2017

Intangible Privacy Rights: How Europe Will Set the Bar for Worldwide Data Protection

Beata Safari

Intangible Privacy Rights: How Europe Will Set the Bar for Worldwide Data Protection

By Beata Safari*

I. Introduction

The European 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, enacted in 2000, provided 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 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") 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]

Data protection is so important to European citizens that the European Union requires other countries—particularly the United States, where most technology companies are headquartered—

* I am a student at the Seton Hall Law School interested in international data privacy law, and graduating in 2017. I have a BA from The George Washington University in international affairs. First, I would like to thank Professor Tracy Kaye for introducing me to the Schrems Case. I would like to thank my faculty advisor, Professor David Opderbeck, for driving home the analysis and for providing me with the foundation I needed to analyze privacy law. I also want to thank Christina Pellino, my comment advisor, for clawing through the Bluebook to help me with difficult citations, among other things. As always, I am eternally grateful for the support of my family and friends.

[1] *See* Daniel Dimov, *Differences between the Privacy Laws in the EU and the US*, INFOSEC INSTITUTE (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*, EUROPEAN 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')." Council Directive 95/46/EC, art. 2(a), 1995 O.J. (L 281) art. 2(a) [hereinafter Data Protection Directive].

[4] Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C 364) art. 8.

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

to adhere to their stringent requirements.[6] The US-EU Safe Harbor Program ("Safe Harbor Program" or "the Program") was created by the U.S. Department of Commerce while working with the European Commission as a means of implementing the "adequacy" framework adopted by the European Union's Data Protection Directive.[7] Under the Program, American organizations avoid interruptions or delays in their dealings with the Union due to Member State privacy laws.[8] The Program provides a number of benefits to participating American and European organizations, including: providing "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.[9]

The European Union vowed to reform data protection because although Data Protection Directive set an unprecedented foundation for personal data protection, it has not remained current through the immense technological advances that have taken place since, and the nature of the legislation has prevented every EU Member State from implementing uniform standards across the board.[10] Now, the new proposed Regulation, if successful, will "make Europe fit for the digital age."[11]

This Comment will argue that certain articles in the General Data Privacy Regulation would impose greater requirements for data privacy, particularly the provisions on "profiling," the

[6] 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.
[7] *See id. US-EU Safe Harbor Overview*, THE COMMERCIAL SERVICE http://www.export.gov/safeharbor/ [hereinafter *Safe Harbor Overview*] (last visited Apr. 24, 2016).
[8] *Id.*
[9] *Id.*
[10] Press Release, European Commission, 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.
[11] *Id.*

"right to be forgotten," and consent. Part II explores the goals of Data Protection Directive and the Safe Harbor Principles, as well as some of their major criticisms. Part III will break down the extent of the information the European Commission has provided regarding the direction in which the General Data Privacy Regulation will go and its effects on foreign companies. Part IV will review and analyze the evolution of the "right to be forgotten." Part V will discuss how data privacy changes will affect the future state of affairs of a company such as LinkedIn through application of the information known from Part III and the analysis from Part IV. Finally, Part VI will aggregate the analysis from Part V and superimpose it upon anticipated new technological advances and the effectiveness of the Regulation in light of those advances. The directive proposed to accompany the Regulation in the areas of investigation, prosecution, among other police duties, in relation to criminal offenses and other judicial activities,[12] is outside the scope of this Comment.

II. The Data Protection Directive and Safe Harbor Principles

A. Goals of Data Protection Directive

When 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 Organisation 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."[13] 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

[12] Press Release, European Commission, Commission Proposes a Comprehensive Reform of Data Protection Rules To Increase Users' Control Of Their Data And To Cut Costs For Businesses, IP/12/46 (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.pdf.

[13] The OECD Guidelines have since been updated. *2013 OECD Privacy Guidelines*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

country; for the prevention of disorder or crime; for the protection of health or morals; or for the protection of the rights and freedoms of others.[14]

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 ease of the flow of personal data from one Member State to another, while also preserving fundamental rights of individuals.[15] 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 in the protection granted to European Union citizens.[16] 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.[17] 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.[18] Although not expressly provided for in the Directive, article 12(b) could be considered the first real primer on the "right to be forgotten."[19]

B. Safe Harbor Program Framework

Until February 2016, the Safe Harbor Program allowed American companies to enter the European marketplace through an assurance that the American companies were complying with

[14] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter ECHR].
[15] Data Protection Directive, *supra* note 3, at ¶¶ 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 . . . .").
[16] *Id.* at ¶ 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 . . . .").
[17] *Id.* at ¶ 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 . . . . ").
[18] Data Protection Directive, *supra* note 3, at pmbl. (1), (2).
[19] *Id.* at art. 12.

the basic data requirements imposed by Data Protection Directive.[20] Entering into the US-EU Safe Harbor Program was an entirely voluntary decision and required adherence to only a few conditions. 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.[21]

