we believe that the VWP model offers better privacy protections, but there is considerable urgency to making progress on such reform. If reform is delayed for a considerable period, then countries seeking records will have the time and incentive to pass sweeping data localization and extra-territoriality laws.[231] Once those laws are in place, those countries have far less reason to agree to U.S.-style safeguards to gain access to the records held by U.S.-based companies. Today, by contrast, the leverage of the United States for strong privacy protections is at its peak—many of the most valuable sources of evidence are held by U.S.-based companies, and those companies today operate under the strict U.S. regime for government access to data.

In short, the VWP model offers the best current approach to achieve all the major public policy goals. For privacy, it avoids a slippery slope into localization and extra-territoriality. For legitimate law enforcement requests, the streamlined process offers access to evidence under workable and timely procedures for many such requests (while keeping current safeguards where adequate safeguards are lacking). For a well-functioning Internet, the approach dissipates pressure for localization and extra-territoriality.

Similarly, if well crafted, the VWP model offers the best current approach for all the major stakeholders. For privacy supporters, we have explained reasons to believe that the VWP model offers the best long-term protections, even though it may mean compromise on some of the specific safeguards cherished by privacy supporters, such as a U.S.-style probable cause requirement. For the technology companies, the VWP approach offers a rule-of-law structure that enables response to legitimate requests, protection of customer data from illegitimate requests, and protection against pressure from extra-territorial requests. For non-U.S. governments, streamlined access responds to their diminishing access to important evidence. For the U.S. government, the DOJ has a new incentive to support MLA and ECPA reform in the wake of *Microsoft*

Agreement: A Tremendous Opportunity, If Done Right, JUST SECURITY BLOG (Feb. 8, 2016, 8:10 AM), https://www.justsecurity.org/29203/british-searches-america-tremendoUS-opportunity/. It is a complex topic to consider how the U.S. courts in the future could analyze the relative sensitivity of stored records and real-time intercepts. Removing the stronger protections for real-time intercepts, however, would be a momentous change in landmark privacy protections offered by *Katz* and *Berger*, so as matter of predicting U.S. courts' views, we believe that warrantless real-time wiretaps in the United States would quite likely be struck down as unconstitutional.

[231] There are other reasons that countries may pass data localization laws. *See* REVIEW GROUP REPORT, *supra* note 42, at 214–16. Our point is that lack of law enforcement to evidence of local crimes can be a significant additional factor leading to support of data localization laws.

Ireland. The VWP approach to reform thus can gain support from a potentially powerful coalition of privacy supporters, technology companies, and the DOJ.

CONCLUSION

This Article has demonstrated important ways that both the EU and the United States are stricter when it comes to privacy protections for government access to data. At a descriptive level, the relative strictness of both sides is important to debates about whether the United States has adequate privacy protection, and thus should be a lawful destination for flows of personal data from the EU. Since the Snowden leaks began in 2013, many EU discussions of U.S. privacy protections have underestimated the number and vigor of U.S. protections, notably against excessive government surveillance. The United States has more than two centuries of experience with an independent judiciary applying effective limits on government surveillance. For criminal investigations, the Fourth Amendment and ECPA are stricter than the standards for government access in much of the EU. For foreign intelligence surveillance, an international team of experts found that U.S. law "contains much clearer rules on the authorisation and limits on the collection, use, sharing, and oversight of data relating to foreign nationals than the equivalent laws of almost all EU Member States."[232]

The relative strictness of U.S. criminal law is also important to our ongoing research project on MLA in an era of globalized communications. This Article has explored the understandable reasons why privacy supporters in both the United States and EU have been reluctant in MLA reform debates to agree to compromises on specific privacy safeguards. With that said, our analysis supports the VWP model as the best hope for long-term privacy protection, as well as the best approach for fulfilling legitimate law enforcement requests, providing a workable regime for information technology companies, and preserving a well-functioning Internet against balkanization and localization rules. In short, we conclude with words from a 2016 essay by Ian Brown of Oxford, Vivek Krishnamurthy of Harvard, and Swire:

> US efforts to reform MLATs must occur in tandem with reform efforts in Europe and globally. There must be genuine appreciation that other democratic nations differ in the details of their systems, while seeking essentially the same goals. When discussing global communications,

---

[232] Ian Brown et al., *Towards Multilateral Standards for Foreign Surveillance* 3 (Oxford Internet Discussion Paper, 2015), https://ssrn.com/abstract=2551164.

> the debate in the US should not be US-centric, just as the debate in the rest of the world must not be reflexively anti-American. We need much more robust engagement with civil society and experts from many nations. Only then can reform be achieved in ways that return the "mutual" to Mutual Legal Assistance.[233]

[233] Brown, Krishnamurthy & Swire, *supra* note 204.