UPDATING THE LAW OF INFORMATION PRIVACY: THE NEW FRAMEWORK OF THE EUROPEAN UNION

MARC ROTENBERG* & DAVID JACOBS**

---

* A.B. Harvard University; J.D., Stanford Law School; Executive Director, Electronic Privacy Information Center ("EPIC"), Washington, DC.; Adjunct Professor of Law, Georgetown University Law Center. Mr. Rotenberg teaches the law of information privacy at Georgetown and frequently testifies before Congress about emerging privacy issues.

** B.S., Univ. Wisconsin–Eau Claire; J.D., Harvard Law School; Consumer Protection Counsel, EPIC.

The authors wish to acknowledge the assistance of Emilio De Capitani, Marie George, Paul de Hert, and Yves Poullet. The authors are also grateful for the assistance of EPIC's 2012 summer clerks, Eric Felleman, Allegra Funsten, Kimberly Koopman, John Sadlik, and Pavel Sternberg.

In early 2012, the European Commission published its proposed General Data Protection Regulation,[1] which updates European data protection law and will significantly impact business practices around the globe, much as did the European Union Data Protection Directive of 1995. Although there will be considerable debate about the various provisions contained in the Regulation, an overview of the developments leading up to it shows the natural evolution of the newest legal instrument to safeguard the modern right to privacy. This Article develops that picture.

---

1. *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 (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter GDPR], *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

This Article proceeds in five parts. Part I describes the origins of European privacy law, including the development of the significant modern privacy instruments. Part II explores the key provisions of the proposed General Data Protection Regulation. Part III focuses on the Regulation's application outside the European Union (EU), and the "ratcheting-up" effect that is likely to result. Part IV examines related international privacy developments, including efforts to update the Council of Europe Privacy Convention, enforce the Organization of Cooperation and Development (OECD) Privacy Guidelines, and develop a privacy framework in the United States that is broadly applicable to global privacy challenges. Finally, the Article concludes by noting the significance of the Regulation in the development of modern privacy law.[2]

I. ORIGINS OF EU PRIVACY LAW

After World War II, privacy attained the legal and cultural status of a fundamental right in Europe. The right of privacy was recognized in the Universal Declaration of Human Rights,[3] in other post-war international instruments such as the European Convention on Human Rights (ECHR),[4] and in legislation implementing these instruments at the national level. Although EU member states have interpreted these instruments in light of new practices, such as wiretapping and DNA collection, the advent of automated data processing prompted the adoption of the Data Processing Convention and, later, the Additional Protocol, which created data protection authorities in all of the

2. It is worth noting at the outset that much of the European law that is the subject of this article describes the protection of fundamental rights and freedoms associated with the processing of personal data; against this background, the right of privacy is viewed narrowly. In adopting the phrases "information privacy law" or "modern privacy law" it is the authors' intent to capture this broader meaning of privacy.

3. Universal Declaration of Human Rights art. 12, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).

4. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter European Convention on Human Rights], *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/CONVENTION_ENG_WEB.pdf.

member states.[5] Most recently, the evolution of privacy as a fundamental right is reflected for the EU member states in the adoption of the Lisbon Treaty and the Charter of Fundamental Rights, which added the protection of individuals' fundamental rights and freedom with regard to the processing of personal data ("data protection") as a fundamental right.[6]

A. Integration of the European Union Economies

After World War II, six European countries united to create the European Coal and Steel Community (ECSC), as well as the European Economic Community (EEC) and the European Atomic Energy Community (EAEC).[7] Over the next forty years the integration of the European economies grew in both scope and size until 1986 when, now called the European Community composed of twelve member states, it has become following the Single European Act treaty an "internal market" without internal borders.[8] In 1992, those twelve members signed the Maastricht Treaty, which formed the European Union (EU) covering at the same time the competencies of the European Community and new domains of external policy as well as justice and home affairs.[9] This treaty started the process by which

---

5. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data art. 1, Jan. 28, 1981, E.T.S. No. 108, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm; Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows art. 1, Aug. 8, 2001, E.T.S. No. 181, *available at* http://conventions.coe.int/Treaty/EN/treaties/html/181.htm.

6. Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community art. 16B, Dec. 13, 2007, 2007 O.J. (C 306) 51 [hereinafter Treaty of Lisbon], *available at* http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:EN:HTML; Charter of Fundamental Rights of the European Union arts. 7–8, Dec. 18, 2000, 2000 O.J. (C 364) 10, [hereinafter EU Charter of Fundamental Rights], *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

7. *See generally* Treaty Instituting the European Coal and Steel Community (with Annexes), Apr. 18, 1952, 261 U.N.T.S. 140, *available at* http://treaties.un.org/doc/Publication/UNTS/Volume%20261/v261.pdf.

8. *The changing face of Europe—the fall of the Berlin Wall*, EUROPA, http://europa.eu/about-eu/eu-history/1980-1989/index_en.htm (last visited Feb. 4, 2013).

9. Consolidated Version of the Treaty of European Union, Feb. 7, 1992, 2008 O.J. (C 115) 13 [hereinafter Treaty on European Union], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0013:0046:en:PDF;

the member states moved to consolidate their legal authorities and regulatory frameworks across a wide range of economic activity to facilitate the free movement of goods, services, labor, and capital.[10] As new member states were admitted to the European Union, they were required to comply with the "Copenhagen Criteria," as well as demonstrate that they had adequate privacy protection to safeguard personal data.[11] The countries were required to show the stability of democratic institutions and the protection of human rights, the existence of a functioning market economy, and the acceptance of the Community *acquis*, the ability to comply with the aims of political, economic and monetary union.[12] The adoption of a pan-European framework for privacy protection is thus part of the process of European integration.

B. Establishment of Privacy as a Fundamental Right

European countries have recognized privacy as a fundamental right for many years. Although the EU has only officially existed since 1993,[13] privacy is well established in the constitutions of member countries and the national courts. Most notably, the German Constitutional Court has set out substantial opinions on the right to privacy,[14] as well as the right to "informational privacy."[15]

Europe without frontiers, EUROPA, http://europa.eu/about-eu/eu-history/1990-1999/index_en.htm (last visited Feb. 4, 2013).

10. *See Treaty of Maastricht on European Union*, EUROPA, http://europa.eu/legislation_summaries/institutional_affairs/treaties/treaties_maastricht_en.htm (last visited Feb. 4, 2013).

11. *See Europa,* Accession Criteria (Copenhagen Criteria), http://europa.eu/legislation_summaries/glossary/accession_criteria_copenhague_en.htm ("Any country that wishes to join the Union must meet the accession criteria.").

12. *Id.*

13. *See* Treaty on European Union, *supra* note 9, at 45; MARGOT HORSPOOL & MATTHEW HUMPHREYS, EUROPEAN UNION LAW 16 (4th ed. 2006).

14. *See, e.g.*, Robert G. Schwartz, Jr., *Privacy in German Employment Law*, 15 HASTINGS INT'L & COMP. L. REV. 135, 145 (1992) (noting German Constitutional Court ruling that the German Constitution protects an "untouchable sphere of private life withdrawn from the influence of state power") (quoting Judgment of July 16, 1969, BverfG, 27 BVerfGE 1, 6) (internal quotation marks omitted).

15. *See, e.g.*, J.C. Buitelaar, *Privacy: Back to the Roots,* 13 GER. L.J. 171, 187–93 (2012) (describing German Constitutional Court rulings on the right to informational privacy).

International agreements, declarations, and treaties have deeply influenced EC and EU privacy law. The initial post-war expression of privacy as a fundamental right is found in the United Nations's Universal Declaration of Human Rights (UDHR).[16] Soon after its inception, and very shortly after the experiences of World War II, the UN adopted the UDHR to recognize formally the inalienable rights of every person.[17] The UDHR enumerates many rights, including those established in Article 12, which states that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[18] The UNHR thus not only set out a universal articulation for the right of privacy; it simultaneously called on nations to establish privacy as a legal right.

Soon after the UNHR, European countries followed suit and established a privacy right within the Council of Europe (COE). Created in 1949, the COE is an organization of forty-seven member states, including Belgium, Denmark, France, Germany, Latvia, Spain, and Sweden, all of which are also members of the EU.[19] In 1953, the COE ratified the Convention for the Protection of Human Rights and Fundamental Freedoms, commonly known as the European Convention on Human Rights.[20] Drawing inspiration from the UNHR, the Convention set the broad goal of "maintenance and further realisation of human rights and fundamental freedoms,"[21] and aimed to "take the first steps for the collective enforcement of certain of the rights stated in the Universal Declaration."[22] To meet this goal, the Convention bound all member states to "secure to everyone within their jurisdiction [the] rights and freedoms" contained within the Convention.[23] Furthermore, the Conven-

16. Universal Declaration of Human Rights, *supra* note 3.

17. *Id.* pmbl.

18. *Id.* art. 12.

19. *See* THE COUNCIL OF EUROPE: AN OVERVIEW 2 (2012), *available at* http://www.coe.int/AboutCOE/media/interface/publications/tour_horizon_en.pdf.

20. *The Convention in 1950*, COUNCIL OF EUROPE, http://human-rights-convention.org/the-texts/the-convention-in-1950/ (last visited Feb. 4, 2013).

21. European Convention on Human Rights, *supra* note 4, pmbl.

22. *Id.*

23. *Id.* art. 1.

tion established a European Court of Human Rights and gave individuals, as well as states, standing to file claims in that venue.[24]

Among the rights the Convention enumerated is privacy. Article 8, entitled "Right to respect for private and family life," states, "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[25] Article 8 ensures privacy rights in relation to government actors and, although it contains some exceptions,[26] the European Court of Human Rights has interpreted "private life" broadly.[27] In fact, the court has said that

> [I]t would be too restrictive to limit the notion [of "private life"] to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.[28]

This broad interpretation includes the right to protection against government monitoring of employees' e-mails and telephone conversations to obtain evidence of improper actions at work,[29] wiretapping phone calls without the proper checks and minimization procedures,[30] collecting and accessing stored personal data without consent,[31] and the right to have the govern-

---

24. *See id.* arts. 19, 33, 34.

25. *Id.* art. 8.

26. *See id.* para. 2.

27. *See, e.g.*, Costello-Roberts v. United Kingdom, 19 Eur. Ct. H.R. 112, paras. 35–36 (1993), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57804.