The notice principle required organizations to notify data users about the purposes for which information was collected and used.[22] The choice principle required that data users be given the opportunity to opt out from disclosing personal information to a third party.[23] 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.[24] The onward transfer principle simply acknowledged that in order to disclose information to a third party, an organization must comply with the notice and choice principles.[25] The organization needed to ensure that the third party subscribed to the Safe Harbor Program principles (or it needed to enter into a contractual agreement to confirm that it did so).[26] 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 the information when it was inaccurate.[27] This access principle resembles the "right to be forgotten" principles, in that the General Data Regulation would ensure that users have the ability

[20] Although, arguably, the Safe Harbor program is not defunct until the EU-U.S. Privacy Shield is fully administered. *Safe Harbor Overview*, *supra* note 7.
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Safe Harbor Overview*, *supra* note 7.
[27] *Id.*

to control their level of engagement, as well as the extent of the information they share with the world on the Internet. However, the right does not require that the information posted be inaccurate in order to be eligible for correction, amendment or deletion, just that it be unwanted by the data user. The security principle charged organizations to implement precautions in protecting personal information from loss, misuse and unauthorized access, disclosure, alteration, and destruction.[28] The data integrity principle needed organizations to take sensible steps to ensure that data was reliable for its intended use, accurate, complete, and current.[29] The enforcement principle required: (1) instantly available and affordable mechanisms so that each individual's complaints and 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.[30]

Some of the most prominent criticisms of the Safe Harbor Program include: a lack of adequate compliance to principles, a failure to renew certification, current lack of existence or double entries, and distribution of false and misleading information regarding certification under the Framework, when in fact it was never granted.[31] 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.[32] The Principles had not worked properly in a long time, so when the European Union proposed the General Data Regulation, it was clear that the United States would be directly affected. That is why the United States became very involved in negotiations.

---

[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] Chris Connolly, *The US Safe Harbor – Fact or Fiction?*, GALEXIA (Sept. 26, 2008), 1, 4, 7, http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_struggle_public.pdf.
[32] *Id.* at 4.

C. American Involvement in the General Data Regulation and EU-U.S. Privacy Shield

Extensive American involvement in the drafting of the General Data Regulation and implementation of changes in the Safe Harbor Program have culminated in the new EU-U.S. Privacy Shield ("Privacy Shield").[33] In 2013, American companies and the American government lobbied lengthily 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.[34] Since then, the United States has remained actively engaged in negotiations for the enactment of a new safe harbor agreement in Brussels.[35] In fact, American involvement has been so extensive that LobbyPlag, a website whose purpose consists in delivering greater transparency of ongoing deliberations in the European Commission about the Regulation by leaking documents,[36] is merely one among about a dozen privacy groups that called on the U.S. government to cease its "unprecedented lobbying campaign."[37]

Aside from the imposition of American beliefs on European citizens, the United States began a collaborative project with the Dutch Data Protection Authority ("DPA") called the EU-US 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.[38] Although the Bridge Project is not a governmental initiative,

---

[33] 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.

[34] 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/.

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

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

[37] Collier, *supra* note 34 ("[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/.

[38] Cynthia O'Donoghue & Katalina Bateman, *EU-US Privacy Bridge Project Announced*, REEDSMITH (May 8, 2014), http://www.technologylawdispatch.com/2014/05/privacy-data-protection/eu-us-privacy-bridge-project-announced/;

it does have "soft support" from the European Commission and the Obama Administration,[39] so it could be a step in the right direction if the two governments choose to adhere to the recommendations. The Bridge Project published its recommendations in September 2015, offering ten "bridges" to enhancing a "progressive, sustainable model for protecting privacy in the global Internet environment."[40]

D. The Doubtful Efficacy of the Privacy Shield

On February 2, 2016, the European Union and United States confirmed that the two superpowers had agreed upon the provisions of the Privacy Shield.[41] 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."[42] The three major changes that the EU Commission and the United States claim will take effect as a result of the new framework are: greater responsibilities on companies exchanging with European users as well as a more capable enforcement structure; clearer security measures and more transparency of American government access; and a competent and adequate protection of European citizens' rights with multiple avenues for reparations.[43] The United States has assured the European Commission that it will institute an annual joint review, discussing the companies' adherence to the principles.[44] The Privacy Shield aims to provide Europeans the opportunity for redress in the United States through

Angela R Matney et al., *The Challenges of Third-Party Data Privacy Protection*, 61 RISK MANAGEMENT 32, 34 (2014) [hereinafter Matney et al.].

[39] Matney et al., *supra* note 38, at 34.

[40] Jean-François Abramatic et al., *Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solutions*, PRIVACY BRIDGES (2015), http://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf.

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

[42] EU-U.S. Privacy Shield, UNITED STATES DEPARTMENT OF COMMERCE (Feb. 23, 2016), https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf.

[43] *Id.*

[44] *Id.* at 13.

