EU PRIVACY REGULATIONS: IMPLICATIONS FOR U.S. AND EU LAW ENFORCEMENT

Carlton Forbes & Jacob Victor*

December 3, 2012

EXECUTIVE SUMMARY

In January 2012, the European Commission released drafts of two new pieces of legislation that would provide more stringent and more uniform regulation to the processing of electronic data relating to EU citizens. The proposed General Data Protection Regulation would govern the processing of data for general purposes, while the proposed Criminal Justice Directive would govern data processed in the specific context of criminal investigations. The Data Protection Regulation has proven controversial because of the significant number of requirements it imposes on private data processors, including requirements that the processor notify a consumer when her data is shared with a third party, and requirements that processors respect a number of new individual rights, such as the right of a consumer to request that her data be deleted (a.k.a. "the right to be forgotten"). Furthermore, the Regulation would mandate that many non-EU corporations would need to comply with its requirements when processing the data of EU citizens, or face harsh penalties.

This memo summarizes the existing EU data protection regime, analyzes the changes proposed by the new Data Protection Regulation and Criminal Justice Directive, and explores the implications of this new legislation for U.S. criminal and national security investigations. We arrive at three main conclusions:

1. *The new legislation is unlikely to affect existing law enforcement data sharing agreements between the U.S. and EU.*

The proposed Criminal Justice Directive seems to have been crafted to explicitly allow the existing EU-U.S. Mutual Legal Assistance Treaty (MLAT) to remain unaffected. The Directive provides EU law enforcement officials with the discretion to determine when an interstate data transfer may take place, and this would presumably be sufficient to allow the EU to abide by its responsibilities under the MLAT.

2. *The new legislation may affect the U.S. government's ability to place gag orders on private corporations when requesting data in the course of a criminal investigation.*

The Data Protection Regulation maintains strict requirements that processors notify consumers when their data is disclosed to a third party. These requirements could conflict with U.S. law enforcement's ability, under existing U.S. law, to place gag orders when requesting

* J.D. Candidates, Yale Law School. This report was prepared in connection with *International Law and Foreign Affairs*, a course at Yale Law School, under the supervision of Professor Oona Hathaway, Gerard C. and Bernice Latrobe Smith Professor of International Law, Yale Law School, and with the assistance of Spencer Amdur, Sally Pei, Julia Brower, Christina Koningisor, Ryan Liss, Aadhithi Padmanabhan, Michael Shih, and Tina Thomas.

certain types of data from private corporations in the course of criminal investigations. However, since the new E.U. Regulation currently exists only on a highly generalized level – and may operate very differently when put into practice – we cannot be sure how significant this concern may end up being.

3. *The new "right to be forgotten" could potentially lead corporations to erase data that might otherwise have proven relevant to future criminal investigations.*

The proposed "right to be forgotten" would require processors to delete the data of any EU citizen, upon request. While exceptions are included within the legislation for data under the control of law enforcement officials, a consumer could presumably exercise her right to be forgotten *before* law enforcement officials have identified the data as relevant and obtained it. Therefore, the ability of law enforcement to gather useful data from private corporations could be hindered by consumers' frequent exercise of the right to be forgotten. However, this problem might be mitigated by data retention laws that have been adopted by EU Member States, requiring corporations to retain data for a period of several months to a year before allowing a consumer to exercise her right to be forgotten.

Contents

INTRODUCTION

In January 2012, the European Commission released two pieces of draft legislation: the General Data Protection Regulation ("Data Protection Regulation")[1] and the Police and Criminal Justice Directive ("Criminal Justice Directive").[2] The proposed legislation is intended to replace previous EU law on data protection, including the 1995 EU Data Protection Directive ("1995 Data Protection Directive").[3] According to the current draft of the Data Protection Regulation and the Criminal Justice Directive, the legislation's requirements would apply to entities that are located outside the EU if they process data "related to: (a) the offering of goods or services to such data subjects in the [European] Union; or (b) the monitoring of their behaviour."[4] Given the importance of international trade between the United States and the EU, the proposed legislation could apply to a substantial number of U.S.-based entities. Consequently, the proposed legislation could affect the U.S. government's ability to obtain information relevant to law enforcement and counterterrorism efforts. This memo evaluates the potential impact and concludes that it will be relatively minor.

As a preliminary matter, it is useful to consider the general European approach to privacy law and how it differs from that of the United States. Whereas American privacy law is generally focused on protecting individual liberty, European privacy law is primarily focused instead on protecting human dignity.[5] As James Whitman explains:

> Continental privacy protections are, at their core, a form of protection of a right to *respect* and *personal dignity*. The core continental privacy rights are . . . closely linked forms of the same basic right: They are all rights to control your public image—rights to guarantee that people see you the way you want to be seen. They are, as it were, rights to be shielded against unwanted public exposure—to be spared embarrassment or humiliation. . . . Any . . . agent that gathers and disseminates information can . . . pose such dangers. In its focus on shielding us from public indignity, the continental conception is typical of the continental legal world much more broadly: On the Continent, the protection of personal dignity has been a consuming concern for many generations.[6]

---

[1] *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *Data Protection Regulation*].

[2] *Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences of the Execution of Criminal Penalties, and the Free Movement of Such Data*, COM (2012) 10 final (Jan. 25, 2012) [hereinafter *Criminal Justice Directive*].

[3] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L. 281) 31 [hereinafter 1995 Data Protection Directive].

[4] *Data Protection Regulation*, *supra* note 1, art. 3(2).

[5] *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004); *see also* Robert Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087 (2001) (discussing competing conceptions of privacy more generally).

[6] Whitman, *supra* note 5, at 1161.

Americans thus conceive of privacy in negative terms, as "the right to freedom from intrusions by the state, especially in one's own home."[7] When government regulation illegitimately invades this space, it limits an aspect of personal liberty.[8] However, as Europeans view privacy rights as protective of human dignity, the government must provide the same affirmative protection for privacy that European law grants to other dignity interests, which Germany, for instance, views as an absolute right.[9] If human dignity is absolute, after all, the state must affirmatively safeguard it by granting individuals unambiguous, broad-ranging rights, such as those created by the EU's new privacy legislation.

This memo begins in Part I by discussing existing EU law under the 1995 Data Protection Directive. It then examines the new legislation. Part II summarizes the 2012 Data Protection Regulation and the Criminal Justice Directive, identifying how the proposed legislation would differ from the status quo. Part III analyzes how the proposed EU legislation would affect information-sharing under the EU-U.S. Mutual Legal Assistance Treaty. It concludes that the Data Protection Regulation and the Criminal Justice Directive would not significantly affect the EU-U.S. Mutual Legal Assistance Treaty. The Criminal Justice Directive ostensibly prohibits transfers of data to non-EU Member States that the European Commission has not deemed to provide adequate data protection safeguards. But the Directive's language is flexible and allows transfers to occur if the data controller makes an independent determination that appropriate safeguards exist or if an EU Member State derogates from the Directive. Derogations are permitted if "the transfer is necessary" for a criminal investigation.[10]

Finally, Part IV identifies two ways that the proposed legislation might affect EU and U.S. law enforcement operations. First, the new Data Protection Regulation could require U.S. corporations that process EU citizens' data to inform an EU citizen whenever his or her data is disclosed to U.S. law enforcement, even if a U.S. court order would otherwise require that disclosure be kept confidential. Second, the "right to be forgotten" could allow EU citizens to demand that data that would otherwise be relevant to law enforcement operations be erased. However, the impact of the right to be forgotten on EU and U.S. law enforcement efforts will be limited. Under the Criminal Justice Directive, data that is in the control of EU or U.S. law enforcement agencies would not be subject to the right to be forgotten. Moreover, EU and Member State data retention laws already require that certain types of data be retained for a period of time, and EU citizens would not be permitted to exercise their right to be forgotten during that time.