28. Niemietz v. Germany, 16 Eur. Ct. H.R. 97, para. 29 (1992), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57887.

29. *See* Copland v. United Kingdom, 45 Eur. Ct. H.R. 37, paras. 43–44 (2007), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-79996 (holding that Article 8 prohibited a public university from monitoring its employees' e-mail and phone conversations even when the monitoring consisted of legal collection of data).

30. Malone v. United Kingdom, 7 Eur. Ct. H.R. 14 (1984), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57533.

31. Gaskin v. United Kingdom, 12 Eur. Ct. H.R. 36, paras. 34–37 (1989), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57491.

ment prevent tabloid magazines from publishing photographs of a person's private life.[32]

Additionally, the European Court of Human Rights has held that the United Kingdom's practice of collecting DNA samples from each individual who is arrested—even if the charges were subsequently dropped or the accused were acquitted at trial—and storing the samples in a nationwide database violates an individual's right to privacy.[33] The court first ruled that the collection of the DNA samples was an interference with a person's right to privacy.[34] However, because of the government's right to enforce its laws, the court also went on to analyze whether this interference was valid. The court acknowledged the United Kingdom's authority to store samples taken from those people who had been convicted, but held that samples collected from people who were either found innocent, or whose charges had been dropped, must be destroyed.[35]

Despite Article 8's broad scope, technological developments and changing business practices began to challenge the post-War conception of privacy. In 1981, recognizing "the increasing flow across frontiers of personal data,"[36] the Council of Europe enacted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter the COE Privacy Convention).[37] Recognizing the increasing use of computing systems to collect, compile, and transfer detailed information on European citizens, the member states decided that "it [was] necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples . . . ."[38] Pursuant to this goal, and echoing Article 8 of European Convention on Human Rights, the drafters of the COE Privacy Convention used language with a very broad

32. Von Hannover v. Germany, 40 Eur. Ct. H.R. 1, paras. 50–53 (2004), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61853.

33. S. v. United Kingdom, 48 Eur. Ct. H.R. 50, paras. 10–22 (2008), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-90051.

34. *Id.* para. 77.

35. *Id.* para. 125.

36. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data pmbl., Jan. 28, 1981, 20 I.L.M. 317 [hereinafter Convention 108], *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

37. *Id.*

38. *Id.* pmbl.

scope,[39] by defining "personal data" as "any information relating to an identified or identifiable individual"[40] and "automatic processing" as the automation in whole or in part of "storage of data, carrying out of logical and/or arithmetical operations on those data, [or] their alteration, erasure, retrieval or dissemination."[41] Unlike Article 8, however, the COE Privacy Convention applies to both public and private actors.[42]

The COE Privacy Convention's substantive provisions are also drafted broadly. Under the Convention, any personal data that "undergo[es] automatic processing" must be collected and processed "fairly and lawfully,"[43] can only be stored "for specified and legitimate purposes,"[44] must be limited to what is needed for those purposes,[45] be accurate and up to date,[46] and contain identifiable data only as long as required for the purpose which the data is stored.[47] Data that reveals race, religion, sexual orientation, political views, criminal convictions, or health information is further protected by a prohibition on the automatic processing of this type of data unless domestic law provides "appropriate safeguards."[48]

Additionally, the COE Privacy Convention gives individuals the right to know how others are using their personal data. Article 8 of the COE Privacy Convention gives anyone within the Convention's jurisdiction the right to find out if an entity possesses an automated personal data file relating to him or her, what that data is, the data's purpose, and where the entity possessing the file is located.[49] It also gives the person a right to have this information erased or corrected if the information has been obtained or processed in a way contrary to the Conven-

---

39. *See id.* art. 1 (establishing the COE Privacy Convention as securing in "the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy").

40. *Id.* art. 2(a).

41. *Id.* art. 2(c).

42. *Id.* art. 3(1).

43. *Id.* art. 5(a).

44. *Id.* art. 5(b).

45. *See id.* art. 5(c).

46. *Id.* art. 5(d).

47. *Id.* art. 5(e).

48. *Id.* art. 6.

49. *Id.* art. 8(a)–(b).

tion.[50] Finally, although there are exceptions to these rights—namely, for purposes of national and domestic security, protection of others' rights, or scientific and statistical research—these exceptions are narrow and require legal authorization before they apply.[51]

As an added measure of protection, the COE Privacy Convention restricts the transfer of personal data that has, or will be, automatically processed.[52] Although the Convention does not allow member states to limit transfer of data solely based on privacy concerns,[53] it does give them the right to create limitations on, first, the transfer of certain kinds of data and, second, the transfer of data to other member states where that member state's sole purpose is to function as an intermediary for the ultimate transfer of the data to a non-member state.[54] The Convention also sets up a system under which the member states will aid each other in monitoring data processing and enforcing the agreement,[55] as well a committee tasked with assessing how the Convention is working and proposing changes to solve any identified problems.[56] Also, because the COE lacks the authority to make binding law, the Convention contains a provision that makes it a duty for signing parties to pass domestic legislation that actualizes the Convention's principles.[57]

In 2001, the COE supplemented the Convention with the "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows" (hereinafter the Additional Protocol).[58] The Additional Protocol directed parties to create independent data protection authori-

50. *Id.* art. 8(c)–(d).

51. *See id.* art. 9. Data processing under the scientific and statistical research exception does not require statutory authority but does require that there be "obviously no risk of an infringement of the privacy of the data subjects." *Id.* art. 9(3).

52. *Id.* art. 12.

53. *Id.* art. 12(2).

54. *Id.* art. 12(3).

55. *See id.* ch. IV.

56. *See id.* ch. V.

57. *Id.* art. 4(1).

58. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Nov. 8, 2001, C.E.T.S. No. 181, *available at* http://conventions.coe.int/treaty/en/treaties/html/181.htm.

ties[59] and added limitations on data exportation to non-member states and entities within those states.[60] These changes mirrored changes taking place elsewhere in the European Union focused on strengthening the authority of privacy agencies and addressing growing challenges from transborder data flows.

C. Modern EU Privacy Instruments

The creation of the European Union set the stage for a flurry of privacy-related activity. The following years saw the enactment of the EU E-Privacy Directive,[61] the EU Cookie Directive,[62] the Treaty of Lisbon,[63] and, most importantly, the EU Data Protection Directive.[64] The EU Data Protection Directive established a series of protections regarding the collection and processing of personal data in Europe.[65] The Directive, however, was passed in 1995, a time before cloud computing, social networks, and nearly ubiquitous data collection. Enforcement of the Directive also depended on each member state,[66] resulting in inconsistent application that hampered business growth and left many individuals underprotected.

---

59. *Id.* art. 1.

60. *Id.* art. 2.

61. 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), 2002 O.J. (L 201) 37 [hereinafter E-Privacy Directive], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF.

62. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, 2009 O.J. (L 337) 11 [hereinafter Cookie Directive], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.

63. Treaty of Lisbon, *supra* note 6.

64. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 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 EU Data Protection Directive], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF.

65. *See id.* ch. II.

66. *Id.* art. 1.

This is the context from which the proposed General Data Protection Regulation emerged last year. As discussed in Part II, the Regulation strengthens data protection rights for individuals, and harmonizes the existing network of European data protection laws which simplifies compliance procedure for multinational firms. Thus, it represents a natural evolution of European privacy law.

1. The EU Data Protection Directive

During the first few decades of its existence, the European Commission, which has the constitutional duty to submit legislative proposals, resisted calls for a regulatory framework for the processing of personal data.[67] As the Commission's focus expanded from solely economic concerns to encompass fundamental rights of European citizens, however, it recognized the need for rules on personal data processing to secure individual liberties.[68] To do so the Commission had to take in account that in 1985, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Convention took effect.[69] However, this Convention required member states to enact domestic laws to protect personal privacy, but it permitted broad variances among states and ratification was slow.[70] Recognizing a need to streamline the uneven and conflicting data protection laws among the European states, in 1990 the Commission published a draft form of the Data Protection Directive.[71]

After the signing of the Maastricht Treaty in 1992, which established the European Union,[72] the Commission's focus expanded from purely economic concerns to include a compre-

---

67. Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 446 (1995).

68. *See id.* at 447–48.

69. *See* Convention 108, *supra* note 36; Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 431–32 (1995).

70. Cate, *supra* note 69, at 432.

71. The amended version was submitted in 1992. *See Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, COM (1992) 422 final (Oct. 15, 1992).

72. *See* Treaty on European Union, *supra* note 9.

hensive array of political issues, including the protection of fundamental rights of European citizens.[73] In 1995, two years after its formation, the EU took action to protect its citizens' privacy rights; in that year the EU passed the "Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (EU Data Protection Directive).[74] The Directive creates a legal framework that governs movement of personal data across national borders within the EU and sets a baseline for the required security to be provided for the storage, transmission, and processing of personal information.[75] In setting up this framework, the EU Data Protection Directive refers to Article 8 of the European Convention on Human Rights, and its classification of privacy rights, as "fundamental"[76] and states that the Directive's purpose is to promote data sharing while protecting the principles espoused in that Convention.[77] The Directive thus achieved the twin goals of promoting the internal market with clear standards for data transfers and simultaneously safeguarding a fundamental right.

The EU Data Protection Directive requires member states to impose restrictions on the "processing of personal data" to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy."[78] The Directive defines key terms broadly: "personal data" includes "any information relating to an identified or identifiable natural person,"[79] and "processing" refers to "any operation or set of operations which is performed upon personal data."[80]

As a directive, the EU Data Protection Directive binds member states to a single objective, but national authorities control

---

73. *See* Cate, *supra* note 69, at 432 ("The shift from economic to broad-based political union brought with it new and more urgent attention to the protection of informational privacy."); Simitis, *supra* note 67, at 447 (describing the "transition from a merely economic union to a decidedly political one").

74. EU Data Protection Directive, *supra* note 64, pmbl.

75. *See id.* pmbl.

76. *See id.* para. 10.

77. *See id.* paras. 1–14.

78. *Id.* art. 1(1).

79. *Id.* art. 2(a).

80. *Id.* art. 2(b).

the implementation, a process known as "transposition."[81] As a result, member states may implement a directive non-uniformly, so long as each state's implementation meets minimum requirements. Unlike a regulation, an EU directive can only directly impose obligations on member states, not individuals.[82] An EU citizen thus may not sue a private entity for violation of the Directive in the absence of national legislation.