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 § 2(d)(1)(A)(i), as it "has entered into an agreement with the United States that provides for appropriate privacy protections for information."[45]

Reports about the new provisions have proved lukewarm, at best. Critics have expressed concern that the Privacy Shield will not become enforceable because it will not pass court scrutiny—nor that the European Member States will agree to pass it—and that the Privacy Shield has no teeth to it.[46] 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."[47] The man who almost single-handedly brought about the demise of the Safe Harbor Program, Maximilian Schrems (discussed *infra*), found the Privacy Shield lackluster: "There are tiny improvements, but the core rules on privacy data usage are miles away for EU law. This is nowhere close to 'essential equivalence' that the Court required."[48] 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."[49]

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 court systems and whether or not the European Member States

---

[45] Text of the Judicial Redress Act of 2015 (H. R. 1428), GOVTRACK (Feb. 12, 2016), https://www.govtrack.us/congress/bills/114/hr1428/text.

[46] *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/.

[47] Downes, *supra* note 46.

[48] Lomas, *supra* note 46.

[49] Max Schrems, Max Schrems Page, TWITTER (Feb. 29, 2016), https://twitter.com/maxschrems/status/704278172708302848/photo/1?ref_src=twsrc%5Etfw.

will accept its provisions, the Privacy Shield will likely be accepted by the Member States, and the European Court of Justice and Supreme Court of the United States will likely not come face-to-face with the agreement until next year. At the same time, it is law, so businesses will need to adapt, fast. One big variable is that the provisions of the Privacy Shield depend to some extent upon what the European Commission's final version of the General Data Regulation will be, come early next year.

III. What is Known about the Data Protection Regulation

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 pieces of legislation which provide guidelines for Member State implementation, but depend on the independent passage of a law in every State within a designated period of time.[50] Regulations are narrow, specific pieces of legislation which become immediately enforceable in every Member State without implementing a law.[51] When the European Commission first considered reforming data protection, it was not yet clear that a directive would be replaced by a regulation.[52] 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

[50] *Regulations, Directives and other acts*, EUROPEAN UNION (Apr. 12, 2016), http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm.
[51] *Id.*
[52] *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, Brussels, 4.11.2010, 7 (2010), http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf [hereinafter A Comprehensive Approach on Personal Data Protection].

> the effective enforcement of data protection rules; (5) Improving the coherence of the data protection legal framework.[53]

The first challenge, addressing the impact of new technologies, focuses on the difficulty in ensuring free and informed consent, securing sensitive data, and thus assuring transparency for individuals on the Internet.[54] 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.[55] In responding to the third challenge of 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-US Privacy Shield supposedly has solved that challenge, as will be discussed *infra*. 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 others in some areas, as well as fewer in others.[56]

The text of the new articles in the Regulation grants users, *inter alia*, new rights and creates the European Data Protection Board. Article 7 provides conditions for consent;[57] article 15 creates a right of access for the data subject;[58] article 16 produces a right to rectification;[59] article 17 forms

---

[53] *Id.* at 3–4.
[54] A Comprehensive Approach on Personal Data Protection, *supra* note 52, at 6, 8–9.
[55] *Id.* at 9–10.
[56] *Id.* at 17–18.
[57] If a data subject—"an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person" under Article 4—needs to give consent, the requirement must be clear. A subject has the right to withdraw consent at any time. *Regulation Proposal*, *infra* note 73, at art. 7.
[58] The article provides data subject's right of access to personal data, supplementing the need to inform data subjects of storage period and of rights to rectification and to erasure and to lodge a complaint.
[59] "The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement." *Regulation Proposal*, *infra* note 73, at art. 16.

the bread and butter of the right to be forgotten and to erasure;[60] article 18 informs the right to data portability;[61] article 19 discusses the right to object to the processing of one's personal data for direct marketing; article 20 explains profiling and the new measures put into effect;[62] article 64 sets up the European Data Protection Board; and article 66 describes the tasks of the newly-formed Board.[63]

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.[64] Specifically, the Commission sought to create "smart, sustainable, inclusive growth"[65] and increased coordination of national and European policy. The Commission proposed five measurable targets to complete by the year 2020, which are: (1) for employment; (2) for research and innovation; (3) for climate change and energy; (4) for education; and (5) for combating poverty.[66] The Commission proposed a priority theme called "a digital agenda for

[60] "[O]bligation of the controller which has made the personal data public to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data. It also integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology 'blocking'." *Regulation Proposal*, *infra* note 73, at art. 17.

[61] "[D]ata subject's right to data portability, i.e. to transfer data from one electronic processing system to and into another, without being prevented from doing so by the controller. As a precondition and in order to further improve access of individuals to their personal data, it provides the right to obtain from the controller those data in a structured and commonly used electronic format." *Regulation Proposal*, *infra* note 73, at art. 18.