Although the EU's proposed legislation has attracted a great deal of attention from privacy advocates and industry actors, our analysis suggests that the Data Protection Regulation

---

[7] *Id*.

[8] *Cf.* Griswold v. Connecticut, 381 U.S. 479, 485 (1965) ("The present case, then, concerns a relationship lying within the zone of privacy. . . . And it concerns a law . . . [that] cannot stand in light of the familiar principle, so often applied by this Court, that a 'governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms.'" (quoting NAACP v. Alabama, 377 U.S. 288, 307 (1964))).

[9] For example, the first line of the German constitution states that "[h]uman dignity shall be inviolable." GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND [GRUNDGESETZ] [GG] [BASIC LAW], art. 1, para. 1, May 23, 1949, BGBl. I (Ger.) (Christian Tomuchat & Donald P. Kommers trans., 2010).

[10] *Criminal Justice Directive*, *supra* note 2, art. 36(d).

and the Criminal Justice Directive will have a relatively limited impact. However, it is important to keep in mind that the new legislation may change before it is finalized. The proposed Data Protection Regulation and the Criminal Justice Directive have now moved to the European Parliament and the Council for further discussion.[11] The legislation will go into effect two years after it enters into force.[12] Nevertheless, if it remains in its current form, the new legislation should not significantly hinder EU or U.S. law enforcement.

I. 1995 EU DATA PROTECTION DIRECTIVE

We begin with the current EU data protection law, which establishes the status quo that would be altered by the proposed legislation. European data privacy law is currently governed by the 1995 EU Data Protection Directive. At the time it was adopted, the Directive was intended "to harmonize the different existing standards of data protection in Europe."[13] Each EU Member State was required to implement the Directive through domestic legislation.[14] Although the European Court of Justice has jurisdiction to force a Member State to eliminate discrepancies between the Directive and the state's implementing legislation,[15] significant variations between Member States' data protection laws remain.[16]

The 1995 Directive covers all forms of personal data, which it defines as "any information relating to an . . . identifiable natural person ('data subject')."[17] It sets forth requirements for data "processors," defined as people or entities that perform "operations . . . upon personal data, . . . such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[18]

---

[11] Procedure File: Personal Data Protection, EUROPEAN PARLIAMENT, http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en#tab-0 (last updated Dec. 3, 2012) (reporting that the proposed legislation's committee referral was announced on Feb. 16, 2012 and was debated in the Council on Oct. 25, 2012); Press Release, European Commission, Commission Proposes a Comprehensive Reform of Data Protection Rules To Increase Users' Control of Their Data and To Cut Costs for Businesses (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm [hereinafter Press Release, Commission Proposes Comprehensive Reform].

[12] *Data Protection Regulation*, *supra* note 1, art. 91; *Criminal Justice Directive*, *supra* note 2, art. 62.

[13] DOROTHEE HEISENBERG, NEGOTIATING PRIVACY: THE EUROPEAN UNION, THE UNITED STATES, AND PERSONAL DATA PROTECTION 27 (2005).

[14] *See id.*

[15] *Id.*

[16] Justin Brookman, *European Commission Proposes Stronger Data Privacy Legislation*, CTR. FOR DEMOCRACY & TECH. (Feb. 2, 2012), https://www.cdt.org/blogs/justin-brookman/22european-commission-proposes-stronger-data-privacy-legislation.

[17] 1995 Data Protection Directive, *supra* note 3, art. 2(a).

[18] *Id.* arts. 2(b), (e). The 1995 Data Protection Directive and the new proposed data protection legislation distinguish between data processors and data "controllers," who "determine[] the purposes and means of the processing of personal data." *Id.* art. 2(d). A single entity can act as both the data controller and the data processor, or the two functions can be carried out by separate entities. Accordingly, data controllers are subject to EU data protection law even if they do not process data directly.

According to scholarship on EU data protection law, the United States considered many of the 1995 Directive's requirements very strict when first adopted.[19] For example, data controllers must ensure that data is "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[20] Data must also be "adequate, relevant and not excessive in relation to the purposes for which they are collected."[21] The Directive also requires that data be "accurate" and "up to date,"[22] and EU citizens' data must be "kept in a form which permits identification of data subjects for no longer than is necessary."[23] In practice, these provisions mean "every business must be vigilant about erasing files of former employees, businesses must ensure that they make changes to the data if they are advised that they are incorrect, and businesses cannot sell names of customers to others."[24]

These guidelines permit processing if the data subject has "unambiguously given his [or her] consent."[25] Alternatively, processing is legitimate if it is necessary for one of the following: "the performance of a contract,"[26] "compliance with a legal obligation,"[27] the "protect[ion] [of] the vital interests of the data subject,"[28] or the "performance of a task carried out in the public interest."[29]

Under the Directive, data controllers must also provide certain information to data subjects. For example, articles 10 and 11 require that the data subject be informed of (1) the identity of the controller, (2) the purposes of the processing, and (3) any other relevant information, such as additional recipients of the data.[30] The data subject also has the right to access information related to his or her data, including whether the data is being processed, the purpose of such processing, and the "knowledge of the logic involved in any automatic processing of data."[31]

The Directive also imposes elaborate notification requirements on data processors. Under articles 18 and 19, processors must notify the relevant supervisory data authorities of what data they are processing and why.[32] Pursuant to the Directive, each Member State has established a supervisory authority to receive this information and monitor the application of data protection laws within the country.[33] Each supervisory authority possesses investigative and quasi-

[19] HEISENBERG, *supra* note 13, at 29.
[20] 1995 Data Protection Directive, *supra* note 3, art. 6(1)(b).
[21] *Id.* art. 6(1)(c).
[22] *Id.* art. 6(1)(d).
[23] *Id.* art. 6(1)(e).
[24] HEISENBERG, *supra* note 13, at 29.
[25] 1995 Data Protection Directive, *supra* note 3, art. 7(a). The Directive is somewhat unclear as to what qualifies as "unambiguously given consent." For example, some have questioned whether the Directive requires data subjects to "opt in" to data collection. *See* HEISENBERG, *supra* note 13, at 29.
[26] 1995 Data Protection Directive, *supra* note 3, art. 7(b).
[27] *Id.* art. 7(c).
[28] *Id.* art. 7(d).
[29] *Id.* art. 7(e).
[30] *Id.* art. 10.
[31] *Id.* arts. 12, 15.
[32] *Id.* arts. 18-19.
[33] *Id.* art. 28.

prosecutorial authority.[34] Additionally, the Directive established a Working Party comprising representatives from each member state's supervisory authority, one representative of the supervisory authority that oversees European Community institutions, and one representative of the Commission.[35]

The Commission was granted the power to determine whether non-EU countries ensure "an adequate level" of data protection.[36] Data controllers and processors are prohibited from transferring data to countries that do not receive an adequacy determination.[37] However, under article 26 of the Directive ("Derogations"), Member States may permit data transfers to non-adequate countries if "the controller adduces adequate safeguards," but they must notify the Commission and the other EU Member States of their decision.[38] However, the European Commission has suggested that while article 26 could "offer[] a permanent[] solution[] for situations in which [they] cannot make [an adequacy determination]," their strong preference in the long term is to share data pursuant to an adequacy determination.[39]

In sum, the 1995 Data Protection Directive established ambitious standards for data protection. However, because the legislation took the form of a directive, states were responsible for implementing the document's broad language. In practice, this has resulted in wide variation in Member States' national data protection laws. For example, EU Member States vary on how they define "consent" in their national data protection laws. While Finland's law repeats the Directive's consent language verbatim, the Luxembourg data protection law additionally requires that consent be "explicit" and "unambiguous," and allows consent to be given by a data subject's "legal representative."[40] These variations can dramatically affect the scope of data protection law in EU Member States. In the UK, for example, the data protection law applies to "living individuals," while in Denmark the data protection law is read to apply to deceased persons as well.[41] Consequently, a company that processes data from multiple EU Member States must juggle these diverse requirements. In order to address these and other variations, the European Commission has proposed a new Data Protection Regulation and Criminal Justice Directive. The following Part compares the proposed legislation to the existing Data Protection Directive.

