INTANGIBLE PRIVACY RIGHTS: HOW EUROPE'S GDPR WILL SET A NEW GLOBAL STANDARD FOR PERSONAL DATA PROTECTION

*Beata A. Safari**

I. INTRODUCTION

The European Union ("EU" or the "Union") prides itself on the extensive privacy protections it affords its citizens: protections that far outweigh those provided to American citizens.[1] The European Union Charter on Fundamental Rights ("the Charter"), enacted in 2000, provides the basis for European recognition of the importance of protecting personal data.[2] Under Article 8 of the Charter, "[e]veryone has the right to the protection of personal data[3] concerning him or

* J.D. Candidate, 2017, Seton Hall University School of Law; B.A., *magna cum laude*, The George Washington University. I am deeply thankful to Professor Tracy Kaye for introducing me to the *Schrems* Case, sparking my interest in this subject matter. I thank my faculty advisor, Professor David Opderbeck, for providing me with the foundation I needed to understand Internet law. I thank Professor Gaia Bernstein for opening my eyes to the world of information privacy and contributing to this Comment. As always, I am eternally grateful for the support of my family and loved ones.

[1] Instead of the omnibus approach of the European Union, the United States has a variety of statutes and regulatory agencies which cover aspects of privacy law. These statutes include, but are not limited to, the following: The Computer Fraud and Abuse Act of 1986 (CFAA), 18 U.S.C. § 1030 (2012); Cybersecurity Information Act of 2015, 6 U.S.C. §§ 1501–1533 (2012); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996); Bank Secrecy Act of 1970 (BSA), Pub. L. No. 91-508, 84 Stat. 1114-2 (2012). *See* Daniel Dimov, *Differences between the Privacy Laws in the EU and the US*, INFOSEC INST. (Jan. 10, 2013), http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/.

[2] *See Charter of Fundamental Rights of the European Union: Explanations Relating to the Complete Text of the Charter*, EUR. UNION COUNCIL 26 (Dec. 2000), http://www.consilium.europa.eu/uedocs/cms_data/docs/2004/4/29/Explanation%20relating%20to%20the%20complete%20text%20of%20the%20charter.pdf.

[3] "Personal data" is defined as "any information relating to an identified or identifiable legal person ('data subject')." "Processing of personal data" is "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Council Directive 95/46/EC, art. 2(a), 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].

her," particularly with regard to the fair processing of data "for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[4] Directive 95/46/EC ("Data Protection Directive" or "the Directive") influenced the freedom of protection of personal data, notably in its preamble where it acknowledges differences in the levels of protection with respect to the right to privacy and that "the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State."[5] Most Americans could not fathom the importance privacy holds to Europeans: one popular theory describes this phenomenon as the difference between valuing liberty, for Americans, and dignity, for Europeans.[6]

Data protection is so important to European citizens that the European Union requires foreign entities—particularly the United States, where most technology companies are headquartered—to adhere to its stringent requirements.[7] The U.S.-EU Safe Harbor Framework ("Safe Harbor Framework" or "Safe Harbor") was created by the U.S. Department of Commerce working with the European Commission ("the Commission") as a means of implementing the "adequacy" framework adopted by the European Union's Data Protection Directive.[8] Under the adequacy framework, American

[4] Charter of Fundamental Rights of the European Union art. 8, 2000 O.J. (C 364/1).

[5] Data Protection Directive, *supra* note 3, at art. 7.

[6] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1163 (2004) ("If I may use a cosmological metaphor: American privacy law is a body caught in the gravitational orbit of liberty values, while European law is caught in the orbit of dignity. There are certainly times when the two bodies of law approach each other more or less nearly. Yet they are consistently pulled in different directions, and the consequence is that these two legal orders really do meaningfully differ: Continental Europeans are consistently more drawn to problems touching on public dignity, while Americans are consistently more drawn to problems touching on the depredations of the state. Indeed, as our many transatlantic conflicts suggest, the distances between us can often stretch into the unbridgeable.").

[7] Companies must adhere to requirements because the Data Protection Directive promises EU citizens protection of personal data, which cannot be achieved without the participation of the countries from whence the data originates. *Safe Harbor Certification*, PRIVACYTRUST (Feb. 2016), http://www.privacytrust.com/guidance/safe_harbor.html. A list of all participants in the Safe Harbor Framework can be found at *U.S.-EU Safe Harbor List*, U.S. DEP'T COM., https://safeharbor.export.gov/list.aspx (last visited Dec. 20, 2016) (a user types an identifier of the company in the search for "Organization Name," which brings up the name of the organization as it was certified, how long it is U.S.-EU certified for, and the nature of its personal data).

[8] *Welcome to the U.S.-EU Safe Harbor*, U.S. DEP'T COM. (Jan. 26, 2017, 12:38 PM), http://2016.export.gov/safeharbor/eu/eg_main_018475.asp [hereinafter *Safe Harbor Overview*]. *See Safe Harbor Certification*, *supra* note 7.

organizations avoided interruptions or delays in their dealings with the Union due to EU member states ("Member States") privacy laws.[9] The program provided a number of benefits to participating American and European organizations, including: delivering "adequate" privacy protection; binding Member States by the European Commission's finding of "adequacy"; bringing claims by EU citizens in the United States; and structuring compliance requirements to be cost-effective, with the benefit resting on small and medium businesses.[10]

Although in 1995 the Data Protection Directive set an unprecedented foundation for personal data protection, in 2012, the European Union proposed a reform of data protection rules[11] because protection has not remained current through the immense technological advances that have taken place since. Furthermore, the nature of the legislation has prevented every EU Member State from implementing uniform standards across the board.[12] Now, the new proposed General Data Protection Regulation (GDPR), if successful, will "make Europe fit for the digital age."[13]

This Comment argues that certain articles in the GDPR would impose greater requirements for data privacy, for example, the provisions on "profiling," the right to data portability, and the "right to be forgotten." The directive proposed to accompany the GDPR in the areas of investigation and prosecution, among other police duties, in relation to criminal offenses and other judicial activities,[14] is outside the scope of this Comment. Additionally, the focus in this Comment is on "controllers" of personal data, not on "processors" of personal data.[15] Part II explores the goals of the Data Protection Directive and

[9] *Safe Harbor Overview*, *supra* note 8.

[10] *Safe Harbor Privacy Principles: Issued by the U.S. Department of Commerce on July 21, 2000*, U.S. DEP'T COM. (Jan. 30, 2009, 3:03 PM), http://2016.export.gov/safeharbor/eu/eg_main_018475.asp.

[11] *Protection of personal data*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/ (last visited Feb. 6, 2017).

[12] Press Release, European Comm'n, Agreement on Commission's EU data protection reform will boost Digital Single Market (Dec. 15. 2015), europa.eu/rapid/press-release_IP-15-6321_en.htm.

[13] *Id.*

[14] Press Release, European Comm'n, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.pdf [hereinafter Commission proposes a comprehensive reform of data protection rules].

[15] A "controller" is "the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and

the Safe Harbor Framework, as well as some of their major criticisms, leading to the adoption of the new GDPR and the EU-U.S. Privacy Shield. Part III breaks down strengths and weaknesses of the GDPR, introduces the cases which influenced change in the Union's privacy regime, and analyzes how some key articles would affect foreign entities. Part IV discusses how data privacy changes would affect the future affairs of a company such as LinkedIn through application of the provisions and analysis discussed in Part III. Part V aggregates the analysis from Part IV and superimposes it upon anticipated new technological advances and the effectiveness of the GDPR in light of those advances. Finally, Part VI, the conclusion, condenses the information in this Comment to predict the implications of the GDPR on a new global privacy standard.

II. THE DATA PROTECTION DIRECTIVE: IMPLEMENTATION IN THE EU AND THE U.S.

A. *Goals of Data Protection Directive*

When the Data Protection Directive passed on October 24, 1995, it was approved in the context of two pieces of legislation: the European Convention on Human Rights (ECHR), and the Organization for Economic Co-operation and Development (OECD)'s "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data."[16] Article 8 of the ECHR introduces the right to respect one's private and family life, home, and correspondence, stating:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of: national security; public safety or the economic wellbeing of the country; for the prevention of disorder or crime; for the protection of health or morals; or for the protection of

repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(7), 2016 O.J. (L 119) 1 [hereinafter GDPR Provisions]. A "processor" is "a natural or legal person, public authority, agency or other body which processes personal data *on behalf of the controller*." *Id.* art. 4(8) (emphasis added). For a list of the kinds of services that a controller could complete which a processor cannot, see Vanessa Barnett, *Data controllers and data processors: what is the difference?*, CHARLESRUSSELLSPEECHLYS (June 4, 2014), https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/tmt/2014/data-controllers-and-data-processors-what-is-the-difference/.

[16] The OECD Guidelines have since been updated. *2013 OECD Privacy Guidelines*, ORG. ECON. CO-OPERATION & DEV. (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

the rights and freedoms of others.[17]

The goals for implementing the Directive were an amalgamation of the promotion of free-flowing data and the protection of fundamental human rights. Under the preamble, the Directive was meant to encourage the easy flow of personal data from one Member State to another, while also preserving fundamental rights of individuals.[18] The general facilitation of cross-border flows of personal data was a major factor. The Commission also recognized that the processing of data carried out by a person in a third country should not interfere with the protection granted to European Union citizens.[19] In addition, the processing of personal data must be carried out with the consent of the individual, unless the personal data may be disclosed due to legitimate ordinary business activities of companies.[20] In the context of the advancement of human rights goals, the Directive sought to strengthen and promote peace and liberty and other fundamental freedoms as provided in the European Convention, primarily the right to privacy.[21] Although not expressly provided for in the Directive, article 12(b) could be considered the first real primer on the "right to be forgotten."[22]

B. *Safe Harbor Framework*

Until February 2016, the Safe Harbor Framework allowed American companies to enter the European marketplace through an assurance that the American companies were complying with the basic data requirements imposed by the Data Protection Directive.[23] Entering into the U.S.-EU Safe Harbor Framework was an entirely voluntary decision and required adherence to only a few conditions.

---

[17] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter ECHR].

[18] Data Protection Directive, *supra* note 3, ¶¶ 8, 9 ("[I]n order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States . . . . Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy . . . .").

[19] *Id.* ¶ 20 ("[T]he fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive . . . .").

[20] *Id.* ¶ 30 ("[T]he processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject . . . .").

[21] Data Protection Directive, *supra* note 3, at pmbl. (1), (2).

[22] *Id.* art. 12.

[23] Although, arguably, the Safe Harbor Framework is not defunct until the EU-U.S. Privacy Shield is fully in place. *Safe Harbor Overview*, *supra* note 8.