[62] A data user has the right not to be subject to a measure producing a quasi-discriminatory effect, "based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour." The Article goes on to list exceptions to the subjection of the measure. *Regulation Proposal*, *infra* note 73, at art. 20.

[63] The Board hereby has duties to advise the Commission; examine Members; review the application of the guidelines; recommendations and best practices; issue opinions; promote cooperation; promote common training programs; and promote exchange of knowledge. *Regulation Proposal*, *infra* note 73, at art. 64.

[64] European Commission, Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth, COM (2010) 2020 final (Mar. 3, 2010). For a brief and pictorial explanation of ordinary legislative procedure in the European Parliament, *see Legislative Powers: Ordinary legislative procedure*, EUROPEAN UNION (Mar. 5, 2016), http://www.europarl.europa.eu/aboutparliament/en/20150201PVL00004/Legislative-powers [hereinafter Europe 2020].

[65] *Id.* 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.* at 3, Executive Summary.

[66] *Id.* at 3.

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."[67]

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."[68] 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 . . . .[69]

In the Communication on Digital Agenda for Europe, the European Commission stresses the need to create a "vibrant digital single market,"[70] because the detachment of policies among the 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.

User rights are fundamental and must be enforced using the widest range of means: application of the principle of "Privacy by Design"[71]—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—and exercise of inhibitive sanctions when necessary. These sanctions seem

---

[67] *Id.* at 6.
[68] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels: A Digital Agenda for Europe, 26.8.2010, 7 (2010), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN.
[69] *Id.* at 14 (emphasis added).
[70] Communication, *supra* note 52 at 7.
[71] *Id.* at 17.

evocative of the procedures the court discusses in *Google Spain*, *infra*, proposed with regard to the "right to be forgotten." Even "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.

A regulation, as opposed to the current Directive, would be a huge step towards increasing coordination of national and European policy. This way, certain countries that might otherwise not be predisposed to a safer security framework would need to work harder to achieve the standards that other countries worked intensively to attain as a result of the initial Directive. It would place all Member States on equal footing, as opposed to the drastic variations the Member States have promoted 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 came to a close.[72]

C. Strengths in the Regulation

LobbyPlag released the current secret version of the Regulation 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.[73] In this section and the section *infra*, the focus will be on identifying the strengths and weaknesses in the Regulation, but limited to the scope of the aforementioned articles of interest from *supra*. These portions are articles 7, 15, 16, 17, 18, 19, and 20.

---

[72] Beth Seals, *"One Continent, One Law": General Data Protection Regulation Text Agreed*, GLOBAL BUSINESS IP AND TECHNOLOGY BLOG (Dec. 18, 2015), http://www.iptechblog.com/2015/12/one-continent-one-law-general-data-protection-regulation-text-agreed/.

[73] *Regulation Proposal*, LOBBYPLAG (Jan. 15, 2016, 15:12 EST), http://www.lobbyplag.eu/governments/gdpr [hereinafter *Regulation Proposal*].

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."[74] Consent may be withdrawn at any time, but any 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.[75] These two subsections evidence a substantially strict rule for consent through terms or privacy policies. Article 7(3) also requires a duty to inform about the right to withdraw consent.

Article 9 shapes the processing of special categories of personal data. Personal data revealing race or ethnicity, political affiliation, religion or beliefs, or genetic, health or sex life, is prohibited.[76] A substantial strength of the article 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.[77] Article 16 delineates the right to rectification, which provides a data subject with the right to rectify any inaccuracies in personal data that concerns him.[78] A data subject may also request the completion of incomplete personal data.[79]

The right to be forgotten and to erasure is embodied in article 17. The description of the right is as follows: "The controller shall have the obligation to erase personal data without undue delay and the data subject shall have the right to obtain the erasure of personal data without undue

[74] *Id.* at art. 7(2).
[75] *Id.* at 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.").
[76] *Id.* at art. 9(1).
[77] *Id.* at art. 9(4)(a).
[78] *Id.* at art. 16 ("The data subject shall have the right to obtain from the controller the rectification of personal data concerning him or her which are inaccurate.").
[79] *Regulation Proposal*, *supra* note 73, at art. 16.

delay where one of the following grounds applies . . . ."[80] The "controller" is the natural or legal person or other authority "which alone or jointly with others determines the purposes and means of the processing of personal data . . . ."[81] The right may be exercised when the data is no longer necessary for its initial purpose, the data subject withdraws his consent under article 6, the subject objects to the processing of personal data under article 19, the data has been unlawfully processed, or the data must be erased in order to comply with certain legal obligations.[82]

The right to object is located under article 19. The Regulation allows a data subject to protest the processing of data if it is "overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[83] While it is a worthwhile endeavor to offer a right to object, it does seem perplexing to identify what kind of fundamental rights might have such an overwhelming effect as to require taking down the information. The fundamental right at issue in the Regulation is the right to privacy: would that right not be affected by every piece of information that ends up on the Internet?