---

[34] *Id.* art. 28(3).
[35] *Id.* art. 29. The Working Party is commonly referred to as "the Article 29 Working Party." *See Article 29 Working Party*, EUROPEAN COMM. (Mar. 2, 2012), http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.
[36] 1995 Data Protection Directive, *supra* note 3, art. 25.
[37] *Id.* art. 25(1). In order to address this restriction, the U.S. Department of Commerce negotiated a "Safe Harbor Agreement" that allowed companies to freely transfer data to and from EU Member States, provided the companies abided by the Safe Harbor principles. Those principles included requirements for notice, security, data integrity, and access. *See U.S.-EU Safe Harbor Overview*, EXPORT.GOV (Apr. 26, 2012), http://export.gov/safeharbor/eu/eg_main_018476.asp.
[38] 1995 Data Protection Directive, *supra* note 3, art. 26(2)-(3).
[39] Susan Binns, Technical Briefing for Journalists on Data Protection—EU/US Dialogue (Dec. 10, 1998), http://ec.europa.eu/justice/policies/privacy/thridcountries/briefing-eu-us-dialog_en.htm.
[40] DOUWE KORFF, EUROPEAN COMM'N, REPORT ON THE IMPLEMENTATION OF THE EC DIRECTIVE ON DATA PROTECTION 32 (2002).
[41] *Id.* at 39.

II. 2012 PROPOSED EU REGULATIONS

In January 2012, the European Commission approved the proposed General Data Protection Regulation and Police and Criminal Justice Data Protection Directive. These instruments were meant to replace the 1995 Directive on Personal Data Protection.[42] During the period following the adoption of the 1995 Directive, the EU had enshrined "the right [of everyone] to the protection of personal data concerning him or her" in the Charter of Fundamental Rights,[43] clearly demonstrating the priority the EU places on data protection. However, the Charter is light on details and did not address the fragmentation of data protection standards that had developed across the EU. Moreover, as discussed above, the 1995 Directive was not directly enforceable by the courts of EU Member States. Instead, each Member State was required to pass implementing legislation. As the advocacy group European Digital Rights explained, "[L]egislators and regulators in the 27 EU Member States implement the Directive in 27 different ways. Harmonisation in the form of a single, directly applicable instrument is . . . needed to ensure legal certainty in the single European market."[44] The new Data Protection Regulation would address this fragmentation because it would be directly applicable law in EU Member States.[45]

A. The Proposed Data Protection Regulation

The EU's proposed Data Protection Regulation retains many of the standards established in the 1995 Directive. The most dramatic change is likely the form of the instrument: by drafting it as a regulation rather than as a directive, the new document will be legally binding in its entirety on EU Member States.[46] This should address the concern of civil society and industry actors that have criticized the 1995 Directive for resulting in varied privacy regulations across the EU. In addition to being legally binding, the new regulation provides for a more streamlined regulatory process—one that is unified across the twenty-seven member states of the EU—and it will expand the rights of data subjects—for example, by providing a more robust "right to be forgotten." We discuss each development briefly in turn.

---

[42] Press Release, Commission Proposes Comprehensive Reform, *supra* note 11.

[43] Charter of Fundamental Rights of the European Union art. 8, Dec. 7, 2000, 2000 O.J. (C 364) 1; *see also* Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Communities art. 16, Dec. 13, 2007, 2007 O.J. (C 306) 1 [hereinafter Treaty of Lisbon] ("Everyone has the right to the protection of personal data concerning them.").

[44] *EDRi Initial Comments on the Proposal for a Data Protection Regulation*, EUROPEAN DIGITAL RIGHTS (Jan. 27, 2012), http://edri.org/CommentsDPR.

[45] Jane Finlayson-Brown, *How to Prepare for Proposed EU Data Protection Regulation*, COMPUTERWEEKLY (Mar. 2012), http://www.computerweekly.com/opinion/Proposed-EU-Data-Protection-Regulation-what-should-companies-be-thinking-about.

[46] *See* Lisbon Treaty, *supra* note 43, art. 288. A directive is binding on Member States only as to the result to be achieved; in contrast, a regulation is binding as to the result as well as to the means.

1. Streamlined Process

In order to streamline the regulatory process, the new Regulation will subject a company to one lead national data protection regulator, rather than twenty-seven different authorities.[47] Previously, if a company was based in France but had satellite locations in other EU Member States, the company would need to report to the French data protection authority as well as the national data protection authorities governing each satellite location.[48] Under the new Regulation, a company would only be supervised by the data protection authority in the nation in which the "main establishment" of the company is located.[49] Thus, a company headquartered in France would only be required to report to the French data protection authority. According to the European Commission, this streamlining effort would save businesses around 2.3 billion euros a year.[50]

The new Regulation will apply to any entity that controls the data of EU subjects even if the entity is not located in the EU.[51] According to article 3 of the Regulation, it "applies to the processing or personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour."[52] In such cases, the Regulation requires that companies "designate a representative in the Union" located in one of the Member States where the data subjects reside.[53] This representative would then be required to report to the supervisory authority in the member state in which the representative is located.[54] However, this requirement will not apply to companies that employ fewer than 250 persons, public authorities, an entity that offers "only occasionally goods or services to data subjects residing in the Union," or any other entity that is located in a country that the Commission has decided "ensures an adequate level of protection."[55]

Even if an entity does fall under the jurisdiction of one of the data protection authorities, the new Regulation will reduce the burden placed on the entity. While the 1995 Data Protection Directive requires companies to provide each supervisory authority with pro forma notification before processing any data,[56] the new Regulation will only require that companies maintain

---

[47] *Data Protection Regulation*, *supra* note 1, art. 51(2); *see* Explanatory Memo, *Data Protection Regulation*, *supra* note 1, at 12; Press Release, Commission Proposes Comprehensive Reform, *supra* note 11.

[48] *How will the EU's data protection reform simplify the existing rules?*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/6_en.pdf (last visited Dec. 1, 2012).

[49] *Data Protection Regulation*, *supra* note 1, art. 51(2).

[50] Press Release, Commission Proposes Comprehensive Reform, *supra* note 11.

[51] It should be noted that many large U.S. corporations have offices in EU Member States and would thus already be subject to EU data protection law. These corporations are likely already familiar with complying with European privacy regulations. *See* Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991, 1020 (1998) ("[L]arge processors of information . . . . typically have large operations in Europe and are clearly subject to enforcement actions there. . . . [W]e would expect the websites of [these companies] to comply relatively well with national laws and to install relatively strict privacy policies.").

[52] *Data Protection Regulation*, *supra* note 1, art. 3(2).

[53] *Id.* art. 25.

[54] *Id.* art. 28(3) ("[T]he controller's representative[] shall make . . . documentation available, on request, to the supervisory authority."); *id.* art. 51(1) ("Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.").

[55] *Id.* art. 25(2).