To qualify for membership in the program, an organization could either join a self-regulatory privacy program that already adhered to the requirements, or it could develop its own self-regulatory privacy program in conformance with the framework. Beyond that, compliance was monitored by adherence to the seven Safe Harbor Privacy Principles, which are: (1) notice; (2) choice; (3) onward transfer; (4) access; (5) security; (6) data integrity; and (7) enforcement.[24]

The notice principle required organizations to notify data users about the purposes for which information was collected and used.[25] The choice principle required that data users be given the opportunity to opt out from disclosing personal information to a third party.[26] For sensitive information, an explicit choice must have been given if the information would have been disclosed to a third party or used for a purpose other than originally intended.[27] The onward transfer principle simply acknowledged that in order to disclose information to a third party, an organization must have complied with the notice and choice principles.[28] The organization needed to ensure that the third party subscribed to the Safe Harbor Framework principles (or it needed to enter into a contractual agreement to confirm that it did so).[29] The access principle required data users to have access to information about themselves that the company held, and to have the ability to correct, amend, or delete information.[30] This access principle resembles the "right to be forgotten" principles, in that the General Data Protection Regulation, described in detail *infra* Part III.C., would ensure that users have the ability to control their level of engagement, as well as the extent of the personal data they share. The security principle charged organizations to implement precautions in protecting personal information from loss, misuse and unauthorized access, disclosure, alteration, and destruction.[31] The data integrity principle needed organizations to take sensible steps to ensure that data was reliable for its intended use, accurate, complete, and current.[32] The enforcement principle required: (1) instantly available and affordable mechanisms so that each individual's complaints and

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Safe Harbor Overview*, *supra* note 8.
[30] *Id.*
[31] *Id.*
[32] *Id.*

disputes could be investigated and resolved; (2) procedures to validate that commitments to Safe Harbor principles had been adhered to; and (3) commitments to solve problems arising out of failure to comply with the principles.[33]

Some of the most prominent criticisms of the Safe Harbor Framework include: a failure to renew certification, lack of certification or receipt of certification twice, distribution of false and misleading information regarding certification under the Framework, and a difficulty in establishing enforcement mechanisms and following through with complaints.[34] With regard to the lack of adequate compliance, only 348 out of 1109 registered organizations under the Safe Harbor complied with the most basic requirements of the Framework.[35] The Safe Harbor had not worked properly in a long time, so when the European Union proposed the General Data Protection Regulation, it was clear that the United States would be directly affected. Thus, negotiations between the United States Commerce Department and the European Commission commenced.

---

[33] *Id.*

[34] *See* CHRIS CONNOLLY, THE US SAFE HARBOR – FACT OR FICTION? 1, 4, 7 (2008), http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf. *See, e.g.*, Comm'n of the European Communities, *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council 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* 8 (Working Paper No. SEC(2002) 196), http://web.archive.org/web/20060724174359/http://www.ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf ("A substantial number of organisations that have self-certified do not meet the requirement in FAQ 6 [on self-certification] quoted above. For some, no public statement of adherence to the Safe Harbour Principles could be found, apart from the self-certification itself. For a small number, the privacy policy mentioned in the self-certification could not be accessed."); Comm'n of the Communities, *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* 7–8 (Working Document No. SEC(2004) 1323) ("Regarding the enforcement Principle, which requires companies to identify either an Alternative Dispute Resolution body or the EU panel to hear individuals' complaints, the Commission notes that a number of companies fail to do so. When companies select the EU panel, almost all of them fail to state their commitment to comply with the advice of the EU panel as required by FAQ 9 [when HR data is transferred from Europe to a Safe Harbor organization], or to indicate how the EU panel can be contacted. When companies select ADRs, they often fail to inform individuals of the arrangements for taking up complaints with the ADR.").

[35] *See* CONNOLLY, *supra* note 34, at 4.

C. *American Involvement in the GDPR and EU-U.S. Privacy Shield*

Extensive American involvement in the drafting of the GDPR, discussed further *infra* Part II.D, and implementation of changes in the Safe Harbor Framework have culminated in the new EU-U.S. Privacy Shield ("Privacy Shield").[36] In 2013, American companies and the American government lobbied at length to amend provisions requiring businesses to obtain explicit consent from consumers before collecting data, and to take out provisions that would allow consumers to remove all traces of personal data upon request.[37] Since then, the United States remained actively engaged in negotiations for the enactment of a new safe harbor agreement in Brussels.[38] In fact, American involvement has been so extensive that LobbyPlag, a website whose purpose consists of delivering greater transparency of ongoing deliberations in the European Commission about the GDPR by leaking documents,[39] is merely one among about a dozen privacy groups that called on the U.S. government to cease its "unprecedented lobbying campaign."[40]

Aside from the imposition of American beliefs on European citizens, the Massachusetts Institute of Technology began a collaborative project with the University of Amsterdam called the EU-U.S. Privacy Bridge Project ("Bridge Project") in May 2014, whose aim is to "bridge the gap between the data privacy regimes in the United States and the European Union," thus strengthening the framework of the Safe Harbor.[41] The Bridge Project published its recommendations

[36] Rob Price, *Europe Narrowly Avoided a Major Disaster for American Businesses – For Now*, BUS. INSIDER (Feb. 4, 2016, 3:00 AM), http://www.businessinsider.com/privacy-shield-european-regulators-article-29-working-party-full-text-2016-2?r=UK&IR=T.

[37] Kevin Collier, *U.S. Lobbyists Are Writing Europe's Data Protection Rules*, DAILY DOT (Feb. 11, 2013, 14:25 CT), http://www.dailydot.com/news/us-lobbyists-european-data-privacy/. The U.S. government struggled with the notion that personal data could be removed upon request of the individual affected: this is contrary to the drafting of American statutes, such as the CAN-SPAM Act, and to the philosophy of "opting out." *See infra* note 101.

[38] Mark Scott, *Data Transfer Pact Between U.S. and Europe Is Ruled Invalid*, N.Y. TIMES (Oct. 6, 2015), http://nyti.ms/1OhKvgl.

[39] *Governments*, LOBBYPLAG (Jan. 16, 2016, 2:14 EST), http://www.lobbyplag.eu/governments.

[40] Collier, *supra* note 37 ("[T]here are 64 instances where proposed amendments to the Data Protection Regulation have text identical to passages from previously-written lobbyist memos."); Zack Whittaker, *Privacy Groups Call on US Government to Stop Lobbying Against EU Data Law Changes*, ZDNET (Feb. 4, 2013, 6:00 GMT), http://www.zdnet.com/article/privacy-groups-call-on-us-government-to-stop-lobbying-against-eu-data-law-changes/.

[41] *Privacy Bridges Project Mission*, MASS. INST. TECH., https://privacybridges.mit.edu/ (last visited Mar. 20, 2017). *See also* Cynthia O'Donoghue & Katalina Bateman, *EU-*

in September 2015, offering ten "bridges" to enhancing a "progressive, sustainable model for protecting privacy in the global Internet environment."[42] Although the Bridge Project is not a governmental initiative, it does have "soft support" from the European Commission and did have "soft support" from the Obama Administration,[43] so it could be a step in the right direction if the EU and U.S. choose to adhere to the recommendations.

D. *The Doubtful Efficacy of the Privacy Shield*

On February 2, 2016, the European Union and United States confirmed that the European Commission and Department of Commerce had agreed upon the provisions of the Privacy Shield.[44] The United States Secretary of Commerce, Penny Pritzker, referred to the agreement as the "product of two years of productive discussions among [European and American] teams."[45] Laura E. Gardner, from the Office of the Chief Counsel for International Commerce—speaking on her own behalf—stated that, "We are really confident that we addressed all of the concerns" from the court, EU Commission, and critics.[46] She exuded excitement at the steady in-flow of self-certifications from American companies; she claimed that nearly 300 had been completed at the time.[47] At the same time, Gardner

US Privacy Bridge Project Announced, REEDSMITH (May 8, 2014), http://www.technologylawdispatch.com/2014/05/privacy-data-protection/eu-us-privacy-bridge-project-announced/; Angela R. Matney et al., *The Challenges of Third-Party Data Privacy Protection*, 61 RISK MGMT. 32, 34 (2014).

[42] JEAN-FRANÇOIS ABRAMATIC ET AL., PRIVACY BRIDGES: EU AND US PRIVACY EXPERTS IN SEARCH OF TRANSATLANTIC PRIVACY SOLUTIONS (2015), http://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf.

[43] Matney et al., *supra* note 41, at 34.

[44] Press Release, European Commission, EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield (Feb. 2, 2016), http://europa.eu/rapid/press-release_IP-16-216_en.htm.

[45] Commission Implementing Decision (EU) 2016/1250, 2016 O.J. (L 207) (Annex I) 1 (letter from U.S. Secretary of Commerce Penny Pritzker).

[46] Laura E. Gardner, Senior Attorney, Office of the Chief Counsel for Int'l Commerce, U.S. Dep't Com., Address at the Seton Hall Law Review Symposium (Sept. 30, 2016) [hereinafter Gardner Address].

[47] *Id.* Since then, it appears that more than 500 companies have self-certified, which still falls far short of the over 4,400 companies certified under the Safe Harbor Framework. Peter Loshin, *EU-U.S. Privacy Shield certification process picks up steam, slowly*, TECHTARGET (Oct. 21, 2016, 8:30 AM EST), http://searchsecurity.techtarget.com/news/450401509/EU-US-Privacy-Shield-certification-process-picks-up-steam-slowly [hereinafter *EU-U.S. Privacy Shield*]. *See, e.g.*, *MobileIron Receives EU-US Privacy Shield Certification from US Department of Commerce*, NEWSWIRE ASS'N LLC (Dec. 19, 2016, 2:00 PM EST), http://www.prnewswire.com/news-releases/mobileiron-receives-eu-us-privacy-shield-

acknowledged that the Privacy Shield complies with the Data Protection Directive, and not the GDPR; she asserted that the Commerce Department is aware of this and will adjust.[48] Per this adjustment process, Gardner provided that this process offers an opportunity to cooperate with the European Union, so the Commerce Department will adapt and respond to changes in Europe and the United States: "We are going to keep working with Europe."[49]

The four major changes that the EU Commission and the United States claim will take effect as a result of the new framework are: (1) greater responsibilities on companies exchanging with European users; (2) a more capable enforcement structure; (3) clearer security measures and more transparency of American government access; and (4) competent and adequate protection of European citizens' rights with multiple avenues for reparations.[50] It is of note that the United States has agreed to deliver clear limitations and oversight mechanisms which would greatly diminish the U.S.'s ability to engage in surveillance.[51] It has also agreed to refrain from indiscriminate mass surveillance.[52] With regard to the last element, the Privacy Shield would institute formal deadlines for companies to reply to complaints, and alternative dispute resolution would be provided without a fee.[53]

The United States has assured the European Commission that it will institute an annual joint review, discussing the companies' adherence to the principles.[54] The Privacy Shield aims to provide Europeans the opportunity for redress in the United States through the Judicial Redress Act of 2015, whose purpose is to "extend Privacy Act remedies to citizens of certified states," with the European Union being one of those certified states under section 2(d)(1)(A)(i), as it "has entered into an agreement with the United States that provides for appropriate privacy protections for information."[55]

Reports about the new provisions have proved lukewarm, at best.

certification-from-us-department-of-commerce-300380686.html; *Ultimate Completes Certification for Cloud Security Standard ISO 27018*, BUSINESSWIRE (Dec. 19, 2016), http://www.businesswire.com/news/home/20161219005684/en/Ultimate-Completes-Certification-Cloud-Security-Standard-ISO.