The right not to be subject to profiling is under article 20. Besides the right to be forgotten and the right to object, this right will also have a substantial effect on a company like LinkedIn.[84] Particularly, the article stipulates that a data subject "shall have the right not to be subject to a decision evaluating personal aspects relating to him or her, which is based solely on automated processing, including profiling, and produces legal effects concerning him or her or significantly affects him or her."[85] The only situations in which the decision evaluating a data subject's personal

[80] *Id.* at art. 17(1).
[81] *Id.* at art. 4(5).
[82] *Id.* at art. 17(1)(a)–(e).
[83] *Id.* at art. 19(1) (quoting art. 6(1)(f)).
[84] The extent of the right not to be subject to profiling is discussed in depth, *infra* Pt. V.
[85] *Id.* at art. 20(1).

aspects might come about are when the 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.[86] In general, this right is to the great benefit of the subject since it prohibits the unreasonable invasion into an individual's personal preferences and characteristics; however, the section pertaining to explicit consent is inconsistent with article 7, because there is no mention of the article's adherence to the framework set up there. Thus, it is ambiguous how much protection is offered under the third point.

D. Weaknesses in the Regulation

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.[87] The Council's revision now stands as allowing the controller to "demonstrate that unambiguous consent was given by the data subject" in the context of article 6(1)(a).[88] The Council also added another provision, which provides the same level of unambiguous consent when article 9(2)(a) applies.[89] 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.[90] The result of these changes is a remarkable favoritism towards the controller; in essence, any ambiguity in the delivery of the consent would be resolved in favor of the controller. In addition, there is no

[86] *Regulation Proposal*, *supra* note 73, at art. 20(1)(a)–(c).
[87] *Id.* at art. 7(1). A "controller" is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data . . . ." *Id.* at art. 4(5).
[88] *Regulation Proposal*, *supra* note 73, at art. 7(1). Article 6(1)(a) states that "[p]rocessing of personal data shall be lawful only if and to the extent that at least one of the following applies: the data subject has given unambiguous consent to the processing of their personal data for one or more specific purposes . . . ." *Id.* at art. 6(1)(a).
[89] *Id.* at art. 7(1)(a). Article 9(2)(a) concerns the processing of special categories of personal data and is discussed in detail *infra*.
[90] *Id.* 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.").

consideration of the imbalance between parties, likely because there would more often than not be a vast differential between the two parties, unless the data subject is a large business.

Article 10 concerns circumstances in which processing of data does not require personal information. In such a case, the controller does not need to receive further information or engage in more processing.[91] This is a significant weakness since the exception allows controllers a large amount of discretion in determining what kinds of activities on the Internet require personal identification, because such a requirement would allow data subjects to exercise rights granted under the Regulation.

The right to data portability is encapsulated under article 18 and all but disappears after the modifications the Council made. Initially, the article allowed a data subject to be able to receive a copy of any data going through processing in an electronic or physical format.[92] This right was moved into articles 15(2) and 15(2a), but with severe limitations: a full copy of the data cannot be supplied because it would be too costly and the data will not be conferred at all if it would disclose the personal data of other subjects.[93] Although the Article allows the opportunity to transmit personal data in a "commonly used and machine-readable format without hindrance form the controller,"[94] that possibility does not replicate that which was removed because it is unclear whether the data subject would be able to request that information or would need to already be in possession of it.

IV. Evolution of the Right to Be Forgotten

A. From Data Protection Directive to Google to Facebook

[91] *Id.* at art. 10(1) ("If the purposes for which a controller processes personal data do not require the identification of a data subject by the controller, the controller shall not be obliged to acquire additional information nor to engage in additional processing in order to identify the data subject for the sole purpose of complying with this Regulation.").
[92] *Regulation Proposal*, *supra* note 73, at art. 18(1).
[93] *Id.* at art. 15(2)–(2a).
[94] *Id.* at art. 18(2).

As discussed *supra* in Part II.A, the right to be forgotten was not included in Data Protection Directive, but the idea was almost implicit in the document under article 12.[95] 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.[96] Another author argues that the two do not represent the same idea, as the right to be forgotten includes data "that does not breach any norm."[97] Such a norm could be a 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."[98] On the other hand, enforcing the right to be forgotten would cause deletion of personal information regardless of whether or not the information proved harmful or was illegally processed.[99]

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*.[100] 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.[101] 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,

[95] *See* Press Release, *supra* note 12.
[96] 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 proposed General Data Protection Regulation.").
[97] Ignacio Cofone, Google v. Spain*: A Right To Be Forgotten?*, 15 CHI.-KENT J. INT'L & COMP. L. 1, 8 (2015).
[98] *Id.* at 6.
[99] *Id.* at 8.
[100] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), [2014] E.C.R. I-317 (May 13, 2014) [hereinafter Google Spain].
[101] *Id.* at ¶ 2.

respectively.[102] 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.[103] 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.[104] Gonzalez supported his assertions by referencing the fact that the attachment proceedings had been resolved and thus that retaining the data was irrelevant.[105]

The court held that by searching for information published on the Internet, the data user "collects" data within the meaning of the Directive.[106] The data user is the "controller" in respect of the processing of the search engine.[107] 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.[108] 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.[109]

[102] *Id.* at ¶ 14.
[103] *Id.*
[104] *Id.* at ¶ 15.
[105] *Id*.
[106] Google Spain, *supra* note 100 at ¶ 28.
[107] *Id.* at ¶ 21.
[108] *Id.* at ¶ 62.
[109] *Id.* at ¶ 81.