[56] 1995 Data Protection Directive, *supra* note 3, art. 18.

documentation regarding data processing and provide the supervisory authority with that information upon request.[57]

2. Expanded Rights for Data Subjects, Including the "Right To Be Forgotten"

Although the new Regulation provides for a more streamlined process, it also expands the rights of data subjects and imposes additional requirements on entities that process data in a number of key ways. Under the new Regulation, consumers must give their explicit consent before a company begins processing their personal data.[58] Additionally, corporations will be required to designate "data protection officers" to ensure compliance with the regulation.[59] These officers must be "involved in all issues which relate to the protection of personal data" and must "perform[] the duties and tasks independently and does not receive any instructions as regards the exercise of the function."[60] Unlike the reporting requirement, public authorities are *not* exempted from this requirement.[61]

The new Regulation also affords EU citizens the right to request to have one's data erased from a database and from all other public fora to which the data has been released, which the Data Protection Regulation refers to as the "right to be forgotten."[62] Under article 17, the right to be forgotten applies only when the data is no longer necessary "in relation to the purposes" for which it was obtained, the data subject has revoked his or her consent, the data subject disputes the legitimacy of the processing of the data, or the processing of the data does not abide by the Regulation for any other reason.[63] The broad language of article 17 gives the data subject the right to obtain erasure of a wide range of data related to him or her.[64] Article 17 does state, however, that a data controller may retain the data if it is necessary for compliance

---

[57] *Data Protection Regulation*, *supra* note 1, art. 28(1)-(3).

[58] *Id.* arts. 4-10. Although the 1995 Data Protection Directive required that data subjects provide their consent "unambiguously," uncertainty existed as to what exactly constituted unambiguous consent. For a brief discussion of this question, see Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 14 n.44 (2000).

[59] *Data Protection Regulation*, *supra* note 1, arts. 35-37.

[60] *Id.* art. 36.

[61] *Id.* art. 35(1).

[62] *Id.* art. 17. As Hans Graux, Jef Ausloos, and Peggy Valcke point out in their recent paper, the right to be forgotten had a "passive" precursor in Article 6(1) of the 1995 Data Protection Directive, which requires that data be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed" and which mandates that "data which [is] inaccurate or incomplete, having regard to the purposes for which [it was] collected or for which [it was] further processed, [be] erased or rectified." Hans Graux et al., *The Right To Be Forgotten in the Internet Era* 10 (Interdisciplinary Cen. for Law & ICT, Working Paper No. 11, 2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2174896 (quoting 1995 Data Protection Directive, *supra* note 3, arts. 6(1)(e), 6(1)(d)). However, practically speaking, there has been little enforcement of this rule. *Id.*

[63] *Data Protection Regulation*, *supra* note 1, art. 17(1).

[64] Graux, Ausloos, and Valcke found the ability to request erasure based on withdrawn consent to be particularly noteworthy, arguing that "giving individuals the possibility to unilaterally end their relationship with a data controller/processor[] addresses an important imbalance in the current data protection regime" because "data processing based on consent very frequently fails to offer true choice and control to the data subject." Graux et al., *supra* note 62, at 13-14. In other words, data subjects often provide their consent without fully understanding how their data will be processed, and the right to be forgotten gives them an opportunity to retroactively withdraw consent to "data that was lawfully processed." *Id.* at 14.

with data retention laws.[65] This could allow EU Member States to require that certain information be retained for law enforcement purposes. However, data retention laws must "meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued."[66] It may be difficult for EU Member States to develop data retention laws that are broad enough to cover all information that may be relevant to an investigation, yet narrow enough to remain "proportionate."[67]

The Regulation remains in draft form, but if its final version is mostly consistent with the central provisions of the current draft, it will likely result in a more streamlined process for entities that process data inside and outside the EU. However, the expanded scope of data subjects' rights will likely mean that companies have less control over the data that they process and retain. The Regulation's impact on *private data collection* has implications for U.S. law enforcement, which often seeks to compel disclosure of data from private entities or relies on those entities to disclose information voluntarily—implications we discuss more fully in Part III below. First, however, we turn to the impact of the Regulations on *public data collection*—which is addressed in a separate Police and Criminal Justice Data Protection Directive.

B. Police and Criminal Justice Data Protection Directive

The new Data Protection Regulation does not apply to data maintained as part of law enforcement activities.[68] Such data is expressly exempt from the Regulation.[69] To address data privacy issues arising in the context of criminal investigations, the European Commission has instead proposed a Directive on Police and Criminal Justice Data Protection.[70] Because it is a Directive, rather than a Regulation, individual EU Member States will have significant flexibility in how they implement its requirements. Moreover, the Directive by its own terms gives a great deal of discretion to EU Member States and data controllers. Hence, the new proposed Directive is unlikely to have a major impact on data maintained by the law enforcement officials in EU Member States or the United States.

Similar to the General Data Protection Regulation, the Police and Criminal Justice Directive expands on the rights of data subjects and imposes additional requirements on data controllers when compared to the 1995 Data Protection Directive. Under both instruments, personal data must be processed lawfully and fairly and "collected for specified, explicit and legitimate purposes."[71] Both also limit the processing of sensitive categories of data, including personal data that reveals "race or ethnic origin."[72] Additionally, under both instruments, data

---

[65] *Data Protection Regulation*, *supra* note 1, art. 17(3)(d).
[66] *Id.*
[67] See discussion *infra* Section IV.C.
[68] *Data Protection Regulation*, *supra* note 1, art. 2(2).
[69] *Id.*
[70] *Criminal Justice Directive*, *supra* note 2, art. 1(1). Neither the Data Protection Regulation nor the Criminal Justice Directive apply to data that is processed "in the course of an activity which falls outside the scope of Union law, in particular concerning national security." *Data Protection Regulation*, *supra* note 1, art. 2(2)(a); *Criminal Justice Directive*, *supra* note 2, art. 2(3)(a).
[71] *Criminal Justice Directive*, *supra* note 2. art. 4(a)-(b); *Data Protection Regulation*, *supra* note 1, art. 5(a)-(b).
[72] *Criminal Justice Directive*, *supra* note 2, art. 8; *Data Protection Regulation*, *supra* note 1, art. 9.

subjects have the right to obtain the "rectification" of inaccurate or incomplete data relating to them, although the Criminal Justice Directive permits Member States to refuse to rectify data provided they furnish the data subject with a written refusal explaining why the request was denied.[73] Both instruments also require data controllers to inform the supervisory authority in the case of any breach of the data,[74] and to designate an individual as a "data protection officer."[75]

However, the Directive includes important exceptions to the rights and duties set forth in the General Data Protection Regulation. These exceptions grant Member States a much larger degree of flexibility on how much information they are required to share with the data subject. According to article 11 of the Directive, "Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject to the extent that, and as long as, such . . . restriction constitutes a necessary and proportionate measure in a democratic society . . . ."[76] The Directive also outlines legitimate interests for which Member States may decline to inform the data subject, including "(a) to avoid [legal] obstruct[ion] . . . ; (b) to avoid prejudicing . . . [criminal] investigation and prosecution; (c) to protect public security; (d) to protect national security; [and] (e) to protect the rights and freedoms of others."[77] Article 13 applies a similar exemption to the right of data subjects to access data relating to them.[78] Based on this exception, EU law enforcement officials would generally not be required to disclose the fact that they are processing data related to a suspect, which could potentially alert the data subject of the investigation. EU privacy advocates have criticized these provisions on the basis of these concerns.[79]