[48] Gardner Address, *supra* note 46.

[49] *Id.*

[50] *EU-U.S. Privacy Shield*, *supra* note 47.

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] Judicial Redress Act of 2015 (H. R. 1428), Pub. L. No. 114-126, 130 Stat. 282 (2016).

Critics have expressed concern that the Privacy Shield will not become enforceable because it will not pass court scrutiny, European Member States will not agree to pass it, and the document has no teeth to it.[56] According to the Harvard Business Review, the Privacy Shield "will likely do nothing to add even a modicum of new protection to the personal information of European citizens."[57] The man who almost single-handedly brought about the demise of the Safe Harbor Framework, Maximilian Schrems (discussed *infra* Part III.D.ii), found the Privacy Shield lackluster: "There are tiny improvements, but the core rules on private data usage are miles away for EU law. This is nowhere close to 'essential equivalence' that the Court required."[58] Schrems even went so far as to say, "They put ten layers of lipstick on a pig but I doubt the [Court and Data Protection Authorities] suddenly want to cuddle with it."[59]

Confirming the predictions of many, in September 2016, a privacy group filed a challenge in the General Court of the European Court of Justice (ECJ).[60] There is very little known about the challenge so far, and according to the procedure of the ECJ, it would take more than a year for the matter to be heard.[61] What is clear is that the privacy

---

[56] *See generally* Caroline Craig, *EU-US Privacy Shield Offers Flimsy Protection*, INFOWORLD (Feb. 5, 2016), http://www.infoworld.com/article/3029969/privacy/eu-us-privacy-shield-offers-flimsy-protection.html; Larry Downes, *The Business Implications of the EU-U.S. "Privacy Shield"*, HARV. BUS. REV. (Feb. 10, 2016), https://hbr.org/2016/02/the-business-implications-of-the-eu-u-s-privacy-shield; Natasha Lomas, *Draft Text of the EU-U.S. Privacy Shield Deal Fails To Impress The Man Who Slayed Safe Harbor*, TECHCRUNCH DAILY (Feb. 29, 2016), http://techcrunch.com/2016/02/29/lipstick-on-a-pig/.

[57] Downes, *supra* note 56.

[58] Lomas, *supra* note 56.

[59] David Gilbert, *Safe Harbor 2.0: Max Schrems Calls 'Privacy Shield' National Security Loopholes 'Lipstick On A Pig'*, INT'L BUS. TIMES (Feb. 29, 2016, 1:30 PM), http://www.ibtimes.com/safe-harbor-20-max-schrems-calls-privacy-shield-national-security-loopholes-lipstick-2327277 (quoting @MaxSchrems, TWITTER (Feb. 29, 2016)).

[60] *Action brought on 16 September 2016 – Digital Rights v Commission (Case T-670/16)*, CURIA, http://curia.europa.eu/juris/document/document.jsf?text=&docid=185146&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=423368 (last visited Dec. 20, 2016) [hereinafter *Digital Rights v Commission*] (reader should make sure that the "Language of document" is in "English").

[61] There is no mention in the ECJ Rules of Procedure how long the court could take to decide a case; yet, given that the privacy group concerned did not request an urgent preliminary ruling, the decision will likely not be expedited. The President of the Court may, however, separately consider whether urgency is necessary. *Consolidated Version of the Rules of Procedure of the Court of Justice of 25 September 2012*, EUR. CT. JUST. arts. 107–08 (2012), http://curia.europa.eu/jcms/upload/docs/application/pdf/2012-10/rp_en.pdf. *See also* Reuters, *This Privacy Group is Challenging the U.S.-EU Data Pact*, FORTUNE.COM (Oct. 27, 2016, 8:59 AM EST), http://fortune.com/2016/10/27/privacy-data-eu-us/.

group, Digital Rights Ireland, petitions the court to "declare that the [Commission Implementing Decision (EU) 2016/1250 of 12 July 2016][62] is null and void" and to "order the annulment of the [Commission Implementing Decision] relating to the adequacy of the protection provided by the EU-US Privacy Shield."[63] Among the court's challenges will be to determine whether the Privacy Shield is even of direct concern to the privacy group, a standing issue.[64]

It remains to be seen what the legacy of the Privacy Shield will be. While it is too early to know how it will be treated in the courts, the Privacy Shield has been accepted by the European Commission[65]—which means that Member States must adhere to the decision[66]—and the European Court of Justice will likely not come face-to-face with the agreement until late 2017 or early 2018. Notwithstanding any challenges, it is law, so businesses will need to adapt, fast. As the Department of Commerce is aware, the Privacy Shield needs modification to conform to the provisions of the GDPR, which will replace the Data Protection Directive in May 2018.[67]

III. THE GENERAL DATA PROTECTION REGULATION (GDPR)

A. *The Distinction Between Directives and Regulations*

There is an important distinction between EU directives and regulations, and that distinction is among the reasons why the European Commission strived to replace the Data Protection Directive by a regulation. Directives are broad, goal-driven pieces of legislation which provide guidelines for Member State implementation, but depend on the independent passage of a law in every Member State

[62] Commission Implementing Decision (EU) 2016/1250, *supra* note 45, at art. 13 ("The Commission has carefully analysed U.S. law and practice, including these official representations and commitments. Based on the findings developed in recitals 136-140, the Commission concludes that the United States ensures an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the Union to self-certified organisations in the United States.").

[63] *Digital Rights v Commission*, *supra* note 60.

[64] *See This Privacy Group is Challenging the U.S.-EU Data Pact*, *supra* note 61.

[65] *See generally* Commission Implementing Decision, *supra* note 45.

[66] For a description of how the European Commission works, see generally *European Commission at Work*, EUR. COMMISSION, http://ec.europa.eu/atwork/index_en.htm (last visited Mar. 4, 2017) (for more information, click on "How decisions are made" and "Decision-making during weekly meetings").

[67] GDPR Provisions, *supra* note 15, at art. 51(4) ("Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.").

within a designated period of time.[68] Regulations are narrow, specific pieces of legislation which become immediately enforceable—and binding—in every Member State without implementing a law in each State.[69] When the European Commission first considered reforming data protection, it was not yet clear that a directive would be replaced by a regulation.[70] The Commission committed to addressing the following issues:

> (1) Addressing the impact of new technologies;
> (2) Enhancing the internal market dimension of data protection;
> (3) Addressing globalisation and improving international data transfers;
> (4) Providing a stronger institutional arrangement for the effective enforcement of data protection rules;
> (5) Improving the coherence of the data protection legal framework.[71]

The first challenge, addressing the impact of new technologies, focuses on the difficulty in ensuring free and informed consent, and securing sensitive data, thus assuring transparency for individuals on the Internet.[72] The second challenge in enhancing the internal market dimension of data protection takes into account the limited remedies available to nationals for bringing complaints in front of their courts, ensuring legal certainty, and curtailing the administrative burden of the notification system.[73] In responding to the third challenge—improving international data transfers—the Commission likely only envisioned the passage of a new law in the European Union; that would not have been sufficient. However, the EU-U.S. Privacy Shield supposedly has solved that challenge, as discussed *supra* Part II.C. The fourth and fifth challenges refer to the issue discussed *supra*, in that the Directive is incapable of addressing the inconsistencies across the European Member States because currently each State imposes different regulatory schemes and provides greater protections than

---

[68] *See generally Regulations, Directives and other Acts*, EUR. UNION (Dec. 16, 2016), http://europa.eu/european-union/eu-law/legal-acts_en.

[69] *Id.*

[70] *See generally Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, at 7, COM (2010) 609 final (Nov. 4, 2010) [hereinafter *A Comprehensive Approach on Personal Data Protection*].

[71] *Id.* at 3–4.

[72] *Id.* at 6, 8–9.

[73] *Id.* at 10–13.

others in some areas, as well as fewer in others.[74]

The text of the new articles in the GDPR grants users, *inter alia*, new rights and creates the European Data Protection Board. Article 7 provides conditions for consent;[75] article 15 creates a right of access for the data subject;[76] article 16 produces a right to rectification;[77] article 17 forms the bread and butter of the right to be forgotten and to erasure;[78] article 20 informs the right to data portability;[79] article 21 discusses the right to object to the processing of one's personal data for direct marketing;[80] article 22 explains profiling and the new measures put into effect;[81] article 68 sets up the European Data Protection Board;[82] and article 70 describes the tasks of the newly-formed Board.[83]

---

[74] *Id.* at 17–18.

[75] If a data subject—"an identified or identifiable natural person"—needs to give consent, the requirement must be clear. GDPR Provisions, *supra* note 15, at arts. 4(1), 7. A subject has the right to withdraw consent at any time. *Id.* art. 7(3).

[76] The article provides data subject's right of access to personal data, supplementing the need to inform data subjects of a storage period and of rights to rectification and to erasure and to lodge a complaint. *Id.* art. 15.

[77] "The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement." *Id.* art. 16.

[78] "Where the controller has made the personal data public and is obliged pursuant to [of article 17(1)] to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data." *Id.* art. 17(2).

[79] "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent . . . or on a contract . . . ; and (b) the processing is carried out by automated means." *Id.* art. 20(1).

[80] *Id.* art. 21.

[81] A data user has the right not to be subject to a measure producing a quasi-discriminatory effect, "based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." GDPR Provisions, *supra* note 15, art. 22(1). The article goes on to list exceptions to the subjection of the measure. *Id.* art. 22(2).

[82] "The European Data Protection Board . . . is hereby established as a body of the Union and shall have legal personality." *Id.* art. 68.

[83] The Board hereby has duties to advise the Commission; examine Members; review the application of the guidelines; make recommendations and best practices; issue opinions; promote cooperation; promote common training programs; and promote exchange of knowledge. *Id.* art. 70.

B. *Alignment with Europe 2020 Strategy*

Europe 2020 was a strategy proposed by the European Commission on March 3, 2010, to advance the EU's economy.[84] Specifically, the Commission sought to create "smart, sustainable, inclusive growth"[85] and increased coordination of national and European policy. The Commission proposed five measurable targets to complete by the year 2020, which are: (1) employment; (2) research and innovation; (3) climate change and energy; (4) education; and (5) combating poverty.[86] The Commission proposed a priority theme called "a digital agenda for Europe," under which Member States would "speed up the roll-out of high-speed internet and reap the benefits of a digital single market for households and firms."[87]

Under "A Digital Agenda for Europe," the proposal lists elements that the Commission will work on—at the EU level—to produce sustainable economic and social benefits from what it calls a "Digital Single Market."[88] One of the elements has the following broad-based aim:

> To create a true single market for online content and services (i.e. borderless and safe EU web services and digital content markets, with high levels of trust and confidence, a *balanced regulatory framework with clear rights regimes*, the fostering of multi-territorial licences, *adequate protection and remuneration for rights holders* and active support for the digitisation of Europe's rich cultural heritage, and to shape the global governance of the internet . . . .[89]

In the Communication on Digital Agenda for Europe, the European Commission stresses the need to create a "vibrant digital single market,"[90] because the detachment of policies among the

---

[84] *Europe 2020: A strategy for smart, sustainable and inclusive growth*, COM (2010) 2020 (Mar. 3, 2010) [hereinafter *Europe 2020*]. For a brief and pictorial explanation of ordinary legislative procedure in the European Parliament, see *Legislative Powers: Ordinary legislative procedure*, EUR. UNION (Mar. 5, 2016), http://www.europarl.europa.eu/aboutparliament/en/20150201PVL00004/Legislative-powers.