The ECJ recognized a right to be forgotten under Data Protection Directive. 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.[110]

2. Schrems Case

The second pivotal case the European Court of Justice heard involving the right to be forgotten was in 2015, in *Maximilian Schrems v. Data Protection Commissioner*.[111] Maximilian Schrems filed a class action type of 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,[112] tracked Internet 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.[113] Procedurally, the following occurred: the Safe Harbor was sent to the European Court of Justice;[114] and the case was tried in 2015 in the European Court of Justice, but the opinion by Advocate General Bot was delayed, likely because of talks behind closed doors between the US and the EU.[115] Following the postponement, the plaintiff applied to have the case considered

[110] 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.

[111] C-362/14, Maximilian Schrems v. Data Protection Commissioner, [2015] E.C.R. I-____ (Oct. 6, 2015) [hereinafter Schrems Case].

[112] The PRISM surveillance program 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/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

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

[114] *News*, EUROPE VERSUS FACEBOOK (Mar. 24, 2015), http://europe-v-facebook.org/EN/en.html.

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

in the first instance in the Vienna Regional Court (Landesgericht), but the court found that a "class action" is not admissible on procedural grounds.[116] The case was appealed to the Higher Regional Court (Oberlandesgericht). As the matter stands, the Oberlandesgericht will decide whether class actions are lawful, and in all likelihood, the case will once again be referred to the European Court of Justice. 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.[117] If nothing else, Mr. Schrems joked that he would like to be the litigant who had appeared most often in front of the ECJ.[118]

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.[119]

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;[120] Decision 2000/520[121]—which implemented the safe harbor privacy principles—does not

[116] *Id.* (Oct. 21, 2015).
[117] 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].
[118] *Id.*
[119] *CJEU: First Reaction to AG's Opinion on NSA "PRISM" Scandal Facebook's EU-US Data Transfers Under "Safe Harbor" Not Legal*, EUROPE VERSUS FACEBOOK, (Sept. 23, 2015), http://www.europe-v-facebook.org/GA_en.pdf.
[120] Schrems Case, *supra* note 111 at ¶ 144.
[121] Commission Decision of 26 July 2000 pursuant to Data Protection Directive of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor, privacy principles and related frequently asked questions issued by the US Department of Commerce, Official Journal L 215, 25/08/2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

contain sufficient guarantees;[122] and finally that Facebook did not breach the safe harbor principles,[123] 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."[124] 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.[125]

There are some practical difficulties in implementing the findings of this decision. The right to be forgotten is intended to allow individuals to control their data and not overcrowd cyberspace with needless information. 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.[126] This occurrence symbolizes the fact that although the Regulation might convince companies to remove information from their websites that consumers request be taken down, it will never truly disappear. 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

[122] Schrems Case, *supra* note 111111 at ¶ 159.
[123] *Id.* at ¶ 168.
[124] *Id.* at ¶ 181.
[125] *Media Update for 21/10/2015*, EUROPE VERSUS FACEBOOK (Oct. 21, 2015), http://www.europe-v-facebook.org/PA_OLG_en.pdf.
[126] Schrems Lecture, *supra* note 117.

probably the most filmed stack of papers, ever!"[127] 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.

V. LinkedIn and How it Will Be Affected

A. The Unique Nature of LinkedIn

LinkedIn was officially launched on May 5, 2003.[128] The company's mission is to "connect the world's professionals to make them more productive and successful."[129] From its mission statement, it is already clear that 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.[130] 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, a certain brand of individuals—employers—seek a certain brand of individuals—employees—and vice versa. Employees and employers would likely not seek out like categories of individuals, unless the intention was to engage in a forum.

---

[127] *Id.*

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

[129] *Id.*

[130] The most popular social networks that resemble LinkedIn include Facebook, Twitter, Google Plus+, VK, and Meet-Me. Facebook's mission statement is "to give the power to share and make the world more open and connected." *About Facebook*, 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).

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;[131] (2) IP addresses;[132] (3) URLs from whence users arrived at the page; (4) URLs to which the users go; (5) OS details;[133] (6) type of Internet browsers; (7) mobile IDs; and (8) location data.[134] 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," LinkedIn provides a user's "Rights and Limits" to be the following:

> 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

[131] 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).