Member states must require that data processors collect personal data only for a specific legitimate purpose, that they ensure it is accurate, and that they keep it in a form that permits identification for no longer than is necessary.[83] Consent is, in general, required before processing.[84] Member states also must ensure that processors inform data subjects, as well as the recipients or categories of recipients of the data, of the purposes of the data processing.[85] Member states also must ensure that processors conduct data processing confidentially and securely.[86] The Directive also specially protects personal data related to sensitive categories, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, or sexual activity.[87]

The EU Data Protection Directive grants data subjects a "right of access" to personal data being processed, the purpose of the processing, the categories of data concerned, the recipients or categories of recipients to whom the data is disclosed, an intelligible form of the data undergoing processing, and

---

81. *See* Consolidated Version of the Treaty on the Functioning of the European Union art. 288, Mar. 3, 2010, 2010 O.J. (C 83) 47, 172 [hereinafter TFEU], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:EN:PDF ("leav[ing] to the national authorities the choice of form and methods" for the implementation of EU directives); *Transposition and Application of EU Law,* EUR. COMM'N, http://ec.europa.eu/governance/better_regulation/transp_eu_law_en.htm (last visited Feb. 5, 2013).

82. *See, e.g.*, Marshall v. Southampton and S. Hampshire Area Health Auth., 1986 E.C.R. 737, 749 ("[A] directive may not of itself impose obligations on an individual and . . . a provision of a directive may not be relied upon as such against such a person.").

83. EU Data Protection Directive, *supra* note 64, art. 6(1).

84. *Id.* art. 7(a). The Directive provides exceptions for the satisfaction of legal obligations, the protection of the public interest, journalistic needs, and freedom of expression. *See id.* arts. 7, 9.

85. *Id.* arts. 10–11(1).

86. *Id.* art. 16–17.

87. *Id.* art. 8(1).

knowledge of the logic involved in any automatic processing.[88] Subjects may also request that processors rectify, erase, or block data that is incomplete, inaccurate, or otherwise not in compliance with the directive, as well as notify any third parties who have received the data of this rectification, erasure, or blocking, if feasible.[89] The Directive did not cover national security and criminal prosecutions, because these domains were initially excluded from Community competencies.[90]

Data subjects are given the right to object that data processing does not serve the public interest or other legitimate interests.[91] If the objection is justified, the data processor must remove the data from processing.[92] Subjects may object to the processing of their personal data for direct marketing,[93] and have a right not to be subject to decisions with legal effects based solely on automated processing.[94]

The EU Data Protection Directive also establishes the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, or the "Article 29 Working Party," which has an independent advisory status.[95] The Working Party is composed of representatives of each member state's data protection authorities, as well as other representatives from each member state and the European Commission.[96] The Directive charges the Working Party with examining questions of application of the Directive, providing the Commission with an opinion on the level of protection both inside and outside of the EU, advising the Commission on any proposed amendments, and giving its opinion on EU codes of conduct.[97]

88. *Id.* art. 12(a).
89. *Id.* art. 12(b)–(c).
90. *Id.* art. 13(1).
91. *Id.*
92. *Id.* art. 14(a).
93. *Id.* art. 14(b).
94. *Id.* art. 15(1).
95. *Id.* art. 29(1).
96. *Id.* art. 29(2).
97. *Id.* art. 30(1).

2. The E-Privacy Directive

The 2002 Directive on Privacy and Electronic Communications,[98] also known as the E-Privacy Directive, further developed the effort to ensure that processing of personal data in the electronic communications sector does not deprive persons of their fundamental right to privacy.[99] The E-Privacy Directive applies to data processing conducted in connection with the provision of "publicly available electronic communications services in public communications networks."[100]

Under the E-Privacy Directive, electronic communications service providers are required to implement appropriate security measures and provide notification to subscribers in the event of a risk of a breach.[101] Member states are obligated to enact legislation to ensure the confidentiality of communications,[102] although exceptions for reasons of national security and criminal investigation are permitted.[103]

National legislation also must restrict the ability of software residing on a user's terminal without his knowledge to gain information about the user.[104] These provisions are meant to target malicious spyware, while permitting legitimate devices like "cookies" so long as consumers are provided with clear information about their purpose and are allowed to refuse such processing.[105]

Communications providers are required to erase or anonymize data relating to subscribers and users stored on their networks when they no longer need it for the purpose of transmission.[106] Some exceptions apply, including storage of data for the marketing of electronic communication services with the consent of the subscriber or user.[107] Service providers

98. E-Privacy Directive, *supra* note 61.
99. *Id.* art. 1, para. 1.
100. *Id.* art. 3(1).
101. *Id.* art. 4.
102. *Id.* art. 5(1).
103. *Id.* art. 15(1).
104. *See id.* art. 5(3).
105. *See id.* pmbl., paras. 24–25.
106. *Id.* art. 6(1).
107. *Id.* art. 6(3).

may only process location data when made anonymous or with opt-in consent of the user or subscriber.[108]

Service providers are ordinarily required to obtain the user's consent before using e-mails for direct marketing, unless they are marketing their own products to customers who have previously purchased a similar product from them.[109]

In 2009, the E-Privacy Directive was amended by the so-called "Cookie Directive."[110] The amendment requires service providers to meet higher security requirements for the storage and handling of personal data.[111] In the event of personal data breaches, providers must inform the national data protection authorities and, where the breach is likely to adversely affect personal data or privacy, must inform the affected individual as well.[112] The notification must include the nature of the breach, contacts from which more information can be obtained, and recommended measures to mitigate possible adverse effects.[113] The amendment also revises Article 5(3) of the E-Privacy Directive, the section related to cookies, by requiring that users give consent before third parties store or access information in the user's computer.[114]

3. The Treaty of Lisbon

The EU reaffirmed the concept of privacy as a fundamental right in the Treaty of Lisbon.[115] Following the passage of the Treaty of Lisbon, which amended the Treaty on European Union, Article 16 of the resulting Consolidated Version of the Treaty on the Functioning of the European Union states:

> (1) Everyone has the right to the protection of personal data concerning them. (2) The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data

108. *Id.* art. 9(1).
109. *Id.* art. 13.
110. Cookie Directive, *supra* note 62.
111. *See id.* art. 2(4)(b).
112. *Id.* art. 2(4)(c).
113. *Id.*
114. *Id.* art. 2(5).
115. Treaty of Lisbon, *supra* note 6, art. 2(29).

> by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.[116]

Since 2000, the European Union has also been committed to protecting personal data pursuant to Article 8 of the Charter of Fundamental Rights of the European Union.[117] Under Article 8, every citizen has the right of personal data protection.[118] Personal data should be processed fairly for specified purposes, and with the individual's consent, or consistent with some other legitimate basis laid down by law.[119] Compliance with the Article is supervised by an independent body.[120] Article 7 of the Charter protects separately private and family life, stating in terms similar to Article 12 of the Universal Declaration of Human Rights, that "[e]veryone has the right to respect for his or her private and family life, home and communications."[121]

4. The Role of Data Protection Authorities

The EU Data Protection Directive requires each member state to establish a public authority responsible for "monitoring the application within its territory of the provisions adopted."[122] These authorities must possess investigative powers, effective powers of intervention, and the power to engage in legal proceedings where provisions of the Directive have been violated.[123] They must respond to claims filed by any person and create regular reports of their activities.[124]

---

116. TFEU, *supra* note 81, art. 16. The Treaty of Lisbon makes the Charter of Fundamental Rights a legally enforceable document on the EU, its institutions, and its member states as regards its implementation in European law. Treaty on European Union, *supra* note 9, art. 6(1).

117. EU Charter of Fundamental Rights, *supra* note 6, art. 8.

118. *Id.* art. 8(1).

119. *Id.* art. 8(2).

120. *Id.* art. 8(3).

121. *Id.* art. 7; *see also* Universal Declaration of Human Rights, *supra* note 3, art. 12.

122. EU Data Protection Directive, *supra* note 64, art. 28(1).

123. *Id.* art. 28(3).

124. *Id.* art. 28(4)–(5).

The EU Data Protection Directive also requires data controllers to notify the state's data protection authorities before executing any automatic processing.[125] This notification must include the purpose of the processing, the categories of data, and the recipients of the data.[126] The authorities must keep a register of processing operations that is publicly accessible.[127]

Data protection authorities have an affirmative obligation to determine which processing operations are likely to present specific risks to the rights and freedoms of data subjects and examine them before they are commenced.[128] The Cookie Directive also granted authorities the ability to audit communications service providers' security measures and issue recommendations on best practices.[129] They may also adopt guidelines, issue instructions, and conduct audits to ensure that personal data breach notifications are appropriately issued.[130]

D. New Challenges

The 1995 EU Data Protection Directive set out the first comprehensive framework for privacy rights in Europe. The Directive is now seventeen years old, however, and the percentage of Europeans using the Internet and other online services has increased from less than one percent in 1995 to more than sixty percent today.[131] There have also been marked changes in the way that European citizens make use of the internet, with the development and implementation of a myriad of novel web services and features. Such drastic changes in technology and usage have presented significant new challenges that the original Directive is not well equipped to handle.[132] Compounding these new issues is the fact that each of the twenty-seven European member states have implemented the Directive differ-

---

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

126. *Id.* art. 19(1).

127. *Id.* art. 21(2).

128. *Id.* art. 20.

129. Cookie Directive, *supra* note 62, art. 2(4)(b).

130. *Id.* art. 2(4)(c), para. 4.

131. *Internet Usage in Europe*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats4.htm (last visited Feb. 5, 2013).

132. *A comprehensive approach on personal data protection in the European Union*, at 2–3, COM (2010) 609 final (Nov. 4, 2010) [hereinafter Comm'n COM], *available at* http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

ently.[133] These differences have made enforcement difficult, especially given the multinational and trans-European scope of many new web services.