[85] *Europe 2020*, *supra* note 84, at 3. Smart growth is "developing an economy based on knowledge and innovation"; sustainable growth is "promoting a more resource efficient, greener, and more competitive economy;" inclusive growth is "fostering a high-employment economy delivering social and territorial cohesion." *Id.*

[86] *Id.*

[87] *Id.* at 4.

[88] *Id.* at 11–12. *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe*, COM (2010) 245 final/2 (Aug. 26, 2010) [hereinafter *A Digital Agenda for Europe*].

[89] *Europe 2020*, *supra* note 84, at 12 (emphasis added).

[90] *A Digital Agenda for Europe*, *supra* note 88, at 7.

Member States stifles competitiveness in the digital economy worldwide. The Commission must recognize that some of the most successful Internet businesses are based out of the United States; as a result, there is inconsistent implementation of rules across Member States. This inconsistency calls for transparency in defining the scope of data users' rights and legal protection when doing business online.

A regulation, as opposed to the current Directive, would be a huge step towards increasing coordination of national and European policy. This way, certain Member States that might otherwise not be predisposed to a safer security framework would need to work harder to achieve the standards that other Member States have worked more intensively to attain because of the initial Directive. A regulation would place all Member States on equal footing, as opposed to the drastic variations the Member States have upheld thus far, leading to a disjunctive result. If the European Union intends to impose stricter guidelines on foreign companies, it certainly must be a model for its new policies worldwide. On December 15, 2015, negotiations between the EU Commission, Parliament, and Council concluded, resulting in the GDPR.[91]

C. *Strengths and Weaknesses in the GDPR*[92]

Before the text of the GDPR became public information in December 2015, LobbyPlag released a current version of the GDPR proposal, so users could scroll through the document and see what text the Commission proposed and the Council removed, what sections the Council inserted, and the commentary from LobbyPlag as to what would likely be a stronger or weaker law than its predecessor.[93] In this subsection, the focus will be on identifying the strengths and weaknesses in the GDPR, but limited to the scope of the articles of interest, specifically articles 6, 7, 9, 11, 15, 17, 20, 21, 22, 25, and 83.

1. Article 83 – Administrative Fines

Businesses would certainly agree that the most disquieting change to the GDPR is article 83, which provides conditions for imposing

[91] *Reform of EU data protection rules*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/reform/index_en.htm (last visited Jan. 31, 2017).

[92] Strengths and weaknesses are evaluated based on the enforceability of the separate provisions.

[93] *Regulation Proposal*, LOBBYPLAG (Jan. 15, 2016, 15:12), http://www.lobbyplag.eu/governments/gdpr [hereinafter *Regulation Proposal*]. The official text of the GDPR can be found at *supra* note 15.

administrative fines.[94] Given the difference between directives and regulations, the Directive did not have the power to institute a "one size fits all" regimen for liability; the European Commission handed that discretion off to the Member States and their supervisory authorities.[95] The GDPR continues the tradition of the supervisory authorities under article 51, but for the first time provides two definitive levels of administrative fines under article 83.[96] Now, fines could range from 10,000,000 and two percent of the company's total annual turnover, or anywhere from 20,000,000 to four percent of the company's annual turnover, whichever is higher in either case.[97] To put these numbers into perspective, consider Google's revenue, which was $74.5 billion in 2015.[98] A range from two percent of its turnover to four percent would be from $1.49 billion (1.43 billion) to $2.98 billion (2.85 billion). Money talks: the new enforcement mechanism certainly discourages indifference and encourages compliance.

2. Article 7 – Conditions for Consent

When a data subject provides explicit consent under article 9(2)(a), article 7(2) requires that consent be given as a written declaration that is "clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."[99] Consent may be withdrawn at any time, but any

[94] GDPR Provisions, *supra* note 15, at art. 83.

[95] Data Protection Directive, s*upra* note 3, at art. 23 ("Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered."); *id.* art. 24 ("The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.").

[96] GDPR Provisions, *supra* note 15, at art. 51(1) ("The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive."); *id.* art. 83.

[97] *Id.* arts. 83(4), 83(5). For a concise breakdown of the levels of administrative fines and infringement of which articles would affect which level, see Nuria Pastor & Georgina Lawrence, *Getting to know the GDPR, Part 10 – Enforcement under the GDPR – what happens if you get it wrong?*, FIELD FISHER (Mar. 5, 2016, 15:19), http://privacylaw blog.fieldfisher.com/2016/getting-to-know-the-gdpr-part-10-enforcement-under-the-gdpr-what-happens-if-you-get-it-wrong/.

[98] Google, Inc., Annual Report (Form 10-K) (Dec. 31, 2015), at 23, https://www.sec.gov/Archives/edgar/data/1288776/000165204416000012/goog10-k2015.htm ("Google segment revenues of $74.5 billion with revenue growth of 14% and Other Bets revenues of $0.4 billion.").

[99] GDPR Provisions, *supra* note 15, at art. 7(2).

processing of information based on the consent already granted could be lawfully processed; before giving consent, the data subject would be made aware of these circumstances and the controller has a duty to inform about the right to withdraw consent.[100] These two subsections evidence a substantially strict rule for consent through terms or privacy policies, one that is not akin to what American companies are used to, with their opt-out mechanisms.[101]

3. Articles 9 & 16 – Processing of Special Categories of Personal Data, and Right to Rectification

Article 9 shapes the processing of special categories of personal data. Personal data, particularly that revealing race or ethnicity, political affiliation, religion or beliefs, or genetic, health or sex life, is prohibited.[102] A significant change from the Directive is that personal data now includes genetic and biometric data.[103] A substantial strength of the article also consists in its limitation of third-country transfers of "health data," because it requires that data be managed by a medical professional who is answerable to a duty of professional secrecy, whether it is through a third State or a national body.[104] Article 16 delineates the right to rectification, which provides a data subject with

[100] *Id.* art. 7(3) ("The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.").

[101] *Compare* CAN-SPAM Rule, 16 C.F.R. § 316, § 316.5 (2012) ("Prohibition on charging a fee or imposing other requirements on recipients who wish to opt out."), *with* Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), art. 13(3), 2002 O.J. (L 201) ("Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.").

[102] GDPR Provisions, *supra* note 15, at art. 2(a) ("Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.").

[103] *Id. But see* Data Protection Directive, *supra* note 3 ("'[P]ersonal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); 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.").

[104] GDPR Provisions, *supra* note 15, at art. 9(3) ("Personal data . . . may be processed . . . by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.").

the right to rectify any inaccuracies in personal data that concerns him; an attractive feature of the right is that the requesting data subject has the right to receive it "without undue delay."[105] A data subject may also request the completion of incomplete personal data.[106]

4. Articles 6 & 21 – Lawfulness of Processing, and Right to Object

The right to object is located under article 21. The GDPR allows a data subject to protest the processing of data for any of the reasons under article 6(1)(e) or 6(1)(f)—these provisions govern processing carried out in the public interest or processing necessary for the legitimate purposes of the controller or a third party—unless that right is overridden by the "controller demonstrat[ing] compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims."[107] The data subject could also object to his personal data being processed for direct marketing purposes—including profiling to the extent it relates to said marketing—and it does not appear that the controller has an opportunity to rebut the request.[108] From the drafting of the provision, it appears that the right to object applies when data is still in the processing stage, and is not yet collected, or better yet, stored. While it might be a worthwhile endeavor to offer a right to object, it is perplexing to identify what kind of personal data could qualify as being processed for a public interest or is necessary for the legitimate purposes of the controller or a third party.[109]

5. Article 22 – Automated Individual Decision-Making, Including Profiling

The right not to be subject to "automated individual decisions-making," better understood as profiling, is under article 22.[110] Besides

[105] *Id.* art. 16 ("The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.").

[106] *Id.* ("[T]he data subject shall have the right to have incomplete personal data completed . . . .").

[107] *Id.* art. 21(1).

[108] *Id.* art. 21(2)–(3).

[109] It must be that a legitimate purpose would include processing for a "legitimate business purpose" of the controller, such as payment. Yet, if the personal data concerns the subject who requested it not be processed in the first place, wouldn't that legitimate purpose no longer be valid?

[110] *See supra* note 81.

the right to be forgotten and the right to object, this right will also have a substantial effect on a company like LinkedIn.[111] The only situations in which the right would not apply are when the automated decision is essential in carrying out a contract between the subject and controller, the decision is authorized by a law to which the controller is held, or the decision is made possible by the subject's explicit consent.[112] In general, this right is to the benefit of the data subject since it prohibits the unreasonable invasion into an individual's personal preferences and characteristics; however, a data subject might be caught in a dilemma if it is found his consent was conditional under article 7 upon "the performance of a contract, including the provision of a service."[113]

The draft first written by the Commission for article 7(1) stated that the controller would bear the burden of proof for the data subject's consent.[114] The Council's revision now stands as requiring the controller to "be able to demonstrate that the data subject has consented to processing of his or her personal data" in the context of article 6(1)(a).[115] The Council removed the last provision under article 7, which nullified the legality of any consent provided by the data subject in the case of a noteworthy imbalance in bargaining power between the two parties.[116] In essence, any ambiguity in the delivery of consent would be resolved in favor of the controller. In addition, there is no consideration of the imbalance between parties—likely because there would often be a vast differential between the two parties—unless the data subject is a large business.

6. Article 11 – Processing Which does not Require Identification

Article 11 concerns circumstances in which processing the data does not, or does no longer, require personal information. In such a case, the controller does not need to receive further information or

---

[111] The extent of the right not to be subject to profiling and its practical application is discussed *infra* notes 200–03 and accompanying text.

[112] GDPR Provisions, *supra* note 15, at art. 22(2)(a)–(c).

[113] *Id.* art. 7(4).

[114] *Regulation Proposal*, *supra* note 93, at art. 7(1). See *supra* note 15 for the definition of a "controller."

[115] GDPR Provisions, *supra* note 15, at art. 7(1). Article 6(1)(a) states that "[p]rocessing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes . . . ."

[116] *See Regulation Proposal*, *supra* note 93, at art. 7(4) ("Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.").

engage in more processing.[117] This is a strength since the provision does not require controllers to maintain or process more information than necessary simply to be able to comply with the GDPR;[118] this way, it takes the burden off the controller as soon as the controller no longer possesses personal data, for whatever reason.