Similarly, the Directive severely limits the "right to be forgotten." Article 16 declares that data subjects may obtain erasure of personal data, but only when the processing does not comply with article 4(a) to (e), article 7, and article 8.[80] Article 4 sets forth requirements for how data must be processed, including requirements that the data must be processed fairly, collected for a legitimate purpose, relevant, and accurate.[81] Article 7 describes what constitutes lawful processing for the purposes of the Directive.[82] Article 8 prohibits the processing of personal data revealing "race or ethnic origin, political opinions, religion or beliefs, trade-union membership" as well as "genetic data" and "data concerning health or sex life."[83] Therefore, the right to be forgotten under the Directive only applies to data that law enforcement officials have obtained in violation of the other provisions of the Directive. Provided law enforcement officials stay within the bounds of articles 4, 7, and 8, they need not comply with a data subject's request for erasure. Moreover, article 16 grants Member States the ability to refuse erasure if "the personal data have

[73] *Criminal Justice Directive*, *supra* note 2, art. 15; *Data Protection Regulation*, *supra* note 1, art. 16.
[74] *Criminal Justice Directive*, *supra* note 2, art. 28; *Data Protection Regulation*, *supra* note 1, art. 31.
[75] *Criminal Justice Directive*, *supra* note 2, arts. 30, 31(2); *Data Protection Regulation*, *supra* note 1, arts. 35, 36(2).
[76] *Criminal Justice Directive*, *supra* note 2, art. 11(4).
[77] *Id.*
[78] *Id.* art 13(1).
[79] Article 29 Data Protection Working Party, *Opinion 01/2012 on the Data Protection Reform Proposals*, 28-29 (Mar. 23, 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.
[80] *Criminal Justice Directive, supra* note 2, art. 16.
[81] *Id.* art. 4.
[82] *Id.* art. 7.
[83] *Id.* art. 8.

to be maintained for purposes of proof."[84] Such an exemption seems quite permissive for EU law enforcement officials. Presumably, much of the data that law enforcement officials would be interested in obtaining would fall under this exemption.

Like the Regulation, the Directive places limitations on the transfer of data to non-EU Member States. However, the numerous exceptions to the transfer provision allow for a great deal of flexibility here as well. The Directive, like the Regulation, prohibits EU Member States from transferring data to non-EU Member States unless the Commission finds that the non-EU Member State "ensures an adequate level of [data] protection."[85] Yet even if the Commission fails to do so (or has yet to do so), a Member State may transfer data to the non-EU Member State if the two countries adopt a legally binding instrument setting forth "appropriate safeguards" regarding data protection.[86] Alternatively, the EU Member State can forego adopting a legal instrument if it "concludes that appropriate safeguards exist."[87] Finally, if the Member State chooses to do so, it can simply derogate from its obligations under the transfer provision if the transfer is "necessary" to achieve certain aims, including prevention, investigation, detection or prosecution of crime.[88] Derogation is also permitted if the transfer is "essential for the prevention of an immediate and serious threat to public security."[89]

Earlier drafts of the Directive imposed new, harsh restrictions on the transfer of data to states outside the EU, but those changes were altered in response to U.S. lobbying, according to some reports.[90] Some critics claim that the proposed rules on transferring data between states for purposes of criminal investigations and prosecutions are now virtually identical to the status quo.[91] Indeed, an anonymous EU official has been quoted as saying that "[e]xisting EU-U.S. deals will not be challenged by the new proposals."[92] As the above discussion explains, the Police and Criminal Justice Directive largely preserves the status quo. The legislation's flexible language should address any concerns that EU and U.S. law enforcement may have with the expanded scope of individual rights and the additional requirements imposed on government data controllers under the new Criminal Justice Directive.

III. IMPLICATIONS FOR U.S. AND EU LAW ENFORCEMENT

We now turn to examining the implications of the new legislation for U.S. and EU law enforcement. Generally, the language of the proposed legislation is sufficiently flexible that the impact on U.S. and EU law enforcement should be limited. We conclude that, due to the broad

[84] *Id.* art. 16(3)(b).
[85] *Id.* art. 34(1).
[86] *Id.* art. 35(1).
[87] *Id.* According to the Directive, "duly authorised staff" must make the determination that a non-EU Member State has appropriate safeguards and the Member State that is transferring the data must make documentation of the transfer available to the supervisory authority if requested. *Id.* art. 35(2).
[88] *Id.* art. 36.
[89] *Id.* art 36(c).
[90] *U.S. Lobbying Waters Down EU Data Protection Reform*, EURACTIV, Feb. 21, 2012, http://www.euractiv.com/specialreport-data-protection/us-lobbying-waters-eu-data-prote-news-510991.
[91] *EDRi Initial Comments on the Proposal for a Data Protection Regulation*, EUROPEAN DIGITAL RTS. (Jan. 27, 2012), http://edri.org/CommentsDPR.
[92] *U.S. Lobbying Waters Down EU Data Protection Reform*, *supra* note 90..

language written into the Police and Criminal Justice Directive, the new legislation should not affect EU-U.S. law enforcement cooperation under the EU-U.S. Mutual Legal Assistance Treaty. However, we recognize that much of the language in the proposed Data Protection Regulation and Criminal Justice Directive is somewhat ambiguous; we, therefore, cannot predict how the new legislation will be implemented. That being said, our research suggests that law enforcement efforts could be impacted in the following two ways: first, if private entities are compelled under the new Data Protection Regulation to provide the U.S. government with data related to EU citizens, they may be required to inform the data subjects of the disclosure—which could, in turn, affect law enforcement efforts; and second, the "right to be forgotten" could lead to data being erased that is relevant to law enforcement operations of the United States and of EU Member States.

A. The EU-U.S. Mutual Legal Assistance Treaty (MLAT) Will Not Be Affected by the Draft Regulation and Directive

1. Overview of the EU-U.S. MLAT

The 2003 EU-U.S. MLAT was intended to "formalize and strengthen the institutional framework for law enforcement relations between the United States and the European Union."[93] The treaty modernized existing bilateral mutual legal assistance agreements and served as a model for the creation of agreements with EU Member States.[94] Upon the treaty's transmission to the Senate for advice and consent in 2006, President Bush also submitted bilateral implementing instruments with all twenty-five EU Member States.[95] The MLAT contains a range of provisions that are meant to enhance legal cooperation between the U.S. and EU Member States. For example, it sets forth procedures for identifying bank information for natural or legal persons suspected of or charged with a criminal offense (art. 4), for establishing and operating joint investigative teams (art. 5), and for using videoconferencing technology to take and transmit witness testimony (art. 6).[96]

Notably, the EU-U.S. MLAT also sets forth limitations on the use of information "to protect personal and other data."[97] However, these limitations are extremely narrow. According to article 9(1), a State that is requesting information "may use any evidence or information obtained from the requested State" for "criminal investigations and proceedings," for "preventing an immediate and serious threat" to public security, or for "non-criminal judicial or administrative proceedings directly related to" the previously referenced criminal matters.[98]

---

[93] Letter from the President Transmitting the EU-U.S. Mutual Legal Assistance Agreement, Sept. 28, 2006, S. Treaty Doc. No. 109-13 (2006).
[94] Letter from the Secretary of State Submitting the EU-U.S. Mutual Legal Assistance Agreement, Aug. 3, 2006, S. Treaty Doc. No. 109-13, at V (2006).
[95] *Id.* Although the EU-U.S. MLAT served as a model for the bilateral agreements with individual EU Member States, there are a small number of differences between the treaties. For a detailed discussion of how the bilateral treaties differ from the framework agreement, see *id.* at XVII-XXXVII.
[96] Agreement on Mutual Legal Assistance Between the United States of America and the European Union arts. 4-6, Aug. 3, 2006, S. Treaty Doc. No. 109-13 (2006) [hereinafter EU-U.S. MLAT].
[97] *Id.* art. 9.
[98] *Id.* art. 9(1)

According to article 9(1), a requesting State may use the requested information "for *any other purpose*" if the information has been made public as a result of the proceedings for which they were obtained or if the "requested State" (the State from which the information is requested) provides prior consent.[99] In other words, if the requested information is made public as part of the proceeding for which it was originally requested, the requesting State can use the information for a different criminal or non-criminal case. This formulation was "broader . . . than in pre-existing MLATs that require the consent from the requested State if the evidence or information is to be used for an investigation or proceeding different from that set forth in the request."[100] A requesting State would be limited in its use of a particular piece of information only if it could not find a way to make the information public in a proceeding (e.g., it is inadmissible under the applicable rules of evidence) or if it fails to obtain the consent of the requested State.