1. New Technologies and Business Practices

Perhaps the most important and unanticipated development in the way citizens use the Internet is the advent of social networking. The original EU Data Protection Directive was drafted when only a small minority of Europe's population used the Internet, and the personal information collected was limited to data such as the user's name, address, or financial information. Social network users now store pictures, videos, information about their daily lives, and even their location, online.[134]

The EU Data Protection Directive has as one of its seven core principles the right to access[135]—that is, users have a right to access their data and correct inaccuracies. At the time this language was drafted the focus was on correcting or erasing "incomplete or inaccurate" data that might be stored in a database, such as erroneous credit information.[136] Whereas access in the original Directive related to access to ensure accuracy, access now pertains to accessing pictures or video for personal use. Now the user's desire has shifted from correcting mistakes to management of over-sharing and access on a regular basis.[137] The old framework lags behind.

Although the skeletal basis for these rights exists in the current Directive, with some necessary updates coming from the 2002 E-Privacy Directive, the method for exercising these rights is individualized in each of the twenty-seven European Union member states.[138] For example, a social networking provider may limit access to a user's information in the event that a user wants to switch to a competing service.[139] Although against the

---

133. *Id.* at 10.

134. *See, e.g.*, Michael B. Farrell, *The battle for your data on the Web*, BOS. GLOBE, July 23, 2012, http://www.bostonglobe.com/business/2012/07/22/the-battle-for-your-data-web/qUB8nrC7N2CAmcEvfz5QpI/story.html.

135. EU Data Protection Directive, *supra* note 64, pmbl.

136. Cate, *supra* note 69, at 434.

137. *See* Comm'n COM, *supra* note 132, at 2.

138. *Id.* at 10.

139. Francoise Gilbert, *Proposed EU Data Protection Regulation: The Good, The Bad, and The Unknown*, 15 J. INTERNET L., April 2012, at 20, 29.

spirit of the original Directive, exercising the right to access and delete data in this instance might be easier in some member states than others.[140] Additionally, if a user wishes to stop using a social networking service, ensuring the complete deletion of personal data will pose a vexing problem. The sheer volume of data collected and its dissemination among not only a multitude of servers and databases kept by the social network, but also among additional web services, makes complete deletion a significant challenge.[141]

In addition to services such as Facebook and Twitter that store personal information online, the emergence of "cloud computing" is rapidly altering the way in which individuals use the web. The fundamental idea behind cloud computing is the storage of data, files, and programs on remote servers operated by others, rather than on a user's computer.[142] By utilizing the "cloud," users can take advantage of reduced storage costs, but they also confront new risks to privacy.[143] Users store information—conceivably any type of data stored on their computer—online.[144]

Perhaps the most fundamental challenge presented by cloud computing is data protection. In the last few years, companies ranging from LinkedIn to Sony lost control of data stored on their servers.[145] In 2011, over 174 million records were stolen through data breaches worldwide.[146] Europe is not immune to these incidents. According to a British study, seventy percent of organizations within the United Kingdom experienced a data breach incident in 2009.[147] In response to these threats, law en-

---

140. *See* Comm'n COM, *supra* note 132, at 10.

141. *See* Gilbert, *supra* note 139, at 29.

142. Paul Lanois, *Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?*, 9 NW. J. TECH. & INTELL. PROP. 29, 29 (2010).

143. *Id.* at 32.

144. *Id.* at 32–33.

145. *See* Liana B. Baker & Jim Finkle, *Sony PlayStation suffers massive data breach*, REUTERS, Apr. 26, 2011, http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426; Nicole Perlroth, *Lax Security at LinkedIn is Laid Bare*, N.Y. TIMES, June 11, 2012, at B1.

146. VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT 1 (2012) [hereinafter VERIZON REPORT], *available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

147. John Leyden, *UK data breach incidents on the rise*, THE REGISTER (July 9, 2009, 1:15 PM), http://www.theregister.co.uk/2009/07/09/data_breach_survey/.

forcement agencies from around the world have begun to work together to develop better methods of catching hackers and preventing future breaches from occurring.[148] Despite these efforts, data breaches are a continuing concern, and the number of incidents is only rising.[149]

Although security and accountability are two of the seven fundamental principles of the original EU Data Protection Directive, specific protection measures are determined by member states.[150] The delocalization of user data and the outsourcing of storage and processing to other countries, some of which are outside the jurisdiction of the EU, present a murky legal picture as well. Although personal data may be transferred to third parties under the existing directive, it may only be transferred if the transferee country provides adequate protections.[151] The Directive does not clearly specify the exact requirements for ensuring "adequate protection."[152]

The increase in the amount of data being stored in the cloud means an increase in the risks that web service users face in the event of a data breach. Whereas previously a data breach might disclose a user's address, or at worst credit card information, now a data breach might compromise *all* of a user's personal media and documents. Often, the direct consequence of data breaches is identity theft. When banks or credit card companies experience data breaches, thousands, if not millions, of their customers may have personal and financial information stolen. Like the United States, European countries face identity theft issues as well. In 2007, the EU's Fraud Prevention Expert Group estimated that the United Kingdom lost £1.7 billion per year be-

148. *See* VERIZON REPORT, *supra* note 146, at 2 (noting cooperation with the U.S. Secret Service, Dutch National High Tech Crime Unit, Australian Federal Police, Irish Reporting & Information Security Service, and the London Metropolitan Police).

149. *See* EUR. NETWORK & INFO. SEC. AGENCY, DATA BREACH NOTIFICATIONS IN THE EU 4 (2011), [hereinafter ENISA REPORT] *available at* http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn (noting "[r]ecent high profile incidents of personal data loss across Europe"); VERIZON REPORT, *supra* note 146, at 1 (noting that 2011 had the second-highest data loss total since 2004).

150. *See* ENISA Report, *supra* note 149, at 11.

151. EU Data Protection Directive, *supra* note 64, pmbl. para. 57.

152. Comm'n COM, *supra* note 132, at 15.

cause of identity theft.[153] This figure will only rise as a result of the increasing number of European identity theft incidents.[154]

Giving users timely notification of a potential data breach can allow users to take significant steps to reduce potential personal harm.[155] The 2002 E-Privacy Directive addressed this issue by requiring mandatory personal data breach notification, although the mandate applies only to the telecommunications industry.[156]

With the advent of social networking and the increasing amount of time that users spend on the Internet, the phenomenon of behavioral advertising has emerged as a threat to online privacy. Behavioral advertising is, in essence, a technique used by web services and advertisers to track a user's online behavior and attributes to increase the effectiveness of advertising campaigns.[157] In a recent study of European consumers released by Eurobarometer,[158] sixty-four percent were worried about how companies handled their personal data online.[159] The source of this concern may be the lack of regulations regarding data collection. There is a behavioral advertising voluntary code of conduct but, as the name suggests, the code is voluntary and, according to the European Consumers' Organisation, it is weak and incomplete.[160] There is concern that the self-regulatory system fails to provide adequate consumer protection because there is inadequate notification for consumers about what information is being collected and because the opt-

153. FRAUD PREVENTION EXPERT GRP., REPORT ON IDENTITY THEFT/FRAUD 8 (2007), *available at* http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf.

154. *Id.* at 2.

155. *See* Cookie Directive, *supra* note 62, pmbl. para. 59.

156. E-Privacy Directive, *supra* note 61, art. 4(3).

157. *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 30, 2010, at W1.

158. Eurobarometer is an organization created by the European Commission to conduct public opinion surveys regarding various issues pertaining to the European Union. *See Public Opinion*, EUR. COMM'N, http://ec.europa.eu/public_opinion/index_en.htm (last visited Feb. 5, 2013).

159. Jennifer Baker, *Consumers Misled by Online Behavioral Advertising Companies, EU Group Says*, PCWORLD, (Dec. 6, 2011, 8:20 AM), http://www.pcworld.com/article/245563/consumers_misled_by_online_behavioral_advertising_companies_eu_group_says.html.

160. Letter from Monique Goyens, Dir. Gen., Eur. Consumers' Org., to Jacob Kohnstamm, Chairman, Article 29 Working Party (Dec. 5, 2011), *available at* http://www.beuc.org/custom/2011-09975-01-E.pdf.

out tools typically provided are misleading.[161] Because of these concerns, groups from both Europe and the United States have started pressing for changes to how personal data is collected in Europe and the United States.[162] The issue arises when this type of data collection and targeting occurs without the consent or knowledge of the user.

As with other challenges presented by new technology, the fundamental rights were set in place by the EU Data Protection Directive, but further clarification is needed. The Directive lists "consent" as one of its seven principles, and requires an individual's consent for the processing of personal data.[163] Although an "informed indication" of a user's wishes is a requirement of the Directive, member states interpret consent differently.[164] The E-Privacy Directive helped inform this issue to some extent by specifically requiring consent to place cookies, which are used to track behavior, on a user's computer.[165] There remains a large divide in member states' policies, however: Some states may require affirmative written consent to track, while in other states the default settings on an Internet browser may be enough to give user consent.[166]

2. Enforcement

The requirements of the EU Data Protection Directive would have little meaning without the ability to enforce them. It is here, however, that the current EU framework for privacy protection as a directive, rather than a regulation, is perhaps most limiting. To ensure enforcement, the Directive requires that each member state's laws provide for civil liability and penalties for violation of those laws adopted pursuant to the Direc-

161. *Id.*

162. Letter from Julian Knott, Head of Secretariat, Trans Atlantic Consumer Dialogue, to Jacob Kohnstamm, Chairman, Article 29 Working Party, and David C. Vladeck, Dir., Bureau of Consumer Prot., FTC (Sept. 8, 2011), *available at* http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=328&Itemid=40.

163. EU Data Protection Directive, *supra* note 64, pmbl para. 30; *id.* art. 7; Comm'n COM, *supra* note 132, at 8–9.

164. Comm'n COM, *supra* note 132, at 8–9.

165. Matthew S. Kirsch, *Do-Not Track: Revising The EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, 18 RICH. J.L. & TECH. 2, para. 9 (2011).