[132] 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 Adddress?*, ABOUT.COM, http://compnetworking.about.com/od/workingwithipaddresses/g/ip-addresses.htm (citing Bradley Mitchel, *TCP/IP – Transmission Control Protocol/Internet Protocol*, ABOUT.COM (Apr. 26, 2015), http://compnetworking.about.com/cs/basictcpip/g/bldef_tcpip.htm).

[133] 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*, ABOUT.COM (Oct. 29, 2015), http://pcsupport.about.com/od/termshm/g/term_os.htm.

[134] *Privacy Policy*, LINKEDIN, § 2.1, https://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv (last visited Mar. 23, 2016).

information, and your comments on sponsored content may be visible as noted in the Privacy Policy.

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.[135]

Through the information to which the company has access, without a doubt it engages in "profiling," by which it learns enough about a user to be able to put him on a spectrum and tailor his networking experience based off of his information.

C. What Provisions of the General Data Privacy Regulation Would Apply

Under article 20 of the Preamble, the Data Privacy Regulation aims to cover activities of outside controllers when the outsider controllers' processing activities are related to the offering of goods or services, or to the monitoring of the behavior of such data subjects.[136] The question is whether LinkedIn provides goods or services. Neither term is defined under Article 4[137] nor under Data Protection Directive. A definition of the terms might be presumed from the Treaty on the Functioning of the European Union ("TFEU"), an almost constitutional document. Under TFEU 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."[138] "Free circulation"

[135] *User Agreement*, LINKEDIN, § 3.1, https://www.linkedin.com/legal/user-agreement?trk=hb_ft_userag (last visited Mar. 23, 2016) (emphasis added).
[136] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM(2012), 20 (2012).
[137] The definitions in the article are limited to various aspects of data and some definitions of a business nature, among other independent terms.
[138] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, art. 28, Dec. 13, 2007, 2007 O.J. (C 306) [hereinafter Treaty of Lisbon].

implies that import formalities have been conformed to, customs duties or charges have been levied, and the provider did not endure a total or partial drawback of the duties or charges.[139] 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.[140]

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 57(b) and (d), there would likely be a strong argument that LinkedIn engages in activities of a commercial nature, since it engages in marketing and sales. LinkedIn offers the following marketing products: "Lead Accelerator," "Sponsored Updates," "Sponsored InMail," "Display Ads," and "Text Ads."[141] 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."[142] Through the navigator, companies are driven to make the right connections and sell their goals and aspirations to people whom they would personally affect.

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 were to be free from the goods and services analysis, it would certainly fall under the realm of

[139] *Id.* at art. 29.
[140] *Id.* at art. 57.
[141] *Marketing Solutions*, LINKEDIN, https://business.linkedin.com/marketing-solutions (last visited Mar. 23, 2016).
[142] *Sales Navigator*, LINKEDIN, https://business.linkedin.com/biz/sales-solutions/b2b-sales-navigator (last visited Mar. 23, 2016).

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 General Data Privacy Regulation describes that the act of profiling targets decisions concerning the data subject for analyzing or predicting his personal preferences, behaviors, and attitudes.[143]

D. What Aspects of Business Would Change

LinkedIn announced its Fourth Quarter results on February 4, 2016.[144] 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."[145] LinkedIn's revenue increased by thirty-five percent in 2015 from $862 million to $2.991 billion.[146] In its news release, LinkedIn spoke about some risks and uncertainties regarding its "Safe Harbor" statement under the Private Securities Litigation Reform Act of 1995 ("PSLRA"), which covers cases under federal securities laws and ensures that frivolous lawsuits are not brought.[147] Though not immediately harkening to the Privacy Shield, in fact LinkedIn would face the same kinds of difficulties under both laws. In that regard, LinkedIn noted the following difficulties in adhering to the "Safe Harbor" provisions:

> "security measures and the risk that they may not be sufficient to secure our member data adequately or that we are subject to attacks that degrade or deny the ability of members to access our solutions; expectations regarding our ability to timely and effectively scale and adapt existing technology and network infrastructure to ensure that our solutions are accessible at all times with short or no perceptible load times; . . . privacy, security and data transfer concerns, as well

[143] *See supra* note 37.
[144] *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.
[145] 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 [hereinafter *Fourth Quarter Results*].
[146] *Id.*
[147] *Id.*; 15 U.S.C. § 77a, et seq. (2012).

> as changes in regulations which could impact our ability to serve our members or curtail our monetization efforts . . . .[148]

The bulk of the issues that LinkedIn expects to confront with regard to the PLSA are potential inadequate security measures, changing technological advances, and privacy and data transfer concerns.

LinkedIn will no longer be capable of engaging in the extent of the profiling in which it currently engages. 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" as it has been provided for in the Regulation 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 some kind of 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 for, 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 Regulation article 20(2)(a)–(c). 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. Subsection (b) considers whether the processing was authorized by a Member State and lays down procedures by which the subject's interests are protected. Subsection (c) considers whether the data subject gave consent under article 7 (*Conditions for consent*).