7. Article 17 – Right to Erasure ("Right to be Forgotten")

The right to erasure, also known as the right to be forgotten, is embodied in article 17.[119] The description of the right is as follows: "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data where one of the following grounds applies . . . ."[120] The right may be exercised when the data is no longer necessary for its initial purpose,[121] the data subject withdraws his consent under article 6(1) or article 9(2),[122] the subject objects to the processing of personal data under article 21(1),[123] the data has been unlawfully processed,[124] the data must be erased in order to comply with certain legal obligations,[125] or the data has been collected in reference to information services under article 8(1) (which this Comment does not cover).[126]

8. Articles 20 & 25 – Rights to Data Portability & Privacy by Design

Besides the right to be forgotten, discussed *infra* Part III.D, the rights to data portability and privacy by design are likely to have an extensive impact on a global expectation of privacy. These rights can be thought of as original in the sense that they sound very attractive to data subjects aching to maintain greater control over their personal information. On the flip side, they could prove to be immensely expensive to companies that are not capable of handling hundreds of

[117] GDPR Provisions, *supra* note 15, at art. 11(1) ("If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.").

[118] *Id.*

[119] *Id.* art. 17.

[120] *Id.* art. 17(1). See *supra* note 15, for the definition of "controller."

[121] *Id.* art. 17(1)(a).

[122] *Id.* art. 17(1)(b).

[123] GDPR Provisions, *supra* note 15, at art. 17(1)(c).

[124] *Id.* art. 17(1)(d).

[125] *Id.* art. 17(1)(e).

[126] *Id.* art. 17(1)(f).

requests daily to receive, remove, or reorganize personal data.

The right to data portability is encapsulated under article 20 and offers data subjects the right to require data to be provided in a commonly-used electronic form.[127] Read into the context of article 15—right of access by the data subject—the right to data portability and the right of access to let a data subject acquire a full copy of personal data concerning him or her, and: (a) the purposes for the processing; (b) the categories of personal data involved; (c) recipients or categories thereof to whom the personal data has been disclosed or will be disclosed; (d) the period of time for which the personal data will be stored; (e) the right to request rectification or erasure of personal data; (f) the right to file a complaint with a supervisory authority; (g) if personal data is not collected from the data subject, available information as to where it could be found; and (h) whether automated decision-making exists.[128] One of the few limitations to the rights of portability and access is that the right to obtain a copy of personal data being processed may not "adversely affect the rights and freedoms of others," nor could the right to data portability as a whole adversely affect the rights of others.[129] In reality, the likelihood that the request for a data subject's personal data could affect the rights of others is potentially very low: unless the nature of the data about the requesting subject is inextricably linked to another individual who would take issue with its release, likely the controller would need to comply with the data subject's request for data portability and access.

Under the Europe 2020 proposal, what lies critical to the social benefits of the "Digital Single Market" are the fundamental rights of every individual user which must be enforced using the widest range of means: application of the principle of "privacy by design"[130] and exercise of inhibitive sanctions when necessary. Colloquially termed "privacy by design," under article 25, this right is called "data protection by design and by default" and is the idea that privacy and data protection are, in some way, embedded within the entire life cycle of hard- and soft-ware, from early design, to use, to disposal.[131]

---

[127] *Id.* art. 20(1)(a)–(b) ("The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where (a) the processing is based on consent . . . and (b) the processing is carried out by automated means.").

[128] *Id.* art. 15(1)(a)–(h).

[129] GDPR Provisions, *supra* note 15, at arts. 15(4), 20(4).

[130] *A Comprehensive Approach on Personal Data Protection*, *supra* note 70, at 12.

[131] *See generally* Charith Perera et al., *Privacy-by-Design Framework for Assessing Internet*

Essentially, a controller would ensure that it is limiting the amount of data it uses to only a minimum amount of personal data; that way, "by default, only personal data which are necessary for each specific purpose of the processing are processed."[132] The only problem with privacy by design is: how could it be enforced? There are too many variables a regulatory authority would consider before slapping a company with a fine claiming it did not comply with article 25.[133] It appears that privacy by design is merely a utopian declaration that from this point forward, all companies should adhere to the ideal of minimizing the amount of personal data that is required by nature of their information processing.

These sanctions seem evocative of the procedures the European Court of Justice discusses in *Google Spain*, *infra* Part III.D., proposed with regard to the "right to be forgotten." "Privacy by design" suggests an early acknowledgment that it is within an individual's fundamental rights to be able to securely dispose of his data and that it is the responsibility of the company which processes data to ensure its infrastructure is designed with privacy in mind.[134]

D. *Evolution of the Right to be Forgotten*

Although the right to be forgotten was not included in the Data Protection Directive, the idea was almost implicit in the document under article 12.[135] Even though the GDPR conflates the two terms under article 17, which is titled "Right to erasure ('right to be forgotten')," there are debates as to whether the right to be forgotten and the right to erasure represent the same idea. According to one author, the right to erasure and the right to be forgotten are interchangeable terms.[136] Another author argues that the two do not

of Things Applications and Platforms, CORNELL UNIV. LIBR. 4 (2016), https://arxiv.org/pdf/1609.04060.pdf.

[132] GDPR Provisions, *supra* note 15, at art. 25(2).

[133] *Id.* art. 25(1) ("Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing . . . .").

[134] A ready list of which companies have embraced the philosophy is not yet available, and might never be. Therein lies one of the difficulties in applying this framework: it would be near impossible to quantify who did or did not adopt the scheme.

[135] *See* Commission proposes a comprehensive reform of data protection rules, *supra* note 14.

[136] Cooper Mitchell-Rekrut, Note, *Search Engine Liability Under the Libe Data Regulation Proposal: Interpreting Third Party Responsibilities as Informed by Google Spain*, 45 GEO. J. INT'L L. 861, Abstract (2014) ("The 'right to be forgotten'—now branded as the 'right to erasure'—has been publicized as one of the 'four pillars' of the EU's

represent the same idea, as the right to be forgotten includes data "that does not breach any norm."[137] Such a norm could be any general provision of the Directive or Regulation. The right to erasure "allows data subjects to request the elimination of their personal data when its retention or processing violates the terms of the directive, in particular (but not exclusively) because of being incomplete or inaccurate."[138] On the other hand, enforcing the right to be forgotten would cause deletion of personal information regardless of whether the information proved harmful or was illegally processed.[139]

1. Google Spain Case

The first time the European Court of Justice (ECJ) heard a case involving the right to be forgotten was in *Google Spain SL v. Gonzalez*.[140] Mario Costeja Gonzalez, a Spanish national, filed a complaint with the Spanish Data Protection Agency against La Vanguardia Ediciones SL—the publisher of a daily newspaper—and against Google Spain and Google, Inc.[141] Gonzalez claimed that when any user entered Gonzalez's name into a Google search engine, the results would link to two pages of La Vanguardia's newspaper, January 1998 and March 1998, respectively.[142] Those pages did not speak well of Gonzalez because they announced a real estate auction effected for the recovery of social security debts owed by Gonzalez.[143] First, Gonzalez requested that La Vanguardia either remove or alter the pages—so that the material would no longer be widely available—or use search engines to protect the data; second, Gonzalez requested that Google Spain or Google, Inc. remove or suppress the data so that it no longer linked to La Vanguardia.[144] Gonzalez supported his assertions by referencing the fact that the attachment proceedings had been resolved and thus that retaining the data was irrelevant.[145]

The court held that by searching for information published on the Internet, the data user "collects" data within the meaning of the

proposed General Data Protection Regulation.").

[137] Ignacio Cofone, Google v. Spain*: A Right To Be Forgotten?*, 15 CHI.-KENT J. INT'L & COMP. L. 1, 8 (2015).

[138] *Id.* at 6.

[139] *Id.* at 8.

[140] *See* Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, [2014] E.C.R. I-317, EU:C:2014:317.

[141] *Id.* ¶¶ 2, 14.

[142] *Id.* ¶ 14.

[143] *Id.*

[144] *Id.* ¶ 15.

[145] *Id.*

Directive.[146] The data user is the "controller" in respect of the processing of the search engine.[147] The operator of the search engine is—in certain circumstances—responsible for removing links to web pages that are published by third parties which contain information relating to a person from the list of results displayed.[148] Such an obligation may also exist when the name or information is not erased from those pages and even when initial publication was lawful.

A fair balance should be struck between the interest of potential future users in the data sought and the data subject's fundamental rights. Courts must consider: (1) the nature of the information; (2) the sensitivity for the data subject's private life; and (3) the interest of the public in having that information.[149]

The ECJ recognized a right to be forgotten under the Data Protection Directive.[150] The court found that a citizen may require a provider like Google to remove his or her name from searches if the personal data has become inadequate, irrelevant, and excessive in relation to the purpose for which it was originally processed due to the lapse of time.[151]

2. Schrems Case

The second pivotal case the ECJ heard implicating—though never directly referring to—the right to be forgotten was in 2015, in *Maximilian Schrems v. Data Protection Commissioner*.[152] Maximilian Schrems filed a class-action-type civil suit in Ireland against the Data Protection Commission, alleging that Facebook Ireland violated data use policy, did not provide effective consent to many types of data use, supported the NSA's PRISM surveillance program,[153] tracked Internet

[146] *Google Spain SL*, [2014] E.C.R. I-317, ¶ 28.

[147] *Id.* ¶ 21.

[148] *Id.* ¶ 62.

[149] *Id.* ¶ 81.

[150] Data Protection Directive, *supra* note 3, at art. 12.

[151] Patrick Van Eecke & Jim Halpert, *The 'Right to be Forgotten' in Today's Information Age*, 32 WESTLAW J. 1, 3 (Nov. 20, 2014), https://www.dlapiper.com/~/media/Files/Insights/Publications/2014/12/The_right_to_be_forgotten_in_todays_info_age.pdf.

[152] Maximilian Schrems v. Data Protection Commissioner, Case C-362/14, EU:C:2015:650.

[153] The PRISM surveillance program—the existence of which was leaked by Edward Snowden—is an American surveillance program that was started in 2007 whose purpose is to monitor the communications of users on nine popular Internet services: Microsoft, Apple, Google, Facebook, Skype, AOL, PalTalk, Yahoo, and YouTube. It was tacitly confirmed by the Obama Administration, but technology companies have denied their participation. Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, WASH. POST (June 12, 2013), https://www.washingtonpost.com/

users on external websites, monitored and analyzed users through "big data" systems, unlawfully introduced "graph search," and passed user data to external applications without authorization of the data user.[154] Procedurally, the following occurred: the Safe Harbor was sent to the European Court of Justice;[155] and the case was tried in 2015 in the European Court of Justice, but the opinion by Advocate General Bot was delayed,[156] likely because of talks behind closed doors between the US and the EU. Following the postponement, the plaintiff applied to have the case considered in the first instance in the Vienna Regional Court (Landesgericht), but the court found that a "class action" is not admissible on procedural grounds.[157] The case was appealed to the Higher Regional Court (Oberlandesgericht).[158] The Oberlandesgericht was to decide whether class actions are lawful; as the matter stands, the case has been referred to the European Court of Justice, once more.[159] The reason the case was referred so quickly to the ECJ in the first place was because, as Mr. Schrems called it, the courts were "playing hot potato," either being unwilling to answer the difficult questions posed, or simply at wits' end.[160] If nothing else, Mr. Schrems joked that he would like to be the litigant who had appeared most often in front of the ECJ.[161]

On September 24, 2015, Advocate General Yves Bot released his opinion, in which he ruled that: the Safe Harbor was invalid; the Irish Data Planning Commissioner could not rely on the Safe Harbor; American companies which have active "safe harbor" certification would need to find another basis to transfer data from the US to the EU, such as "Binding Corporate Rules" included in the data protection directive; and Facebook did not participate in mass surveillance in the United States, nor was EU data made available to American authorities.[162]

news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

[154] *Class Action Against Facebook Ireland*, EUR. VERSUS FACEBOOK (Dec. 1, 2015), http://europe-v-facebook.org/EN/Complaints/Class_Action/class_action.html.