166. *Id*. para. 23.

tive.[167] The Directive also requires the creation in each state of a supervisory authority to enforce those laws and hear complaints.[168] Traditionally, under the Directive, an individual state's supervisory or data protection authority cooperate with those of other states when dealing with enforcement of the rights set out in the directive.[169]

Given the multinational nature of many cloud and web service companies, and their international user bases, confusion has arisen regarding the enforcement of principles in the Directive. The extent to which coordination and cooperation are required is not clear, although the Article 29 Working Party has contributed to the effort to enhance clarity and cooperation among member states' data protection authorities.[170] Nevertheless, divergent enforcement regimes within the various member states may produce different outcomes for substantially identical privacy violation claims.[171]

Civil liability and penalties are not the only methods available to ensure enforcement; self-regulatory initiatives and codes of conduct are also available.[172] In fact, the Directive laid down the scope for drawing up codes of conduct; this has, however, rarely been used and private entities consider it inadequate,[173] due largely to the lack of any economic and legal incentive for private companies to create effective self-regulatory schemes.[174]

3. Coordination and Harmonization

The current state of data protection law varies greatly among the twenty-seven European Union member states.[175] The manner in which the EU Data Protection Directive directed member states to pass data protection laws means that each state's data protec-

---

167. Cate, *supra* note 69, at 436–37.
168. *Id.* at 436.
169. EU Data Protection Directive, *supra* note 64, art. 28(6).
170. *See* Comm'n COM, *supra*, note 132, at 17–18.
171. *See id*. at 15.
172. *Id.* at 12.
173. *Id*.
174. *See* Kirsch, *supra* note 165, at para. 47.
175. *See* Comm'n COM, *supra* note 132, at 10.

tion authority (DPA) enforces that particular state's laws.[176] When two member states' DPAs seek to cooperate to enforce the obligations set out in the Directive, problems may arise because of the differences between the member states' laws.

There are currently two bodies in place attempting to facilitate coordination and harmonization among the member states: the Article 29 Working Party and the European Data Protection Supervisor (EDPS).[177] The EDPS helps to supervise certain activities, including those of multinational information technology systems.[178] The Article 29 Working Party, made up of representatives from each member state's DPA, is an expert body that advises DPAs and promotes equal application of the EU Data Protection Directive in all member states.[179] In actuality, however, the Article 29 Working Party has difficulty promoting the equal application of the Directive when each individual member state is responsible for enforcing and enacting the laws.[180] As such, no organization, apart from the Commission as "guardian of the treaty," presently possesses any substantive power to foster cooperation between member states.

II. THE EU GENERAL DATA PROTECTION REGULATION

The European Commission's proposed General Data Protection Regulation (GDPR)[181] responds to two problems. First, the principles outlined in the EU Data Protection Directive of 1995 did not adequately address rapidly advancing technological developments, especially the growth of Internet-based business services, and increasing globalization.[182] Second, previous EU and national regulations created a patchwork of rules that did not did not protect individual privacy sufficiently or give economic stakeholders the uniformity and legal certainty necessary for business growth.[183] EU-level regulation was necessary

176. *See* Part I.C.1, *supra*.

177. Comm'n COM, *supra* note 132, at 17.

178. *Id*. at 17 & n. 48.

179. EU Data Protection Directive, *supra* note 60, arts. 29–30.

180. *See* Comm'n COM, *supra* note 132, at 17–18.

181. GDPR, *supra* note 1.

182. *Id*. pmbl para. 5.

183. Press Release, Eur. Comm'n, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of their Data and to Cut

to create a more cohesive, balanced framework of laws that apply the same data protection to all fields of EU activity.[184] Many of the provisions of the GDPR are adopted from the Data Protection Directive, with an eye to strengthening consumer rights and promoting efficiency.

A. Overview of the GDPR

The proposed GDPR expands the universe of regulated data by revising and clarifying the Data Protection Directive's definition of "personal information." As with the previous Directive, the GDPR covers any processed information concerning an identified or identifiable natural person that forms or is intended to form part of a filing system.[185] The GDPR, however, extends coverage of sensitive information to new categories of personal information, including genetic data.[186] Similarly, the GDPR explicitly notes that online identifiers, such as e-mails, Internet Protocol addresses, or cookie identifiers, are "identifiers" for purposes of the GDPR.[187] Like the EU Data Protection Directive, the GDPR applies to all controllers based in the EU or which offer services and products to individuals based in the EU.[188] Unlike

---

Costs for Businesses (Jan. 25, 2012) [hereinafter Explanatory Memorandum], *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=en&guiLanguage=en.

184. GDPR, *supra* note 1, pmbl. paras. 6–8, 11; Jan Philipp Albrecht & Dimitrios Droutsas, *On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* 4 (Eur. Parl. Cmty. On C.L. Just. & Home Aff., Working Document No. PE491.322v01-00, 2012).

185. *Compare* EU Data Protection Directive, *supra* note 64, art. 2 (stating that personal data is "any information relating to an identified or identifiable natural person," where "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity"), *with* GDPR, *supra* note 1, art. 4(3) (processed information includes data subject to "collection, recording, use, disclosure by transmission, [and] dissemination.").

186. *Compare* EU Data Protection Directive, *supra* note 64, art. 8 *with* GDPR, *supra* note 1, art. 9.

187. *Id.* pmbl., para. 24.

188. *Id.* art. 3.

the Directive, it shifts the burden of responsibility and accountability from consumers to controllers of data.[189]

Data controllers and processors may legally process personal information in relation to contracts with the data subject, vital interests of the data subject, legal obligations of the data controller, and the public interest or exercise of official authority.[190] Data may also be processed with the consent of the data subject or when the processing is necessary to the purposes of the legitimate interests of the controller.[191]

B. Strengthening Individual Control: Substantive Rights and Transparency

The GDPR is intended to strengthen consumer data protection rights by facilitating individual control over personal information. Unlike under the Data Protection Directive, to meet the consent category under the GDPR, the data controller must obtain written, explicit consent for the specified purpose.[192] Implied consent is no longer a legal basis.[193] Consent is not valid where there is an imbalance between the data subject and the controller,[194] and the data subject has the right to withdraw consent at any time.[195]

The GDPR also grants substantive rights to data subjects. In addition to the rights of access, correction, and erasure, it establishes the "right to be forgotten" by implementing stronger rights to erase: The data subject will be able to require a data collector to erase the data subject's information if there is no legitimate reason for retaining it.[196] If the data subject exercises the right of erasure, the GDPR puts the burden on the data collector to contact all third-party processors of data with whom the data collector has shared information about the data subject

---

189. *Id.* at 8 ("Additional new elements are in particular . . . the establishment of comprehensive responsibility and liability of the controller.").

190. *Id.* art. 6.

191. *Id.*

192. *Id.* pmbl. para. 25 ("Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes . . . . Silence or inactivity should therefore not constitute consent.").

193. *See id.*

194. *Id.* art. 7(4).

195. *Id.* art. 7(3).

196. *Id.* arts. 16–17.

if the data subject exercises the right of erasure; the data collector must use reasonable technical measures to inform these third parties that they must erase any copies of or links to that personal data.[197] Under the right of portability, individuals can transfer their data from one automated, electronic system to another.[198] As with the Data Protection Directive, the GDPR protects individuals from behavioral profiling,[199] and data subjects retain the rights of access,[200] correction,[201] objection,[202] and erasure,[203] as well as the right to obtain from the controller a copy of the data.[204]

Third, the GDPR facilitates consumer rights by expressly incorporating a "transparency principle."[205] It requires data collectors to implement transparent and easily accessible data processing policies,[206] which must be written in clear, plain language.[207] The GDPR adopts the EU Data Protection Directive's language requiring data collectors to inform data subjects about the logic and purposes of the processing, the period of data retention, and the existence of rights.[208] The GDPR also establishes a system of certification, data protection seals, and marks intended to allow data subjects to quickly understand the data protection associated with a product or service.[209] The transparency principle helps ensure that data subjects understand the uses of their data as is necessary to give informed consent, prevents data collectors from discriminating against users on the basis of their personal data, and promotes accountability in the maintenance and use of personal data.[210] The

197. *Id.* art. 17.
198. *Id.* art. 18.
199. *Id.* art. 20.
200. *Id.* art. 15.
201. *Id.* art. 16.
202. *Id.* art. 19.
203. *Id.* art. 17.
204. *Id.* art. 18(1).
205. *Id.* art. 11.
206. *Id.* art. 11(1).
207. *Id.* art. 11(2).
208. *See id.* arts. 14–15.
209. *Id.* pmbl. para. 77.
210. *See id.* at 8 n.32 (noting that the transparency principle is inspired by the INT'L CONFERENCE OF DATA PROT & PRIVACY COMM'RS, INTERNATIONAL STANDARDS ON THE PROTECTION OF PERSONAL DATA AND PRIVACY: THE MADRID

rights of individuals, however, are subject to the same restrictions, such as law enforcement and the public interest, found in the EU Data Protection Directive.

C. Increased Responsibility and Accountability of Data Processors and Controllers

The GDPR establishes a "privacy by default" system, in which controllers of personal data are responsible and liable for any processing of that data on their behalf.[211] The burden will be on the controller to keep the data secure and to demonstrate compliance with the GDPR.[212] The GDPR includes many of the data minimization provisions of the EU Data Protection Directive, such as allowing the storage of data for only as long as necessary,[213] but also explicitly requires controllers to take affirmative actions to protect data.[214] In the case of a security breach, collectors must contact those data subjects whose personal data or privacy could be adversely affected by the breach and must notify the supervisory authorities.[215] The data collector must submit notice to supervisory authorities "without undue delay and, where feasible, not later than 24 hours after becoming aware of it."[216] When controllers are responsible for notifying data subjects, they must include recommendations on how the data subjects can protect themselves from harm.[217] Despite these substantive rules, the GDPR as a whole contemplates a "privacy by design" framework, in that the regulation establishes general guidelines for privacy protections that companies and member states must meet.[218]

RESOLUTION (2009), *available at* http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf.

211. *See id.* arts. 22, 27.

212. *Id.* pmbl. paras. 32, 56.

213. *Id.* art. 23(2).

214. *See id.* ch. IV, arts. 22–39.

215. *Id.* arts. 31–32.

216. *Id.* art. 31.

217. *Id.* art. 31(3)(c). However, Article 32(3) also specifies that such notification is not necessary where the data is subject to technological protection measures (for example, encryption) such that it is rendered unintelligible to any person who is not authorized to access it.

218. *See, e.g.*, *id.* art. 30 (regarding security of processing).