Article 9 goes on to state that "[g]eneric restrictions with respect to the legal standards of the requesting State for processing personal data may not be imposed by the requested State as a condition . . . to provide evidence or information."[101] Further demonstrating the preference for uninhibited information sharing, the MLAT allows States to "apply the use limitation provisions" of their other bilateral agreements, provided those provisions "result in *less* restriction on the use of information and evidence" than article 9 of the EU-U.S. MLAT imposes.[102] According to the State Department's analysis of the MLAT, this provision applied to bilateral MLATs "in which there is no use limitation unless specifically invoked by the requested State. In such cases, the requested State remains free to impose no limitation."[103] As we explain in the next Section, the proposed EU Data Protection legislation does contain provisions that limit data transfers, but in practice they would not be more restrictive than those limitations already imposed by the 2003 MLAT. Unfortunately, as we will discuss below, transfers would likely occur under the Criminal Justice Directive on a case-by-case basis. This may delay law enforcement investigations that require data transfers.

2. The EU Criminal Justice Directive Contains Flexible Language on Data Transfers that Would Not Conflict with the MLAT

Based on the flexible language contained in the final version, the draft Criminal Justice Directive's provisions on data transfers should not conflict with the information sharing framework established by the EU-U.S. MLAT. The Criminal Justice Directive ostensibly prohibits data transfers when the Commission has failed to find the requesting State "ensures an adequate level of protection."[104] But it allows the transfer to take place without a formal finding by the Commission if "the controller or processor has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data."[105] A U.S. law enforcement official would likely have an easier time convincing an individual controller, rather than the entire European Commission, as to the

[99] *Id.* art. 9(1)(d)-(e) (emphasis added).
[100] Letter from the Secretary of State, *supra* note 94, at XV.
[101] EU-U.S. MLAT, *supra* note 96, art. 9(2)(b).
[102] *Id.* art. 9(4).
[103] Letter from the Secretary of State, *supra* note 94, at XV.
[104] *Criminal Justice Directive*, *supra* note 2, art. 34.
[105] *Id.* art. 35(1)(b).

adequacy of the existing safeguards—particularly if that controller is the U.S. law enforcement official's European law enforcement counterpart.

Even if the United States is unable to convince a controller or processor that its safeguards are appropriate, an EU Member State may derogate from the adequacy requirement for a number of reasons, including because

> the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; or . . . the transfer is necessary in individual cases for the establishment, exercise, or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal penalty.[106]

These exceptions would likely include information requests connected to any form of law enforcement activity.

There is an important caveat, however. The Criminal Justice Directive's language suggests that these exceptions must be exercised on a case-by-case basis, which could potentially lead to delays in otherwise fast-paced law enforcement operations. It is impossible to predict how the Directive will be implemented, and it could be that this obstacle is relatively minor in practice. If this process results in significant delays, it may be preferable for the United States Government or particular law enforcement entities to obtain a decision by the European Commission, pursuant to article 34 of the Directive, that U.S. data protection policies are adequate.[107]

B. The Proposed General Data Protection Regulation Would Require Data Controllers To Notify Data Subjects When the Controller Discloses their Data to the U.S. Government

While we suspect that the Police and Criminal Justice Data Protection Directive will have a limited impact on the information sharing arrangement established by the EU-U.S. MLAT, it is possible that it will affect the ability of U.S. law enforcement officials to access information that is currently controlled by third parties, including in particular private corporations.

The new Regulations are designed to apply to any company that offers goods or services or monitors the behavior of EU citizens, even when those companies are based outside the EU.[108] Compliance with this provision would even be interpreted to require that these non-EU companies establish a designated representative to the EU, provided certain exceptions do not apply.[109] And it would require non-EU companies to abide by the Regulation's numerous consumer protection rights, including the right to be forgotten.

---

[106] *Id.* art. 36(d)-(e).

[107] In 2007, the United States negotiated an adequacy agreement with the EU that allows the sharing of air passenger name records, suggesting that the Commission is willing to cooperate with the United States on national security and law enforcement efforts. *See* Agreement Between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security, July 23-26, 2007, 2007 O.J. (L 204) 18.

[108] *Data Protection Regulation*, *supra* note 1, art. 3(2).

[109] *Id.* art. 25.

Any corporation that does not abide by the Regulation could be sued in the court that has jurisdiction over the EU resident lodging the complaint.[110] These corporations could also be subject to additional administrative sanctions and penalties.[111] Failing to comply with the right to be forgotten, for example, carries a fine of up to €500,000 or 1% of the company's annual turnover.[112]

The Regulation will thus force many U.S. companies that process data on EU citizens to abide by the EU regulations or risk paying large fines and/or dealing with frequent lawsuits. The Regulation strictly controls corporations' ability to share data without first gaining approval from EU regulators or consent from the individual whose data is being shared.[113] It also requires data controllers to notify data subjects that their information has been transferred and processed.[114] This is certain to affect aspects of U.S. criminal investigations. To clarify the implications, we first provide an overview of U.S. law enforcement tools for obtaining personal data from third parties before examining how these tools will likely be affected by the proposed Regulations.

1. Background on U.S. Law Enforcement Tools for Obtaining Personal Data from Third Parties

U.S. law enforcement officials have a range of tools at their disposal to access the type of data that is covered by the EU General Data Protection Regulations. These tools include general search and seizure procedures—limited by the Fourth Amendment of the U.S. Constitution—applied to computers and other forms of electronic equipment, governmental requests for information pursuant to the Electronic Communications Privacy Act, and the procedure for issuing National Security Letters under the Patriot Act.

The Fourth Amendment limits the ability of U.S. law enforcement agents to search for and seize evidence.[115] Generally, a government actor must obtain a warrant to access information on an individual's computer or electronic device when the individual enjoys a reasonable expectation of privacy in the electronic information. Courts have sometimes analogized a computer to a suitcase, footlocker, or briefcase, holding that the owner of a computer has a reasonable expectation of privacy in the contents of a computer.[116] However, individuals may lose that expectation of privacy when a third party controls their electronic information.[117] Some

---

[110] *Id*. art. 75.
[111] *Id*. arts. 78-79.
[112] *Id*. art. 79(5).
[113] *Id*. arts. 41, 42, 44(1)(a).
[114] *Id.* art. 14(1).
[115] U.S. CONST. amend. IV.
[116] U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 3 (2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (citing United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (finding a reasonable expectation of privacy in a personal computer); United States v. Buckner, 473 F.3d 551, 554 n.2 (4th Cir. 2007) (same); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers.")).
[117] *See* United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995) (finding that the sender's expectation of privacy in a letter "terminates upon delivery").

courts have held that this logic applies to email communications as well.[118] Whether an individual retains a reasonable expectation of privacy in data sent to a third party depends in part on the degree to which the data subject expects to retain control over the data.[119] This is particularly relevant for the storage of data on electronic servers when the owner of the data does not intend to share the information with anyone.