[148] *Fourth Quarter Results*, *supra* note 147145.

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 General Data Regulation will have negligible effect on LinkedIn's ability to do business. LinkedIn has built-in mechanisms that are capable of addressing 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 been able to build a sustainable model, which will certainly adapt to changing rules and regulations. The same, however, cannot be said for companies that want to want to make their first step into the European market: with these new rigorous requirements—enforceable or not—new businesses might find themselves dissuaded from the European market until they make enough revenue to instill greater data protections.

VI. New Advances in Technology and their Effects

A. Google Glass Version 2

Google Glass is 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 allows its user to remain engaged with his electronics, such as a phone or e-mail account.[149] The purpose behind the technology is to allow a user to disengage with electronics by never needing to look down at a screen.[150] 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

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

features, and no easy way to purchase the product.[151] Google made a second attempt, made public on December 28, 2015, through a few FCC filings, detailing the next version of Google Glass.[152] Google expects that this time, the product will be successful because it is no longer aimed at the general public, but rather will be engaging in the business marketplace.[153] This new development brings further legal complications; particularly, the extent to which employers could monitor their employees on the job.

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.[154] 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.[155] 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.[156] 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,

---

[151] 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.

[152] A few photos of the new device could be seen at: *OET Exhibits List*, FCC (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.

[153] 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.

[154] Safety Module, MERCEDES-BENZ (Feb. 11, 2016), http://www.mbusa.com/mercedes/benz/safety#module-1; Pre-Collision Safety, TOYOTA (Feb. 11, 2016), http://www.toyota-global.com/innovation/safety_technology/safety_technology/pre-collision_safety/; Safety, LEXUS (Feb. 11, 2016), http://www.lexus.com/models/RX/safety.

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

[156] *Id.*

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.[157]

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. The project, started by the National Center for Human Genome Research, combined with the United States Department of Energy to become the International Human Genome Project.[158] 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.[159] The most recent and riveting research project is entitled the MatchMaker Exchange, 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.[160] Doctors cannot diagnose patients with rare diseases because they are not definitively confident about what causes the genetic variances to occur.[161] The beauty of the enterprise is that 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.[162]

D. Long-Term Effect of the Regulation

---

[157] *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).
[158] *About the Institute*, NATIONAL HUMAN GENOME RESEARCH INSTITUTE, http://www.genome.gov/27534788 (last visited Feb. 11, 2016).
[159] *See generally About NHGRI: A Brief History and Timeline*, NATIONAL HUMAN GENOME RESEARCH INSTITUTE, http://www.genome.gov/10001763#2003 (last visited Feb. 11, 2016).
[160] *The Solution*, MATCHMAKER EXCHANGE, http://www.matchmakerexchange.org/ (last visited Apr. 24, 2016). *See* Antonio Regalado, 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/.
[161] *Id.*
[162] The Challenge, MATCHMAKER EXCHANGE, http://www.matchmakerexchange.org/ (last visited Apr. 24, 2016).

All of these technological advances point to the fact that it would be difficult to maintain a few of the rights encapsulated in the Regulation, particularly the right to be forgotten. With regard to connected cars, attempting to retrieve information from the vehicles would likely constitute a breach of privacy. As for the MatchMaker Exchange, if an European with a rare disease were 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. An additional example 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.[163] 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."[164] 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."[165] Quoting Spiros Simitis, Germany's leading privacy scholar and practitioner, Morozov disagreed with his libertarian approach 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 control over his or her data—through

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

> 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.[166]

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.

VII. Conclusion

Agreement on the final draft of the General Data Regulation is set for early 2016,[167] so there is certainly much opportunity for the results of the *Google Spain* and *Schrems* cases, and the Privacy Shield to affect the draft legislation. It appears that the "right to be forgotten" will increase data users' capacity to control what information will be available to others after it has been published on the Internet. The fact that any data would become vulnerable—even data that is not 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 Regulation in 2018. As a means of preventing this kind of 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.

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 General Data Regulation. 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 will significantly affect these emerging companies' business models. The right to be forgotten might essentially disappear from the actual application

---

[166] *Id.*

[167] *Timeline of the New EU Data Protection Regulation – Latest Developments and Implementation*, ALLEN & OVERY, http://www.allenovery.com/publications/en-gb/data-protection/Pages/Timetable.aspx (last visited Nov. 17, 2015).

of the General Data Regulation with the widespread use of some newer technologies, such as Google Glass, Car-to-Car Communication, and the MatchMaker Exchange, because they would prove to substantially undermine the entire purpose of these inventions.

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 its relationship with the United States. This shift could also bring great privacy improvements for American citizens as well, because if companies will have to adhere to heightened requirements so that they could conduct business in the European Union, they might as well implement those safeguards for their employees and American customers, too.