D. Harmonization, Consistency, and Clarification of Process

The GDPR was intended to be a "one-stop shop" for data protection for businesses in Europe.[219] The streamlined system envisioned by the GDPR was intended to respond to the European Parliament's call for a strong framework that avoided fragmentation and legal uncertainty by harmonizing EU and national law.[220] Harmonization allows companies operating in multiple member states to enact consistent, robust privacy protection policies for processing personal data across their operations.[221] By adopting the EU Data Protection Directive's network of data protection authorities in each member state, the GDPR seeks to simplify the process. Under the EU Data Protection Directive, businesses were required to notify DPAs in each of the countries in which they operated, wasting their resources and time and those of the DPAs.[222] Under the GDPR, a multinational business will contact the DPA where its business has its main establishment.[223] Similarly, a data subject may contact the DPA in either his or her home member state or else that of the data controller whose practice the data subject seeks to challenge.[224] In either case, the DPA will coordinate with the DPAs of other member states affected by the matter.[225] The GDPR envisions that the national DPAs will have extensive powers to regulate the private sector, including the power to order the controller or processor to order rectification, erasure, or destruction of data processed contrary to the GDPR,[226] to subpoena information from controllers or processors,[227] and to "impose a temporary or definitive

---

219. *Id.* pmbl. para. 98; Viviane Reding, Vice-President, Eur. Comm'n, Strong and Independent Data Protection Authorities: The Bedrock of the EU's Data Protection Reform (May 3, 2012) (transcript available at http://europa.eu/rapid/press-release_SPEECH-12-316_en.pdf).

220. *See* GDPR, *supra* note 1, at 6.

221. EUR. PRIVACY OFFICERS FORUM, EPOF INITIAL COMMENTS ON THE PROPOSED EU DP REGULATION 2 (2012), *available at* http://www.epof.org/files/Uploads/Documents/EPOF/EPOF-Comments_on_Proposed_General_Data_Protection_Regulation_March_2012.PDF.

222. Gilbert, *supra* note 139, at 21; Reding, *supra* note 219.

223. *See* GDPR, *supra* note 1, art. 4(19) (defining "supervisory authority"), arts. 28–29 (governing notification of the supervisory authority).

224. *Id.* pmbl. para. 116; *Id.* art. 75(2).

225. *Id.* arts. 52(1)(c), 55–56.

226. *Id.* art. 53(1)(f).

227. *Id.* art. 53(1)(c).

ban on processing."[228] The national DPAs also have the power to issue opinions and to bring violations of the GDPR to the attention of judicial authorities.[229]

The GDPR also establishes a "consistency mechanism" intended to harmonize the application of the GDPR and to encourage cooperation among the national DPAs.[230] When a DPA adopts a measure that affects more than one member state, such as when it approves binding corporate rules, the DPA must first submit a draft measure to the Commission and the European Data Protection Board, an entity created by the GDPR,[231] for approval.[232] The European Data Protection Board and the Commission may then issue opinions to ensure correct and consistent application of the GDPR.[233]

Finally, in addition to available administrative remedies provided by the EU Data Protection Directive, the GDPR guarantees the data subject the right to a judicial remedy against a controller or processor, or in response to a decision of a DPA.[234] The data subject can bring an action against a data controller where the data controller is established or in the data subject's home jurisdiction.[235] The GDPR also guarantees the right to compensation.[236] Additionally, bodies, organizations, and associations may file group action lawsuits against data controllers or supervisory authorities.[237]

III. APPLICATION TO THIRD COUNTRIES

In a global environment, the transfer of personal data across national borders is an inevitable consequence of modern business. The GDPR attempts to prohibit transfer to a jurisdiction that does not provide adequate privacy and security protections. Apart from the transfer mechanism, it might also impact privacy in for-

228. *Id.* art. 53(1)(g).
229. *Id.* arts. 53(1)(i), 53(3).
230. *See id.* art. 57.
231. *Id.* art. 64.
232. *Id.* art. 58.
233. *Id.* arts. 58(7), 59(1)–(2).
234. *Id.* arts. 74, 75.
235. *Id.* art. 75(2).
236. *Id.* art. 77.
237. *See id.* art. 76(1).

eign jurisdictions through the so-called "California" or "Ratcheting-Up" effect, wherein businesses adopt a uniform set of data practices that satisfy the rules of the most protective jurisdiction.

A. Under the EU Data Protection Directive (Articles 25 and 26)

Under the EU Data Protection Directive, member states are required to prohibit transfers of personal data to non-member states unless the transferee state ensures an adequate level of protection.[238] States should determine whether a level of protection is adequate based on the "nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law . . . in force in the third country in question and the professional rules and security measures which are complied with in that country."[239] Member states and the Commission exchange information on states that they feel do not meet the standard, but the Commission's finding is binding on the States.[240]

Article 26 of the Directive provides that member states shall permit transfers to take place to countries that do not ensure an adequate level of protection where the data subject has consented to the transfer, the transfer is necessary for the performance of a contract, the transfer is necessary to serve important public interest grounds or to protect the vital interests of the data subject, or the transfer contains information in a public register.[241] A series of exemptions allow states to permit transfers to take place where they would otherwise be prohibited.[242]

B. The EU-U.S. Safe Harbor Arrangement

The International Safe Harbor Privacy Principles are a set of principles for certifying that a U.S. organization that handles a European citizen's data provides "adequate" privacy protection as required by the 1995 EU Data Protection Directive.[243]

---

238. EU Data Protection Directive, *supra* note 64, art. 25(1).

239. *Id.* art. 25(2).

240. *Id.* art. 25(3)–(4).

241. *Id.* art. 26(1).

242. *Id.* art. 26(2).

243. *See* Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection

The process for certifying a U.S. organization was developed by the U.S. Department of Commerce in conjunction with the EU.[244] Essentially, the Safe Harbor arrangement provides a framework for U.S. organizations dealing with European customers to send personal data across borders in compliance with EU privacy laws, specifically the EU Data Protection Directive.

To receive certification under the Safe Harbor arrangement, an organization must voluntarily opt in and either perform a self-assessment or hire a third party to perform an assessment to find that it complies with the seven Safe Harbor principles.[245] The Safe Harbor principles provide:

- *Notice.* Individuals must be informed that their data is being collected and about how it will be used.
- *Choice.* Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
- *Onward Transfer.* Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- *Security.* Reasonable efforts must be made to prevent loss of collected information.
- *Data Integrity.* Data must be relevant and reliable for the purpose for which it was collected.
- *Access.* Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
- *Enforcement.* There must be effective means of enforcing these rules.[246]

---

provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, Annex 1, 2000 O.J. (L 215) 7 [hereinafter Safe Harbor], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF.

244. *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, EXPORT.GOV, http://export.gov/safeharbor/ (last visited Feb. 6, 2013).

245. *See* Safe Harbor, *supra* note 243, Annex II (FAQ 6 on self-certification).

246. Safe Harbor, *supra* note 243, Annex I.

Once an organization has self-certified, that organization must recertify every twelve months to remain compliant.[247]

Enforcement of the self-certification program falls under the jurisdiction of the FTC and its ability to prosecute organizations for "deceptive trade practices."[248] If an organization misrepresents that it is certified under the Safe Harbor arrangement, the FTC can seek civil penalties of up to $12,000 per day.[249]

The Safe Harbor arrangement has come under substantial criticism, especially regarding compliance and enforcement of the principles.[250] In 2002, a review performed by the European Commission revealed that organizations which had self-certified under the Safe Harbor arrangement did not live up to the expected degree of transparency.[251] Another study in 2004, which performed a detailed review of ten percent of Safe Harbor organizations, found that numerous companies failed to identify an alternative dispute resolution body, as required by the enforcement principle.[252] By failing to do so, those organizations gave citizens that might be harmed by personal data transfers no recourse to address the harm done to them.[253] Additionally, the Commission found that few organizations post privacy policies that reflect all seven Safe Harbor principles.[254]

---

247. *Id.* Annex II.

248. *See* Robert R. Schriver, Note, *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777, 2781 (2002).

249. *Id.* at 2792.

250. *See, e.g.*, Comm'n of the Eur. Communities, *Commission Staff Working Pape: The Application of Commission Decision on the Adequate Protection of Personal Data Provided by the Safe Harbor Privacy Principles*, SEC (2002) 196 (Feb. 13, 2002) [hereinafter Application of Safe Harbor], *available at* http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf; Comm'n of the Eur. Communities, *Commission Staff Working Document: The Implementation of Commission Decision 520/2000/EC on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce*, SEC (2004) 1323 (Oct. 20, 2004) [hereinafter Implementation of Safe Harbor], *available at* http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf; CHRIS CONNOLLY, THE US SAFE HARBOR—FACT OR FICTION? (2008), http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf.

251. Application of Safe Harbor, *supra* note 250, at 2.

252. Implementation of Safe Harbor, *supra* note 250, at 7–8.

253. *See id.* at 11.

254. *Id.* at 8.

The U.S. FTC has taken some steps to address concerns about the adequacy of the Safe Harbor arrangement. In 2009, the FTC settled with six companies that it determined had deceived consumers by falsely claiming they were abiding by the Safe Harbor arrangement,[255] although no sanctions were imposed.[256] The companies were simply prohibited from misrepresenting the extent to which they participated in any privacy, security, or other compliance program sponsored by a government or any third party.[257] Similarly, in its 2011 settlement with Google, the FTC charged that "Google's assertion that it adhered to the Safe Harbor principles was false because the company failed to give consumers notice and choice before using their information for a purpose different from that for which it was collected."[258] But again the FTC imposed no fines. The settlement simply barred "Google from misrepresenting the privacy or confidentiality of individuals' information or misrepresenting compliance with the U.S.-E.U[.] Safe Harbor or other privacy, security, or compliance programs."[259]

C. Under the General Data Protection Regulation

The GDPR adopts the Data Protection Directive's prohibition on the transfer of data to party countries, regions, or sectors within a country that offer inadequate protection for personal data or are not in compliance with the GDPR.[260] The GDPR clarifies the conditions under which data may be transferred: First, transfers are permitted when the Commission certifies that a third country, territory, or processing sector ensures an adequate level of protection.[261] Second, a controller or processor may transfer data if a legally binding and enforceable instru-

255. Press Release, FTC, FTC Settles with Six Companies Claiming to Comply with International Privacy Framework, (Oct. 6, 2009), *available at* http://ftc.gov/opa/2009/10/safeharbor.shtm.

256. *See id.*

257. *Id.*

258. Press Release, FTC, Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network: Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm.

259. *Id.*

260. *See* GDPR, *supra* note 1, pmbl. paras. 78–82.