The Electronic Communications Privacy Act (ECPA) established "Fourth Amendment-like" privacy protections for electronic communications.[120] The Act governs when such information can be requested by government actors or voluntarily disclosed by private parties. According to 18 U.S.C. § 2703, the government can compel companies to disclose information related to Internet users, provided the government takes certain steps, such as obtaining a search warrant, a subpoena, or a court order offering "specific and articulable facts showing that there are reasonable grounds to believe" the information is "relevant and material to an ongoing criminal investigation."[121] However, if the government chooses to use a subpoena or court order, it must provide "prior notice . . . to the subscriber or customer."[122]

The ECPA also regulates voluntary disclosure of information by private entities. Non-content information can be freely disclosed to nongovernment entities.[123] For example, private entities often disclose non-content information to other private corporations for marketing purposes.[124] Content information may also be voluntarily disclosed under a limited number of circumstances, including if it is disclosed to the intended recipient, if disclosure is authorized by law, if disclosure is consented to by the originator or recipient, and if it relates to child exploitation (and in that case only to the National Center for Missing and Exploited Children).[125] Content information may also be disclosed to the government if it relates to an emergency involving danger of death or serious physical injury.[126]

---

[118] *See, e.g.*, Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001).
[119] *See, e.g.*, United States v. James, 353 F.3d 606, 614 (8th Cir. 2003) (finding that the defendant retained a reasonable expectation of privacy in a sealed envelope containing computer disks that he had left with a friend for storage).
[120] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212 (2004).
[121] 18 U.S.C. §§ 2703(b)-(1)(B)(ii), 2703(d) (2006).
[122] *Id.* § 2703(b)(1)(B).
[123] *Id.* § 2702(c)(6). The distinction between content and non-content information may seem obvious—for example, the body of an email is clearly content information, while the time that the email was sent is non-content information—but disagreement exists about the boundary between the two types of information. While the email address to which an email is sent may not sound like content information, if it belongs to a mailing list of known political dissidents, it could invite an inference that the sender somehow endorses the dissidents' views or identifies with their cause. For a sample of the debate in the literature, see Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1287-1288 (2004) (arguing that the distinction between content and non-content information "is not always clear"); and Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1034-1037 (2010) (acknowledging that distinguishing between content and non-content information will lead to "difficult cases," but arguing that "the existence of difficult cases does not provide a reason that . . . the distinction should not be drawn").
[124] Kerr, *supra* note 120, at 1220.
[125] *See* 18 U.S.C. § 2702(b).
[126] *See id.*

Finally, the Patriot Act amended the ECPA and several other federal statutes, expanding the authority of law enforcement officials to issue National Security Letters (NSLs) seeking general "non-content" information from companies on online transactions, phone numbers dialed, email addresses emailed (but not the actual text of emails or recording of phone calls), and the like.[127] These records are gathered in order to find trends that point to illegal behavior (terrorism, fraud, organized crime). The FBI may use NSLs without first receiving a warrant from a judge, and it may also obtain a gag order that prevents companies from disclosing to consumers that their data has been shared. It is here that the current law enforcement practice is likely to conflict with the new EU regulations. [128]

2. The Proposed General Data Protection Regulation May Require Data Controllers to Inform EU Citizens when Their Data is Disclosed to U.S. Law Enforcement

The General Data Protection Regulation requires data controllers to notify data subjects of the "recipients of the[ir] personal data" and "that the controller intends to transfer [his or her data] to a third country."[129] Under the statutory framework established by the ECPA and the Patriot Act, law enforcement authorities can rely on gag orders to conduct investigations without alerting the data subject. Theoretically, this could put a private entity in a difficult situation in which it must choose between violating a U.S. court authorized gag order or violating the EU Data Protection Regulation and receiving a hefty fine. Currently, the General Data Protection Regulation and the Police and Criminal Justice Data Protection Directive provide no guidance on how to resolve this conflict.[130]

However, this conflict may actually have less of an impact on U.S. law enforcement than one would initially think. First, under the proposed Data Protection legislation, the requirement to inform data subjects would not apply to non-EU residents.[131] Moreover, U.S. law enforcement officials could attempt to obtain the information from their EU counterparts under the MLAT. Under the Criminal Justice Directive, Member States may adopt legislative measures that allow law enforcement officials to delay, restrict, or omit the information that they would otherwise

---

[127] *See National Security Letters*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/nsl/ (last visited Dec. 1, 2012).

[128] *See* Andrew Charlesworth, *Europe's New Data Protection Laws Will Cause Conflict with the US, Warn Legal Experts***,** COMPUTING.CO.UK (Mar. 13, 2012), http://www.computing.co.uk/ctg/news/2162386 /europe-s-protection-laws-cause-conflict-warn-legal-experts. For a description of NSLs generally, see *National* -security-technology-and-liberty/national-security-letters.

[129] *Data Protection Regulation*, *supra* note 1, art. 14(1).

[130] Some industry observers have suggested that companies will likely follow the requirements of their home jurisdiction, meaning that U.S. companies that process data of EU citizens would likely comply with a request under the PATRIOT Act, even if doing so results in a violation of EU data protection laws. *See* Patrick Baillie, *Can European Firms Legally Use U.S. Clouds to Store Data?*, FORBES.COM (Jan. 2, 2012, 6:05 PM), http://www.forbes.com/sites/ciocentral/2012/01/02/can-european-firms-legally-use-u-s-clouds-to-store-data/. In 2011, Microsoft indicated that, pursuant to a general policy decision that predated the Regulation, it would comply with requests by U.S. law enforcement under the PATRIOT Act, even if the relevant data is stored in EU based datacenters. Zack Whittaker, *Microsoft Admits Patriot Act can Access EU-based Cloud Data*, ZDNET (June 28, 2011), http://www.zdnet.com/blog/ igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225. Gordon Frazer, managing director of Microsoft UK, suggested that "customers would be informed [of data transfers] whenever possible," but he said that Microsoft could guarantee that customers would be informed if they received a gag order or injunction: "Microsoft cannot provide those guarantees. Neither can any other company." *Id.*

[131] *See Data Protection Regulation*, *supra* note 1, art. 3(2).

provide to EU residents when their data is collected.[132] Therefore if U.S. law enforcement officials wanted to obtain data related to, for example, an Irish resident without alerting him or her of the investigation, they could request the information from an Irish law enforcement agency, which, under Irish law, can obtain information without informing the data subject.[133]

C. The "Right To Be Forgotten" Could Lead to the Erasure of Data That Would Otherwise be Relevant to Law Enforcement Officials

The existence of the "right to be forgotten" also means that the records held by most companies could be erased at the request of consumers. This could potentially impact the ability of law enforcement agencies to derive useful information from these companies over the course of an investigation. However, the right to be forgotten cannot be exercised when EU or Member State law requires the retention of the relevant data.[134] The impact of the right to be forgotten on EU and U.S. law enforcement efforts will therefore be limited.