[155] *News*, EUR. VERSUS FACEBOOK (Mar. 25, 2015), http://europe-v-facebook.org/EN/en.html.

[156] *Id.* (June 9, 2015).

[157] *Id.* (Oct. 21, 2015).

[158] *Id.* (Nov. 23, 2015).

[159] *Id.* (Sept. 12, 2016). It stands to reason that what the European Court of Justice decides pertaining to class actions could be a separate topic ripe for discussion.

[160] Maximilian Schrems, Initiator of Europe v. Facebook, Address at the CUNY Graduate Center: The US v. Europe v. Facebook: Digital Divisions? (Feb. 22, 2016) [hereinafter Schrems Lecture].

[161] *Id.*

[162] *See CJEU: First Reaction to AG's Opinion on NSA "PRISM" Scandal Facebook's EU-US*

On October 6, 2015, the CJEU found that: transfers of personal data between third countries should not be given lower levels of protection than transfers within the European Union;[163] Decision 2000/520[164]—which implemented the safe harbor privacy principles—does not contain sufficient guarantees;[165] and finally that Facebook did not breach the safe harbor principles,[166] but that its interference with the fundamental rights of EU citizens was contrary to provisions of the Charter because it did not pursue an "objective of general interest defined with sufficient precision."[167] In late October 2015, the Higher Regional Court issued a decision in favor of the plaintiff, ruling that the plaintiff is not a "professional litigant," so he is entitled to bring his claims in his home court, but the status of the class action remains in dispute so the regional court referred it to the Austrian Supreme Court.[168]

There are some practical difficulties in implementing the findings of this decision. The right to be forgotten allows an individual to control his personal data if it is no longer necessary for its original purpose, or if for some other reason, he wishes to withdraw consent as to its processing, among other reasons.[169] As a result, there would be higher protection for individuals and the right could ensure a more effective regulatory scheme. In reality, however, is it possible to ask a company to delete information that was posted by an individual, in light of the fact that it might have been widely distributed already? When Mr. Schrems engaged in his "war" against Facebook, he requested all of the documents that the company possessed about him: what he received was a log of every single bit of information that even mentioned his name, whether it was still on the website or supposedly deleted a long time ago, in a huge stack of papers.[170] This occurrence symbolizes the fact that although the GDPR might convince companies to remove information from their websites that consumers request be

Data Transfers Under "Safe Harbor" Not Legal, EUR. VERSUS FACEBOOK (Sept. 23, 2015), http://www.europe-v-facebook.org/GA_en.pdf.

[163] *Maximilian Schrems*, EU:C:2015:650, ¶ 144.

[164] *See* Commission Decision 2000/520, 2000 O.J. (L 215) 7 (EC).

[165] *Maximilian Schrems*, EU:C:2015:650, ¶ 159.

[166] *Id.* ¶ 168.

[167] *Id.* ¶ 181.

[168] *Media Update for 21/10/2015*, EUR. VERSUS FACEBOOK (Oct. 21, 2015), http://www.europe-v-facebook.org/PA_OLG_en.pdf.

[169] GDPR Provisions, *supra* note 15, at art. 17. *See Guide to the General Data Protection Regulation*, BIRD & BIRD 31 (Jan. 2017), https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird—bird—guide-to-the-general-data-protection-regulation.pdf?la=en.

[170] Schrems Lecture, *supra* note 160.

taken down, it might never truly disappear.[171] In the struggle to immortalize the privacy right and render it tangible, privacy advocates have taken a picture of this stack of papers to the extent that Schrems joked about it and said, "It's probably the most filmed stack of papers, ever!"[172] This massive interest in Schrems' stack of papers is the European and American attempt at rendering palpable this elusive privacy right. In reality, it is unclear what actual privacy the right to be forgotten provides.

IV. LINKEDIN AND HOW IT WILL BE AFFECTED

A. *The Unique Nature of LinkedIn*

LinkedIn was officially launched on May 5, 2003.[173] The company's mission is to "connect the world's professionals to make them more productive and successful."[174] From its mission statement, LinkedIn expects to be able to extend its social network to people and businesses worldwide, which would certainly include Europe and the European Union Members.

LinkedIn is unique from other popular social networks because its primary mission is to connect professionals around the world.[175] From the onset, the nature of its enterprise indicates that it is likely the company's users would benefit from engaging in more secure practices: this view is a result of the perception that reputation is fundamental to any individual using the site. Unlike other social networks, certain entities—namely employers—seek a certain category of individuals—employees—and vice versa. Employees and employers

---

[171] Although outside of the scope of this Comment, "processors" which processed personal data on behalf of the controllers, could still maintain copies of that removed data, as there appears to be little to no regulation of the activities of processors in the GDPR.

[172] *Id.*

[173] *About Us*, LINKEDIN, https://www.linkedin.com/about-us?trk=uno-reg-guest-home-about (last visited Mar. 23, 2016).

[174] *Id.*

[175] The most popular social networks that resemble LinkedIn include Facebook, Twitter, Google Plus+, and VK. Facebook's mission statement is "to give people the power to share and make the world more open and connected." *About*, FACEBOOK, https://www.facebook.com/facebook/info?tab=page_info (last visited Mar. 23, 2016). Twitter's mission is "[t]o give everyone the power to create and share ideas and information instantly, without barriers." *About*, TWITTER, https://about.twitter.com/company?lang=en (last visited Mar. 23, 2016). Google+ is "a place to connect with friends and family, and explore all of your interests." *About*, GOOGLE+, https://plus.google.com (last visited Mar. 23, 2016). "VK is a social network that unites people all over the world and helps them communicate comfortably and promptly." *About VK*, VK, http://www.vk.com/about (last visited Mar. 23, 2016).

would likely not seek out like categories of individuals, unless the intention was to engage in a forum.

B. *Current Policies in Place*

Through its exclusive applications, LinkedIn engages in marketing and sales to optimize business solutions to employers. LinkedIn collects information from the devices and networks used to access the site. It has access to: (1) cookies;[176] (2) IP addresses;[177] (3) URLs from whence users arrived at the page; (4) URLs to which the users go; (5) OS details;[178] (6) types of Internet browsers; (7) mobile IDs; and (8) location data.[179] Taking into account the rather large amount of personal identifying information to which the company has access, it is necessary to taper its effects with some safeguards for users. As a result, LinkedIn allows individual users a great deal of control over the content they post on the site. Under its "User Agreement,"[180]

[176] There is an entire Cookie Policy dedicated to describing detailed information about how the website uses cookies. *Cookies on the LinkedIn site*, LINKEDIN, https://www.linkedin.com/legal/cookie-policy?trk=hb_ft_cookie (last visited Mar. 23, 2016).

[177] An IP address is a number which uniquely identifies a computer and any other electronic device on a computer network protocol, called TCP/IP. Bradley Mitchell, *What is an IP Address?*, LIFEWIRE (Oct. 29, 2016), https://www.lifewire.com/what-is-an-ip-address-818393.

[178] OS stands for "operating system," which is a program that controls and manages the hardware and software on a computer. Tim Fisher, *Definition of an Operating System*, LIFEWIRE (Oct. 20, 2016), https://www.lifewire.com/operating-systems-2652912.

[179] *Privacy Policy*, LINKEDIN § 1.10, https://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv (last visited Apr. 4, 2017).

[180] The Rights and Limits to the "User Agreement" provide as follows:

> As between you and LinkedIn, *you own the content and information that you submit or post* to the Services and you are only granting LinkedIn the following non-exclusive license: A worldwide, transferable and sublicensable right to use, copy, modify, distribute, publish, and process, information and content that you provide through our Services, without any further consent, notice and/or compensation to you or others. These rights are limited in the following ways:
>
> a. You can end this license for specific content by *deleting such content from the Services*, or generally by *closing your account*, except (a) to the extent you shared it with others as part of the Service and they copied or stored it and (b) for the reasonable time it takes to remove from backup and other systems.
> b. We will not include your content in advertisements for the products and services of others (including sponsored content) to others *without your separate consent*. However, we have the right, without compensation to you or others, to serve ads near your content and information, and your comments on sponsored content may be visible as noted in the Privacy Policy.

LinkedIn provides a user's "Rights and Limits" to include: (1) the ability to end LinkedIn's broad license to the user's content by deleting his content from the website or closing his account; (2) the requirement of user's consent before information is used in ads for products and services of others; (3) the requirement of user's consent before others may publish posts; and (4) the right not to have LinkedIn modify "the meaning of [the user's] expression." LinkedIn has already included in its User Agreement a rather liberal policy with a few safeguards to user's privacy and freedom to take down certain kinds of information.

C. *Which Provisions of the General Data Protection Regulation (GDPR) Would Apply*

Under article 23 of the Preamble, the GDPR aims to cover activities of outside controllers when such outside controllers' processing activities are related to the offering of goods or services, or to the monitoring of the behavior of such data subjects.[181] The question is whether LinkedIn provides goods or services. Neither term is defined under article 4,[182] nor under the Data Protection Directive. A definition of the terms might be presumed from the Treaty on the Functioning of the European Union (TFEU), a quasi-constitutional document.[183] Under the Treaty of Lisbon—which in 2009 amended

> c. *We will get your consent if we want to give others the right to publish your posts beyond the Service.* However, other Members and/or Visitors may access and share your content and information, consistent with your settings and degree of connection with them.
> d. While we may edit and make formatting changes to your content (such as translating it, modifying the size, layout or file type or removing metadata), *we will not modify the meaning of your expression.*
> e. Because you own your content and information and we only have non-exclusive rights to it, *you may choose to make it available to others*, including under the terms of a Creative Commons license.

User Agreement, LINKEDIN § 3.1, https://www.linkedin.com/legal/user-agreement?trk=hb_ft_userag (last visited Dec. 21, 2016) (emphasis added).

[181] GDPR Provisions, *supra* note 15, at pbl. (23) ("In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the *processing activities are related to offering goods or services* to such data subjects irrespective of whether connected to a payment.") (emphasis added).

[182] The definitions in the article are limited to various aspects of data and some definitions of a business nature, among other independent terms.