261. *Id.* art. 41.

ment establishes appropriate legal safeguards and specified principles, such as minimization and individual control.[262] Finally, data may be transferred under certain specified conditions, such as with consent or if the transfer is necessary for the public interest.[263]

D. The "Ratcheting-Up" Effect

Globalization has had, and continues to have, a profound impact on data privacy regulation and business practices in both the European Union and the United States. This is due primarily to a phenomenon known as the "ratcheting-up effect."[264] This occurs when regulations in one jurisdiction create positive externalities in another jurisdiction. This is the case with the EU Data Protection Directive.[265] Because European privacy regulation affects companies and services that operate in both the EU and the United States, users outside EU jurisdiction can experience benefits.[266] Privacy regulations imposed on U.S. companies by the EU are often more strict than U.S. regulations. When U.S. companies comply with privacy laws in other jurisdictions, they typically raise the privacy and security standards for all users, whether or not they have the benefit of EU legal rights.[267]

In the privacy world, Article 26 of the EU Data Protection Directive drives the ratcheting-up effect.[268] Article 26 seeks to ensure that when data on European citizens is transferred outside the European Union, the protection of the data will be "ade-

---

262. *Id.* art. 42(1)(a), (d).

263. *Id.* art. 44.

264. *See generally* DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY 248–71 (1995).

265. *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, 78 (2000) (describing ratcheting effect of Safe Harbor arrangement on domestic U.S. data processing).

266. *See, e.g.*, Letter from U.S. Consumer Orgs. to European Parliament (Sept. 5, 2012), *available at* http://www.epic.org/privacy/intl/US-Cons-Grps-Support-EU-Priv-Law.pdf ("[W]e believe that the promotion of stronger privacy standards in Europe will benefit consumers around the globe, as businesses improve their privacy practices and security standards.").

267. *See, e.g.*, Shaffer, *supra* note 265.

268. EU Data Protection Directive, *supra* note 64, art. 26.

quate," considering a variety of factors set out in the Directive.[269] The practical consequence of compliance is to raise privacy standards for customers both within and without the European Union, thus "ratcheting up" the standards for data privacy regulation globally.[270] Indeed, the author of the Philippines' new data protection law cited business and investment interests as a reason for basing the law on the EU Data Protection Directive.[271]

IV. RELATED DEVELOPMENTS

The GDPR shoud be placed in the larger international context of related privacy developments, which includes the need for a Third-Pillar Directive regarding data privacy, the Council of Europe Convention 108, the OECD Privacy Guidelines, the APEC Privacy Guidelines, and the U.S. Consumer Privacy Bill of Rights. These frameworks all influenced the development of the GDPR, either as reflections of a similar approach to data protection, or as frameworks that the Commission will have to evaluate through the adequacy mechanism.

A. The Need for a Third-Pillar Directive

The Treaty of Maastricht transformed the European Community into a union with an institutional structure of three "pillars."[272] The first pillar—the European Community and the integration of the common market—was the pillar to which Data Protective Directive activities were limited.[273] The second pillar, Common Foreign and Security Policy, served as the hub of decision making and oversaw the adoption of legislative acts introduced by the European Council.[274] The third pillar was

---

269. *See id.*

270. *See* Todd A. Nova, *The Future Face of the Worldwide Data Privacy Push as a Factor Affecting Wisconsin Businesses Dealing with Consumer Data*, 22 WISC. INT'L L.J. 769, 786–87 (2004).

271. *Senate approves Data Privacy Act on 3rd Reading*, ABS-CBN NEWS, Mar. 20, 2012, http://www.abs-cbnnews.com/business/03/20/12/senate-approves-data-privacy-act-3rd-reading.

272. *See Pillars of the European Union*, EUROPA, http://europa.eu/legislation_summaries/glossary/eu_pillars_en.htm (last visited Feb. 6, 2013).

273. *The Lisbon Treaty and Privacy*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/intl/lisbon_treaty.html (last visited Nov. 24, 2012, 11:42 AM).

274. *Id.*

designated as being responsible for Cooperation on Justice and Home Affairs.[275] Each principal field of activity undertaken by the third pillar had separate data protection responsibilities, undertaken by the EU institutions, agencies and bodies in the framework of the Europol convention, the Council Decision which established Eurojust, the Convention that implemented the Schengen Agreement, and finally the Convention on the use of Information Technology for Customs Purposes.[276]

The Treaty of Lisbon transformed this structure in 2009.[277] The judicial cooperation and police functions of the third pillar were integrated into the European Community, creating a need for a harmonizing approach to data protection and information sharing between member states.[278] Now that the three-pillar system has been eliminated, European Data Protection Supervisor Peter Hustinx has stated that revision of the EU Data Privacy Directive is necessary for three reasons.[279] First, the revision of the current framework will ensure continued effectiveness in a changing world.[280] Second, weaknesses of the present Directive must be addressed.[281] Although the current Directive attempts to harmonize the policies of its member states, having twenty-seven different national versions of the basic principles is too diverse and too complex, creating unnecessary business expenses and a loss of data protection for individual citizens in transborder situations.[282] Third, the Treaty of Lisbon has restructured Europe. Now, data protection is emphasized as an important fundamental human right. The Treaty has "provided a legal basis for horizontal rules on data protection in all EU policy fields,"[283] and must be expanded on to

275. *Id.*
276. *Id.*
277. *Id.*
278. *Id.*
279. Peter Hustinx, Eur. Data Prot. Supervisor, Video Message at Monash University, Melbourne: Review of the EU Framework for Data Protection—The Current State of Play (Feb. 23–24, 2012) (transcript available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2012/12-02-24_Videomessage_Melbourne_EN.pdf).
280. *Id.*
281. *Id.*
282. *Id.*
283. *Id.*

provide coverage in areas that were part of the Third Pillar under the Maastricht Treaty.

B. Modernization of Council of Europe Convention 108

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108,[284] was signed into law on January 28, 1981, and "was the first legally binding international instrument in the data protection field."[285] Parties to the Convention were obliged to enact personal data protection principles into domestic legislation as a fundamental human right.[286] Personal data includes a person's "sensitive" data, such as race, politics, criminal record, sexual life, religion, and health.[287] As of July 24, 2012, forty-four member states of the Council of Europe have signed and ratified the Convention.[288]

The Convention originally sought to provide adequate data protection for current and future growth of automatic data processing.[289] As computers have become increasingly used for administrative purposes, the growth, development, and accessibility of automatic data processing has increased while costs have steadily decreased.[290]

The Convention focused on the social responsibility created by the "information power" that data users in both the public and private sectors possess.[291] Computerized data files including medical information, social security records, and payroll should be protected from misuse or unauthorized disclosure.[292] Advantages of automatic data processing must not weaken the

---

284. Convention 108, *supra* note 36.

285. *Data Protection*, COUNCIL OF EUR., http://www.coe.int/t/dghl/standardsetting/dataprotection/convention_en.asp (last visited Feb. 6, 2013).

286. *See id.*

287. *Summary of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, COUNCIL OF EUR., http://conventions.coe.int/Treaty/en/Summaries/Html/108.htm (last visited Feb. 6, 2013).

288. *See Table of Signatories of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, COUNCIL OF EUR., http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG (last visited Feb. 6, 2013).

289. *See* Convention 108, *supra* note 36, Explanatory Report.

290. *See id.*

291. *Id.*

292. *Id.*

status or well-being of the person to whom it pertains.[293] Furthermore, unnecessary information should not be stored.[294] The Convention recognized that the legal systems of member states covered some of its aims on data protection, but lacked general rules regarding the use and storage of personal information.[295]

The Convention also dealt with protections that should be afforded to the transborder flow of personal data. Principally, fundamental rules of data protection should still apply to data traveling across borders, and such data should be safeguarded as it is in its home country.[296] Practically speaking, however, the wider the geographical area, the weaker data protection is expected to be.[297] Interestingly, many of the principles found in the Convention are similar to those in the OECD's data privacy guidelines,[298] because of "cross-influences between the drafters of the two instruments."[299] The Convention, however, "contains few of the enforcement mechanisms now regarded as essential."[300]

In 2012, the Convention underwent revisions, or "modernisation," and was presented to the Council of Ministers of the Council of Europe in late 2012.[301] The Parliamentary Assembly of the Council of Europe recommended that the proposed revisions not lower protections already established by the Convention and Protocol.[302] The revision also seeks to address future challenges to privacy that will arise as new technologies develop.[303] Furthermore, the Assembly has recommended the

---

293. *Id.*

294. *Id.*

295. *Id.*

296. *Id.*

297. *Id.*

298. *See infra* Part IV.C.

299. Graham Greenleaf, *The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108?*, at 19 (Univ. of Edinburgh Sch. of Law Research Paper Series No 2012/12, 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960299.

300. *Id.*

301. Consult. Comm. of the Convention for the Prot. of Individuals with regard to Automatic Processing of Pers. Data, *Modernisation of Convention 108*, 29th Plen. Mtg. (2012), *available at* http://www.coe.int/t/dghl/standardsetting/DataProtection/TPD_documents/TPD(2012)4Rev3E%20-%20Modernisation%20of%20Convention%20108.pdf.

302. Greenleaf, *supra* note 299, at 24–25.

303. *See* Consult. Comm. of the Convention for the Prot. of Individuals with regard to Automatic Processing of Pers. Data, *Modernisation of Convention 108: new*

creation of a mechanism to monitor compliance.[304] The Committee also made further, more specific recommendations. The definition of sensitive data should be expanded to include genetic, biometric, and health data,[305] and additional measures for controllers, including an obligation to carry out data protection risk analysis and to minimize risk, should be enacted.[306]

Transborder data flows are also addressed. The continuance of an "adequate level of protection" is recommended, especially in the case where data would be communicated or disclosed to recipients who are not subject to the jurisdiction of a Party to the Convention.[307] To maintain an adequate level of protection, standard contractual clauses and binding corporate rules should be encouraged and put in place.[308] The Consultative Committee's powers and functions would be strengthened, further developing its standard-setting functions and role as an international forum for debating emerging privacy issues and forming opinions on accession requests by international organizations or third countries.[309] More flexibility will also be given to amendment procedures.[310]

C. OECD Privacy Guidelines

In 1980, concerned about the increasingly powerful data processing and sharing capability available to both public and private entities, the OECD[311] issued a formal recommendation for the protection of privacy in transborder data flows.[312] The

---

proposals 2, 28th Plen. Mtg. (2012), *available at* http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD-BUR_2012_01Rev_en.pdf.