According to Article 17 of the General Data Protection Regulation, the right to be forgotten entitles consumers to demand that the company erase any and all personal data related to them, and requires that companies comply "without delay."[135] Data subjects can exercise this right if the data is "no longer necessary in relation to the [original] purposes;" if "the data subject withdraws consent . . . or when the storage period consented to has expired;" if the data subject objects to the processing of his or her data as unlawful or improper; or if the processing of the data conflicts with the Data Protection Regulation for any other reason.[136] This broad language would permit an individual to simply withdraw his or her consent and then exercise the right to be forgotten. The Regulation even requires that companies "take all reasonable steps" to arrange that third parties, to whom the data has been made public, also erase the data.[137]

However, there is reason to believe that the impact of this right on EU and U.S. law enforcement efforts would be more limited than one might initially expect. As a preliminary matter, the right to be forgotten, while worded broadly under the General Data Protection Regulation, is narrowly tailored under the Criminal Justice Directive. Under the Criminal Justice Directive, the right to erasure only applies when the relevant data was processed in a way that conflicts with the substantive requirements of the Directive.[138] Even if data was improperly processed, a data controller may "mark" the data, rather than erase it, if the data is required for

---

[132] *See Criminal Justice Directive*, *supra* note 2, art. 11(4). A number of EU Member States have adopted legislation that limits notification requirements for law enforcement or national security related disclosures. *See, e.g.*, Data Protection Act (Act No. 25/1988, amended 2012) 1998, c. 29, § 8 (Ir.) (exempting data processing that is "required for the purpose of safeguarding the security of the State . . . . [or] required for the purpose of preventing, detecting or investigating offences").
[133] *See Id.*
[134] *Data Protection Regulation*, *supra* note 1, art. 17(3)(d).
[135] *Id.* art. 17(3).
[136] *Id.* art 17(1).
[137] *Id.* art. 17(2). This provision has been especially controversial because it would seem to conflict with the right of free speech in certain contexts. *See* Jeffrey Rosen, *The Right To Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 90-92 (2012).
[138] *Criminal Justice Directive*, *supra* note 2, art. 16(1).

purposes of proof.[139] Consequently, once an EU citizen's data is under the control of EU or U.S. law enforcement officials, it would fall under the narrower right to erasure found in the Criminal Justice Directive, and would thus be more difficult to erase than it would while under the control of a private entity.

Moreover, even if the data *is* under the control of private parties rather than law enforcement, the right to be forgotten would still be limited by EU and Member State data retention laws. The Regulation stipulates that individual EU states, or the Union as a whole, may restrict the right to be forgotten (and other rights enumerated in the Regulation) in the name of "public security" or "the prevention, investigation, detection and prosecution of criminal offences."[140] The EU did just that when it adopted Directive 2006/24/EC on the retention of Data (Data Retention Directive). The Directive, which applies to "traffic and location data . . . and to the related data necessary to identify the subscriber or registered user,"[141] was adopted in 2006 following major terrorist attacks in Madrid in 2004 and in London in 2005.[142] EU Member States were required to pass implementing legislation by September 15, 2007 with the option of postponing application of the Directive to Internet communications until March 15, 2009.[143] Since the Directive was adopted, a number of EU Member States have transposed the instrument into their domestic law, including Austria, Bulgaria, Denmark, Estonia, France, Ireland, Italy, Latvia, Liechtenstein, Malta, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Norway, and the United Kingdom.[144] The Directive states that these national laws must require data to be retained from anywhere between six months and two years.[145] For example, Ireland's Data Retention law requires telephonic data be retained for a period of two years,[146] and data related to Internet communications to be retained for one year.[147] According to the European Commission, data retention laws have been critical to several important law enforcement operations. Specifically, the data retention laws were "crucial to the success of Operation Rescue which helped reveal the identities of 670 suspected members of an international paedophile network and protect children from abuse in Member States where the directive has been transposed."[148]

---

[139] *Id.* art. 16(3)(b). According to the Criminal Justice Directive, "marking" data restricts its processing in the future, but it does not require erasure. *See id.* art. 3(4) ("'[R]estriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future.").

[140] *Id*. art. 21.

[141] Directive 2006/24/EC of the European Parliament and of the Council 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, art. 2, 2006 O.J. (L 105) 54, 56 [hereinafter Directive 2006/24/EC].

[142] Press Release, European Commission, Commission Evaluates the Directive on Retention of Telecommunications Data, Apr. 18, 2011, http://europa.eu/rapid/press-release_IP-11-484_en.htm [hereinafter Press Release, Commission Evaluates the Directive].

[143] Directive 2006/24/EC, *supra* note 143, art. 15(1), 15(3).

[144] *Mandatory Data Retention: European Union*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/mandatory-data-retention/eu (last visited Dec. 1, 2012). Other Member States are actively resisting implementation of the law or are facing constitutional challenges in EU or domestic courts. *Id.*

[145] Press Release, Commission Evaluates the Directive, *supra* note 142.

[146] Communications (Retention of Data) Act 2011 (Act No. 3/2011) (Ir.), http://www.irishstatutebook.ie/2011/en/act/pub/0003/print.html.

[147] *Id.*

[148] Press Release, Commission Evaluates the Directive, *supra* note 145.

Because data controllers must comply with Member States' data retention laws before allowing a data subject to exercise his or her right to be forgotten, data that is relevant to law enforcement would be protected for a considerable window of time. For example, if an individual located in Ireland places a phone call to an acquaintance who later carries out a criminal act, Irish law enforcement officials would have two years to request that information from his or her telephone carrier. If that data is transferred to EU or U.S. law enforcement officials before the two-year period has expired, it can be retained indefinitely provided it remains relevant "for purposes of proof."[149] If law enforcement officials miss the two-year deadline, the data subject could exercise his or her right to be forgotten.[150]

In sum, the degree to which law enforcement operations will be affected by the right to be forgotten will depend on the degree to which law enforcement officials can successfully predict what types of information would be relevant to an investigation and identify that information within the data retention period. The EU Data Retention Directive focuses on data related to online and telephonic communications, which are undoubtedly useful to a criminal investigation. But other forms of information may be less obviously relevant at first. Many records that later become relevant to a criminal investigation presumably seem innocuous when first gathered (online purchases, GPS location information, photographs on social networking sites, etc.). And depending on the scope of a criminal investigation, law enforcement officials may not discover the existence of a relevant set of data until the data retention period has expired. If EU and U.S. law enforcement officials can minimize the frequency of situations like this, the impact of the right to be forgotten will likely be limited.

CONCLUSION

According to our analysis of the EU's proposed Data Protection Regulation and Criminal Justice Directive, the impact of the new legislation on EU and U.S. law enforcement efforts should be limited. However, ambiguity exists in the proposed Regulation and Directive. The actual impact of these pieces of legislation will depend on how they are implemented, and we may not have a clear sense of what implementation will look like until after the legislation is adopted. Therefore our observations are, by necessity, preliminary.

Due to the flexible language on data transfers contained in the latest draft, the Criminal Justice Directive should not affect the current framework for information sharing set forth in the EU-U.S. MLAT. However, we have identified two main ways that law enforcement efforts could be substantially affected by the proposed legislation. First, the Data Protection Regulation may require U.S. entities to inform EU citizens when they disclose data related to those citizens to U.S. law enforcement, even if the entity is required to keep that information confidential pursuant to a U.S. court order. Nevertheless, this requirement should not apply to non-EU residents' data. U.S. law officials can, moreover, circumvent the requirement by obtaining the information from EU law enforcement officials, who may not be obligated to inform the EU resident that their data is being processed. Second, the "right to be forgotten" could potentially

[149] *See Criminal Justice Directive*, *supra* note 2, art. 16(3)(b).

[150] Interestingly, nothing in the General Data Protection Regulation or the Criminal Justice Directive instructs courts how to interpret a request for erasure—whether, that is, they may treat an individual's request for erasure as itself evidence. Yet doing so would appear to violate the normative principles that underlie the right to be forgotten.

result in data that would otherwise be relevant to law enforcement operations being erased. Yet the right to be forgotten would not apply to data that is controlled by law enforcement agencies, and EU and Member State laws require that data be retained for a period of time during which the right to be forgotten cannot be exercised. Thus, the right to be forgotten would only affect law enforcement efforts if a law enforcement official became aware of the existence of relevant data only after the data retention period had expired.

The Draft Data Protection Regulation and Criminal Justice Directive are now before the European Parliament and the Council for consideration. It is possible that changes could occur during this stage that would change the legislation's implications for U.S. and EU law enforcement. However, if the Regulation and Directive are adopted in their current form, they should not have a significant effect on the ability of EU and U.S. law enforcement officials to obtain relevant information outside of the two challenges identified in this memo.