[183] *See* Consolidated Version of the Treaty on the Functioning of the European Union, 2012 O.J. C 326/47 [hereinafter TFEU].

the TFEU and the Treaty of Rome—Title II, article 28, "goods" include "products originating in Member States and . . . products coming from third countries which are in free circulation in Member States."[184] "Free circulation" implies that: (1) import formalities have been conformed to; (2) customs duties or charges have been levied; and (3) the provider did not endure a total or partial drawback of the duties or charges.[185] On the converse, "services" include: (a) activities of an industrial character; (b) activities of a commercial character; (c) activities of craftsmen; and (d) activities of the professions.[186]

Under the definitions of goods and services in the TFEU, it would likely not be true that LinkedIn satisfies the requirement of offering any goods to parties in the European Union; it would, however, fall under the offering of services. Under TFEU article 57(b)—activities of a commercial nature—and article 57(d)—activities of the professions—there is likely a strong argument that LinkedIn engages in activities of a commercial nature, since it engages in marketing, sales, and in activities of the professions.[187] LinkedIn offers the following marketing products: "Lead Accelerator," "Sponsored Updates," "Sponsored InMail," "Display Ads," and "Text Ads."[188] These marketing campaigns allow companies to employ various approaches to ensuring that target audiences—whether they are sales teams or prospective employees—are contacted in a way that best suits their needs and is especially likely to get their attention. LinkedIn offers companies the option of "social selling," through its application called "LinkedIn Sales Navigator."[189] Through the navigator, companies are driven to make the right connections and sell their goals and aspirations to people whom they would personally affect.[190]

---

[184] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, art. 28, 2007 O.J. C 306 [hereinafter Treaty of Lisbon].

[185] TFEU, *supra* note 183, at art. 29.

[186] *Id.* art. 57.

[187] There has been little case law regarding the definition of "activities of the professions." Most case law has focused on defining whether the term refers to a type of service, and has always been found to do so. *See* Hubbard, Case C-20/92, [1993] E.C.R. I-3777. Examples of "professions" have included individuals in the health profession, legal profession, and other regulated professions. *See, e.g.*, Khatzithanasis, Case C-151/07, [2008] E.C.R. I-9013; Commission v. Italy, Case 168/85, [1986] E.C.R. I-2945.

[188] *Market to who matters*, LINKEDIN, https://business.linkedin.com/marketing-solutions (last visited Mar. 4, 2017).

[189] *Sales Navigator*, LINKEDIN, https://business.linkedin.com/biz/sales-solutions/b2b-sales-navigator (last visited Mar. 23, 2016).

[190] *Id.*

There is an especially strong argument that LinkedIn would satisfy the services definition under its activities of the professions, since it provides a gateway for employees and employers to reach out across the platform and benefit from interacting with each other. Even if LinkedIn was to be free from the goods and services analysis, it would certainly fall under the realm of monitoring the behavior of its data subjects. It is already clear through the brief description of the sales and marketing in which LinkedIn engages that it would likely qualify as applying a "profile" to an individual. Again, the GDPR describes that the act of profiling targets decisions concerning the data subject for analyzing or predicting his personal preferences, behaviors, and attitudes.[191]

D. *Which Aspects of Business Would Change*

LinkedIn announced its Fourth Quarter results on February 4, 2016.[192] In a news release, the CEO, Jeff Weiner, exalted, "Q4 was a strong quarter for LinkedIn . . . . We enter 2016 with increased focus on core initiatives that will drive leverage across our portfolio of products."[193] LinkedIn's revenue increased by thirty-five percent in 2015 from $862 million to $2.991 billion.[194] LinkedIn started off 2016 in a good place; the question is: would the Privacy Shield now cost the company dearly? LinkedIn doesn't think so; in October 2016, LinkedIn released the following in response to user inquiries on its Help page:

> LinkedIn is in the process of evaluating the Privacy Shield and its benefits for our members and customers. In the meantime, we continue to rely on Standard Contractual Clauses as a legal mechanism for data transfers from the EU. . . . Notably, these Standard Contractual Clauses, adopted by the EU Commission have not been invalidated by the ECJ decision. . . . [T]hese clauses are contractual commitments between companies transferring personal data . . . binding them to protect the privacy and security of the data. . . . . We remain committed to ensuring that our members continue to be able to use our services to advance

[191] GDPR Provisions, *supra* note 15, at art. 4(4).

[192] *LinkedIn Corporation Trended Condensed Consolidated Balance Sheets*, LINKEDIN (Feb. 4, 2016), https://snap.licdn.com/microsites/content/dam/press/Download-Assets/Media%20Resources/Quarterly-Reports/Q4-2015-Consolidated-Metrics.pdf.

[193] LinkedIn Corporate Communications Team, *LinkedIn Announces Fourth Quarter and Full Year 2015 Results*, LINKEDIN (Feb. 4, 2016), https://press.linkedin.com/site-resources/news-releases/2016/linkedin-announces-fourth-quarter-and-full-year-2015-results.

[194] *Id.*

> their careers and pursue professional opportunities worldwide.[195]

The company intends to rely on the Standard Contractual Clauses, which were provided by the European Commission in 2010 in compliance with the Data Protection Directive.[196] The European Commission drafted these clauses as models for what businesses could include in their protection regimes with the knowledge that these clauses have already been deemed to provide adequate protection.[197] The retreat to the Standard Contractual Clauses is explained by reference to the publications of numerous law firms, which have advised their client companies that the clauses would be a means to legitimize international transfers of data.[198] However, it stands to reason if these clauses are not grandfathered into the GDPR, they would be reexamined in the future, as well.[199]

Assuming LinkedIn will need to find an alternative to the clauses, the company would no longer be capable of engaging in the extent of the profiling in which it currently engages; this "data minimization" would likely apply to every social network. The company would likely need to modify its Rights and Limits under the User Agreement. As it currently stands, it would not comply with the "right to be forgotten"

---

[195] *EU Data Transfers and the Safe Harbor*, LINKEDIN, https://www.linkedin.com/help/linkedin/answer/62533/eu-data-transfers-and-the-safe-harbor?lang=en (last visited Jan. 31, 2017).

[196] Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010 O.J. (L 39) 5.

[197] *Id.* art. 1.

[198] *See, e.g.*, *Will EU Standard Contractual Clauses be declared invalid as well?*, LINKLATERS, http://linklaters.de/aktuelles/themen/after-safe-harbor-will-eu-standard-contractual-clauses-be-invalid.html (last visited Dec. 20, 2016); Lothar Determann et al., *The EU-U.S. Privacy Shield Versus Other EU Data Transfer Compliance Options*, BLOOMBERG BNA (Sep. 12, 2016), https://www.bna.com/euus-privacy-shield-n57982076824/; *Privacy Shield is final: What it means for businesses*, DLA PIPER (July 21, 2016), https://www.dlapiper.com/en/us/insights/publications/2016/07/privacy-shield-is-final/; Richard Dickinson et al., *EU-US Privacy Shield Adopted: Where Do We Go From Here?*, ARNOLD & PORTER (July 18, 2016), http://www.arnoldporter.com/en/perspectives/publications/2016/07/eu-us-privacy-shield-adopted-where; *Top Ten – EU Data Transfers: Comparing the Proposed Privacy Shield to the Standard Contractual Clauses*, ASS'N OF CORP. COUNSEL (May 24, 2016), http://www.acc.com/legalresources/publications/topten/transferring-personal-data.cfm.

[199] *Accord Will EU Standard Contractual Clauses be declared invalid as well?*, *supra* note 198. For now, the Article 29 Working Party has confirmed that the Clauses are still valid. Cameron F. Kerry et al., *Article 29 Working Party Confirms that EU Standard Contractual Clauses and Binding Corporate Rules are Still Valid – for the Time-Being*, SIDLEY AUSTIN (Feb. 3, 2016), http://datamatters.sidley.com/article-29-working-party-confirms-that-eu-standard-contractual-clauses-and-binding-corporate-rules-are-still-valid-for-the-time-being/.

as it has been provided for in the GDPR and its likely future interpretation as a result of the case law. The agreement does, however, provide ample consent provisions. These provisions would likely need to be made more apparent to the future users. LinkedIn would likely need to implement a divulgence policy regarding their users' right of access to their personal data. Users would need to be informed of how long their information would be stored, their right to rectify any incomplete or false information about them, their right to request an erasure of any information pertaining to them, and their right to lodge a complaint if the request is not complied with.

However, LinkedIn might not need to disclose any more information than it already has about its profiling if it falls under one of the exceptions in the GDPR article 22(2)(a)–(c).[200] Subsection (a) of this article considers whether entering into a contract immediately initiates the processing, and if the subject's rights have been maintained through the disclosure of information; if so, then the profiling has been authorized.[201] Subsection (b) considers whether the processing was authorized by a Member State and lays down procedures by which the subject's interests are protected.[202] Subsection (c) considers whether the data subject gave consent under article 7 (*Conditions for consent*).[203]

In the same vein, given the extent of the influence that LinkedIn exerts and its consistent growth, it is very likely that the implementation of the Privacy Shield and the GDPR will have a negligible effect on LinkedIn's ability to do business. LinkedIn has built-in mechanisms that can address changes in regulations, underscored by its news release that references changing regulations and the constant need to adapt to existing technology. Since its inception in 2003, LinkedIn has experienced little to no technologies that have so rigorously threatened LinkedIn's business model as to put it out of business. In thirteen years, LinkedIn has built a sustainable model, which will certainly adapt to changing rules and regulations. The same, however, cannot be said for companies that want to make their first step into the European market: with these new rigorous

[200] GDPR Provisions, *supra* note 15, at art. 22(2)(a)–(c) ("Paragraph 1 shall not apply if the decision [including profiling]: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject . . .; or (c) is based on the data subject's explicit consent."). *See also supra* note 110 and accompanying text.

[201] *See id.* art. 22(2)(a).

[202] *See id.* art. 22(2)(b).

[203] *See id.* art. 22(2)(c).

requirements—enforceable or not—new businesses might find themselves dissuaded from the European market until they make enough revenue to instill greater data protection. On the other hand, new companies might want to take their chances with provisions such as privacy by design, which do not have any teeth to them.

V. NEW ADVANCES IN TECHNOLOGY AND THEIR EFFECTS ON THE GDPR

A. *Google Glass Version 2*

Google Glass was a headset designed by Google meant to be worn like a pair of eyeglasses, with "a small prism-like screen tucked into the upper corner of the frame" that allowed its user to remain engaged with his electronics, such as a phone or e-mail account.[204] The purpose behind the technology was to allow a user to disengage with electronics by never needing to look down at a screen.[205] According to one author, the original Google Glass failed because there was no real product launch, no mainstream advertising campaign, no proper explanation about its noteworthy features, and no easy way to purchase the product.[206] Google made a second attempt, made public on December 28, 2015, through a few FCC filings detailing the next version of Google Glass.[207] Google expected that the second time, the product would be successful because it was no longer aimed at the general public, but rather meant to be used in the business marketplace.[208] Google Glass, though, was not meant to be; still, the end of Google Glass is not the end of smartglasses.[209] These new developments would

[204] Hayley Tsukayama, *Everything You Need to Know About Google Glass*, WASH. POST (Feb. 27, 2014, 12:36 PM), https://www.washingtonpost.com/news/the-switch/wp/2014/02/27/everything-you-need-to-know-about-google-glass/.

[205] *Id.*

[206] Siimon Reynolds, *Why Google Glass Failed: A Marketing Lesson*, FORBES (Feb. 5, 2015), http://www.forbes.com/sites/siimonreynolds/2015/02/05/why-google-glass-failed/#55600c412131.