304. Greenleaf, *supra* note 294, at 24.

305. *Convention 108: New Proposal*, *supra* note 299, at 4.

306. *Id.* at 5.

307. *Id.* at 6.

308. *See id.*

309. *Id.* at 7.

310. *Id.*

311. The Organization for Economic Co-operation and Development is an international organization that shares many of the same member states as the Council of Europe and the European Union. *See generally About the OECD*, OECD, http://www.oecd.org/about (last visited Feb. 6, 2013).

312. OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html.

OECD Privacy Guidelines aimed both to protect privacy and promote the free flow of information.[313]

To achieve these goals, the OECD Guidelines set out eight principles for member countries that subsequently became the basis for national laws around the world.[314] The principles are the Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle, and Accountability Principle. As the OECD explained:

> OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it.[315]

The OECD is currently finishing a review of the Privacy Guidelines.[316] The review notes the remarkable success of the Guidelines in promoting and establishing a global framework for privacy protection, even though the Guidelines lack a formal enforcement mechanism.[317] Not surprisingly, the current emphasis in the review is on implementation and enforcement of the Privacy Guidelines, as well as cross-border cooperation.[318]

D. Asia-Pacific Economic Cooperation Privacy Framework

Established in 1989, Asia-Pacific Economic Cooperation (APEC) is a twenty-one member inter-governmental forum that seeks to facilitate trade cooperation, economic growth, and investment in the Asia-Pacific region.[319] APEC created its 1998

313. *Id.* (as discussed in Preface).

314. *Id.* pt. 2.

315. *Id.* (Preface).

316. *See* OECD, THIRTY YEARS AFTER THE OECD PRIVACY GUIDELINES (2011), *available at* http://www.oecd.org/sti/interneteconomy/49710223.pdf; *see also* Marc Rotenberg, Remarks on the 30th Anniversary of the OECD Privacy Guidelines (Mar. 10, 2010), *available at* http://www.oecd.org/internet/interneteconomy/44946274.doc.

317. OECD, *supra* note 312, at 10, 23.

318. *See id.* ch. 3.

319. *About APEC*, ASIA-PACIFIC ECON. COOPERATION, http://www.apec.org/About-Us/About-APEC.aspx (last visited Feb. 6, 2013).

Blueprint for Action on Electronic Commerce to address the necessity of government and business cooperation in order to achieve the full potential of electronic commerce.[320] Its Electronic Commerce Steering Group (ECSG) supports the principles of the Blueprint, promoting the use and development of electronic commerce by creating law, regulations, and policy in the APEC region that are consistent, predictable, and transparent.[321]

The APEC Privacy Framework includes the application of Data Privacy Individual Action Plans by fourteen countries in order to increase the transparency of data protection, "which in effect will enable other economies to be informed of the relevant stage that an economy has reached."[322] The APEC Data Privacy Pathfinder of 2007 was established with the goal of developing and employing a Cross-Border Privacy Rules system consistent with APEC Privacy Framework.[323] The APEC Cross-Border Privacy Enforcement Arrangement (CPEA) is a product of the Pathfinder initiative that facilitates "domestic and international efforts to promote and enforce information privacy protections."[324] The CPEA, which commenced in 2010, endeavors to increase consumer confidence "in electronic commerce involving cross-border data flows by establishing a framework for regional cooperation in the enforcement of Privacy Laws."[325] It establishes a framework for voluntary information sharing and for assistance in enforcing information privacy.[326] Information sharing and cooperation in privacy investigation and enforcement outside APEC is also encouraged.[327]

---

320. *APEC Cross-border Privacy Enforcement Arrangement*, ASIA-PACIFIC ECON. COOPERATION, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx (last visited Feb. 6, 2013).

321. *Electronic Commerce Steering Group*, ASIA-PACIFIC ECON. COOPERATION, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx (last visited Feb. 6, 2013).

322. *Data Privacy Individual Action Plan*, ASIA-PACIFIC ECON. COOPERATION, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/link.aspx?_id=CB717EE6184848D396F31DBB814E5C90&_z=z (last visited Feb. 6, 2013).

323. *APEC Data Privacy Pathfinder*, ASIA-PACIFIC ECON. COOPERATION, http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx (last visited Feb.6, 2013).

324. *APEC Cross-border Privacy Enforcement Arrangement*, *supra* note 320.

325. *Id.*

326. *Id.*

327. *Id.*

E. The U.S. Consumer Privacy Bill of Rights

Although the United States played an active role in the adoption of the OECD Privacy Guidelines in 1980 and the Safe Harbor Arrangement in the late 1990s, not much has happened in the past decade to address the need for a more global approach to privacy protection. However, that may be changing. In February 2012, the White House released a framework to enhance the protection of individual consumer data through a number of general principles that will provide a strengthened baseline of consumer protections while at the same time allowing companies innovation-enhancing flexibility to implement privacy protection.[328] In announcing this Consumer Privacy Bill of Rights, President Barack Obama stated that "even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever."[329]

The Consumer Privacy Bill of Rights set out a seven-point framework, similar to the OECD Privacy Guidelines, governing the treatment of personal data by both the consumers to whom it pertains and the companies that use this information during the course of business.[330] The framework's seven principles are: individual control; transparency; respect for context; security; access and accuracy; focused collection; and accountability.[331]

According to the White House framework, consumers have an inherent right of individual control of their personal data—that is, to be in charge of what data is collected by companies and how it may be used.[332] Companies should present consumers with more control on what data they wish to disclose and what data to suppress by providing consumers with simple and clear choices in a timely manner, enabling consumers to

---

328. *See* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1–2 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

329. *Id.* (un-paginated letter).

330. *See id.*; *id.* at 10.

331. *Id.* at 47–48.

332. *Id.* at 47.

make meaningful decisions.[333] Further, companies should provide a user-friendly, easily accessible mechanism for consumers to limit or withdraw consent.[334]

Second, to achieve individual control, companies must be transparent.[335] Consumers have the right to accessible and easily understandable information about companies' security and privacy practices.[336] This information includes descriptions of the data to be collected and for what purposes, a timeline for the deletion or de-identification of the data, and whether and for what purpose the data may be shared with third parties.[337]

Third, "[c]onsumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."[338] Use and disclosure of personal data must be consistent with the purpose for which it was provided, unless otherwise directed by law.[339] If a company releases or plans to release personal data for another purpose, it should provide heightened measures of transparency and individual control by disclosing said purpose in a user-friendly and easily accessible format when the data is first collected.[340] If the company decides to disclose data after it is collected for purposes different from those of its original collection, it must again provide enhanced transparency and individual choice.[341] Companies must take into account the age and technological sophistication of their consumers.[342] In doing so, companies may have to create varying levels of data protections for children, teenagers, and adults.[343]

Fourth, consumers have the right to have their personal data handled responsibly and securely.[344] To achieve this right, companies should evaluate any security or privacy risks con-

---

333. *Id.*
334. *Id.*
335. *Id.*
336. *Id.*
337. *Id.*
338. *Id.*
339. *Id.*
340. *Id.*
341. *Id.* at 48.
342. *Id.*
343. *Id.*
344. *Id.*

nected to their data practices.[345] Safeguards should be in place to prevent and minimize risks such as improper disclosure, destruction, loss, or unauthorized access.[346]

Fifth, "[c]onsumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate."[347] Companies should take reasonable measures to maintain accurate personal data, and provide consumers with reasonable access to their personal data, along with a method for correcting inaccurate data, or deleting or limiting its use, in a manner consistent with freedom of expression and freedom of the press.[348] Companies should consider the scope, scale, and sensitivity of the personal data they are collecting or maintaining, and the likelihood that it might expose consumers to physical, financial, or other material harms when determining procedures to carry out this provision.[349]

Sixth, "[c]onsumers have a right to reasonable limits on the personal data that companies collect and retain."[350] Companies should only collect the data they need to complete the purposes that have been listed under the "respect for context" principle.[351] Data should be de-identified or securely disposed of after it is no longer needed, unless this would conflict with other legal obligations.[352]

Finally, "[c]onsumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights."[353] Consumers and enforcement authorities must hold companies accountable, and companies should hold their employees accountable for adhering to the Consumer Privacy Bill of Rights through training, evaluation, and audits.[354] If a company divulges personal data to a third party, it needs to ensure that the

345. *Id.*
346. *Id.*
347. *Id.*
348. *Id.*
349. *Id.*
350. *Id.*
351. *Id.*
352. *Id.*
353. *Id.*
354. *Id.*

third party is contractually obliged to adhere to the seven principles, unless they are required to do otherwise by law.[355]

The White House recommends that the Consumer Privacy Bill of Rights be implemented through a multistakeholder approach, including industry groups, privacy advocates, individual companies, consumer groups, academics, and international partners, to produce solutions in a transparent and timely manner without relying "on a single, centralized authority to solve problems."[356] At the same time, President Obama has expressed the view that these rights should be established in law. In setting forth the Consumer Privacy Bill of Rights, the President stated, "My Administration will work to advance these principles and work with Congress to put them into law."[357]

CONCLUSION

The General Data Protection Regulation, now under consideration in the European Union, is the latest stage in the development of modern privacy law. According to Viviane Reding, the Vice President of the European Commission and EU Justice Commissioner, the European Commission anticipates that the member states will pass the draft GDPR by the end of 2013.[358] The GDPR will apply to the member states approximately two years after it is passed and published in the *Official Journal of the European Union*.[359] When adopted, the GDPR will reflect the continued integration of the European member countries, the evolution of modern technology and business practices, and the insights gained from the post-War efforts to safeguard the fundamental human right to privacy. The benefits for users of new Internet-based services will be substantial.[360]

---

355. *Id.*

356. *Id.* at 23–24.

357. *Id.* (preface).

358. Reding, *supra* note 219, at 9.

359. *See* GDPR, *supra* note 1, art. 91.

360. *See, e.g.*, Grant Gross, *U.S. privacy, consumer groups back EU's proposed privacy rules*, COMPUTER WORLD, Sept. 5, 2012, http://www.computerworld.com/s/article/9230931/U.S._privacy_consumer_groups_back_EU_39_s_proposed_privacy_rules.