[207] A few photos of the new device could be seen at: *OET Exhibits List*, U.S. FED. COMM. COMMISSION (June 12, 2015), https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&RequestTimeout=500&calledFromFrame=N&application_id=eDyH1HI%2FRcK9NnzZ4ggP6w%3D%3D&fcc_id=A4R-GG1.

[208] Jon Phillips, *Google Glass Version 2: New Photos in FCC Filing*, COMPUTERWORLD (Dec. 28, 2015, 2:05 PM), http://www.computerworld.com/article/3018501/wearables/google-glass-version-2-new-photos-in-fcc-filing.html.

[209] Hugh Langley, *The patented history and future of. . .Google Glass: Quite the spectacle*, WAREABLE (Nov. 30, 2016), https://www.wareable.com/google/the-patented-history-and-future-of-google-glass-656 ("As we said at the start of this piece, the past hints to the future, and we'd bet our bottom dollar that some of these ideas are still being worked on somewhere in Alphabet land. We still haven't seen many of the patented concepts appear in the flesh, including some of the more advanced gesture controls

bear further legal complications; if, for example, smartglasses were to enter the corporate market, employers could require employees to use the technology for much of the day. To what extent would the employers be capable of monitoring employees through accessing their smartglasses?

B. *Car-to-Car Communication*

Some cars on the road today already have the capability to brake in case their drivers do not foresee an impending collision. Examples of such top-of-the-line cars include the PRE-SAFE® system on select Mercedes-Benz models, Toyota's pre-collision safety, and Lexus' pre-collision system with pedestrian detection on select SUV models.[210] The state of technology currently consists of using radar or ultrasound to detect obstacles or vehicles; but cars could only use this technology to the extent that they could detect the nearest obstruction.[211] Developing technology leads cars into a realm in which they are capable of broadcasting their location, speed, steering-wheel position, brake status, and a variety of other data points to cars in a couple of hundred meters from their location.[212] Despite the fact that companies like AT&T, with its Connected Car, and General Motors, with its car-to-car communication in a 2017-model Cadillac, are pioneering immense changes in the landscape of vehicle safety, it might take longer than a decade for talking cars to prove a reality, and especially for that market to expand to Europe.[213]

C. *Network of Millions of Genomes*

Most people have at least heard of the Human Genome Project, a scientific endeavor initiated in 1990 with the intended goal of mapping the human genome.[214] The project, started by the National Center for

and minimal designs.").

[210] *Safety*, MERCEDES-BENZ (Feb. 11, 2016), http://www.mbusa.com/mercedes/benz/safety#module-1; *Toyota Safety Sense*, TOYOTA (Feb. 11, 2016), http://www.toyota-global.com/safety-sense/; *Safety*, LEXUS (Feb. 11, 2016), http://www.lexus.com/models/RX/safety.

[211] Will Knight, *Car-to-Car Communication: A Simple Wireless Technology Promises to Make Driving Much Safer*, MIT TECH. REV. (Feb. 18, 2015), https://www.technologyreview.com/s/534981/car-to-car-communication/.

[212] *Id.*

[213] *Id.*; *see also Connected Car*, AT&T, https://www.att.com/shop/wireless/connected-car.html (last visited Feb. 11, 2016); *News and Stories*, GENERAL MOTORS, http://www.gm.com/all-news-stories.html (last visited Feb. 11, 2016).

[214] *An Overview of the Human Genome Project*, NAT'L HUM. GENOME RES. INST., https://www.genome.gov/12011239/ (last visited Feb. 5, 2017).

Human Genome Research, combined with the United States Department of Energy to become the International Human Genome Project.[215] The legacy that the project created when it was complete in April 2003 is being capitalized on every year, from the project ENCODE to the promotion of a Genomic Data Sharing Policy.[216] The most recent and riveting research project is entitled the Matchmaker Exchange. Matchmaker Exchange was founded in 2013 with the goal of building a network on the 200,000 genomes that have already been mapped (Exchange) of phenotypic and genotypic profiles, and then linking those profiles (Matchmaker) to similar cases in order to find genetic causes for patients with rare diseases.[217] Doctors cannot diagnose patients with rare diseases because they are not definitively confident about what causes the genetic variances to occur.[218] The beauty of the enterprise is all that is needed to equip researchers with the causative gene is a single additional case with the same deleterious variant: finding one other person with that same variant solves the puzzle.[219]

D. *Long-Term Effect of the GDPR on Emerging Technologies*

These technological advances point to the fact that it would be difficult to maintain a few of the rights encapsulated in the GDPR, particularly the right to be forgotten. With regard to the Matchmaker Exchange, the GDPR properly dispensed with the following concern: if a European with a rare disease was given the option to remove files indicating her genetic variance and she was the only person documented with that variance, she would deprive any other individuals with that variance from ever having the ability to determine what rare disease they possess; her privacy concerns would overtake the ability to provide another affected individual proper medical care. Article 89, however, did not provide for such an exception.[220] Apropos

---

[215] *About the Institute*, NAT'L HUM. GENOME RES. INST., http://www.genome.gov/10001763/about-nhgri-a-brief-history-and-timeline/ (last visited Feb. 11, 2016).

[216] *See generally About NHGRI: A Brief History and Timeline*, NAT'L HUM. GENOME RES. INST., http://www.genome.gov/10001763#2003 (last visited Feb. 11, 2016).

[217] *The Solution*, MATCHMAKER EXCHANGE, http://www.matchmakerexchange.org/ (last visited Apr. 24, 2016). *See* Antonio Regalado, *Internet of DNA: A Global Network of Millions of Genomes Could be Medicine's Next Great Advance*, MIT TECH. REV. (2015), https://www.technologyreview.com/s/535016/internet-of-dna/.

[218] *Id.*

[219] *The Challenge*, MATCHMAKER EXCHANGE, http://www.matchmakerexchange.org/ (last visited Apr. 24, 2016).

[220] GDPR Provisions, *supra* note 15, at art. 89 ("Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the

connected cars, attempting to retrieve information from the vehicles would likely constitute a breach of privacy, concerning which a data subject would be given permission to remove data. An additional difficulty would be that of the hypothesized embedded chips in human bodies: retrieving information from the chips would indisputably entail a breach of the most sacred privacy.

One author analyzed the right to privacy and control over one's data, and concluded that although too little privacy endangers democracy, the same could be said if constituents have too much privacy.[221] Evgeny Morozov devised a theory of the "invisible barbed wire," in which he postulates: "The invisible barbed wire of big data limits our lives to a space that might look quiet and enticing enough but is not of our own choosing and that we cannot rebuild or expand."[222] As for what more personal data on the Internet leads to, he concluded that, "[t]he more information we reveal about ourselves, the denser but more invisible this barbed wire becomes."[223] Quoting Spiros Simitis, Germany's leading privacy scholar and practitioner, Morozov disagreed with the libertarian approach espoused by Simitis, and stated the following very aptly:

> [N]o progress can be achieved, he said, as long as privacy protection is "more or less equated with an individual's right to decide when and which data are to be accessible." The trap that many well-meaning privacy advocates fall into is thinking that if only they could provide the individual with more control over his or her data—through stronger laws or a robust property regime—then the invisible barbed wire would become visible and fray. It won't—not if that data is eventually returned to the very institutions that are erecting the wire around us.[224]

Morozov's reasoning sheds light on the fact that the opportunity to control one's data may not only be a fallacy, but it would likely only tighten the noose around data users.

---

rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation.")

[221] Evgeny Morozov, *The Real Privacy Problem*, MIT TECH. REV. (Oct. 22, 2013), https://www.technologyreview.com/s/520426/the-real-privacy-problem/.

[222] *Id.*

[223] *Id.*

[224] *Id.*

VI. CONCLUSION: A NEW GLOBAL STANDARD

The General Data Protection Regulation comes into full effect in May 2018; until then, the Privacy Shield will need to endure at least one challenge in the General Court in the European Court of Justice and adapt its provisions to conform to the GDPR, not the Directive. Most American companies will continue to resort to use of the Standard Contractual Clauses, until such future point that the European Commission deems them no longer in compliance with the GDPR. It appears that the rights to data portability, to access, to data minimization, and to be forgotten will dramatically increase data users' capacity to control what personal data will be available to others—and what data they could acquire themselves—after it has been published on the Internet. The fact that virtually any personal data would become vulnerable—even data that is not particularly harmful or was not illegally published in the first place—supports the proposition that there will be an influx of individuals who will request erasure of their personal information immediately upon the application of the GDPR in 2018. As a means of preventing this constant debacle among websites and individuals, it is likely that companies will institute more stringent privacy requirements and will make them easily detectable on their websites.

As it stands, the stance of the new presidential administration is uncertain. President Donald Trump has commented on certain surveillance issues, but has not taken an official stance on technology.[225] Ted Dean, Deputy Assistant Secretary for Services at the Department of Commerce, commented, "Bear in mind the history of the Safe Harbor program, which was negotiated under the Clinton administration, implemented under the Bush administration and continued under the Obama administration. This is the type of program that carries on across administrations."[226] Though precedence is by no means the only condition for a good policy, the Privacy Shield—as the successor to the Safe Harbor—would likely withstand the inauguration of new leadership in the United States. That being said, the Privacy Shield's peaceful transition into a new administration on its own does not ensure the continuing viability of

[225] Nicky Stewart, *The Trump effect*, ITPROPORTAL (Dec. 19, 2016), http://www.itproportal.com/features/the-trump-effect/; Stuart Lauchlan, *Privacy Shield – under fire from activists with Donald Trump yet to show his hand*, DIGINOMICA, LTD. (Dec. 20, 2016), http://diginomica.com/2016/12/20/privacy-shield-fire-activists-donald-trump-yet-show-hand/.

[226] David Meyer, *The Trump effect on Privacy Shield: 'There's a great deal that's unknown'*, INT'L ASS'N PRIVACY PROFS. (Nov. 15, 2016), https://iapp.org/news/a/the-trump-effect-on-privacy-shield-theres-a-great-deal-thats-unknown/.

the program.

For current technology moguls, such as Google, Facebook, LinkedIn, Yahoo, and others, it appears that just as they have been flexible with responding to changing technologies in the past, so they will be flexible with responding to the Privacy Shield and GDPR. What is most worrisome is the ability of new companies to adapt to this changing climate, and the actuality with which the right to be forgotten, right to data portability, and especially, privacy by design, will significantly affect these emerging companies' business models. The right to be forgotten might essentially disappear from the actual application of the GDPR with the widespread use of some newer technologies because they would prove to substantially undermine the entire purpose of these inventions; this might occur either through amendment of the GDPR or through practice.

There is no doubt that a huge shift in the understanding of the protection of private information will occur over the next year within the European Union and with its relationship with the United States. This shift could also bring great privacy improvements for American residents as well, because if companies must adhere to heightened requirements so that they could conduct business in the Union, they might as well implement those safeguards for their employees and American customers, too. Likewise, as the United States previously set the guideposts for Internet usage with its advent, it will do it again through compliance with the Privacy Shield and, implicitly, with the General Data Protection Regulation; except this time, American companies are being motivated by the European Union.