The Stimulus for Data Protection Law Around the World: The Development and Anticipated Effect of the European Union’s New Data Rules

ARLETTE NOUJAIM*

INTRODUCTION

Do you ever question the process behind one-click purchases on Amazon? How stores send promotional text messages when you are in the area? How the advertisements on your web browser are reflective of your most recent Google search? Or even how your credit card(s) are prone to fraudulent expenditures through popular department stores such as Target, Neiman Marcus, and Wal-Mart? These questions were not answered in the past because they were never an issue. Today, however, your personal data is everywhere, including in the hands of hackers and exasperating marketing departments. Entering sweepstakes at a local grocery store now resembles signing a right of privacy death wish. Unprotected personal data, a notion that could serve as an answer to the above questions, has brought a wave of apprehension upon organizations concerning an individual’s right of privacy.

Within the last four decades, society has seen a rapid advancement in data collection, storage, and transfer technology. This widespread availability of data, however, is a double-edged sword. On one end, the collection of data by global organizations opens way for technological and behavioral advancements. Nonetheless, on the other end, data collection presents these organizations with complex privacy issues. Thus, countries around the world are forced to balance the two considerations against one another and prioritize accordingly. For the European Union (“EU”), the decision to prioritize privacy issues was not challenging. Currently, Europe is the world leader in protecting the data of its citizens and has developed corresponding laws reflective of its vision to guarantee a uniformly high level of privacy protection for its citizens, whilst ensuring a free flow of personal data.

Part I of this Comment will briefly consider the meaning behind data

---

* Arlette Noujaim is currently pursuing a J.D. and certificate in Intellectual Property and Technology Law from the University of San Francisco School of Law. The Author is a graduate of San Jose State
protection from a European vantage point. This initial analysis will discuss the definitions associated with commonly used terms in the field and will clarify confusing aspects of the concept.

Part II presents readers with a more profound understanding of data protection as it is handled and monitored in the EU. More specifically, this analysis includes a comprehensive discussion on the currently recognized Data Protection Directive 95/46/EC ("Directive"), followed by a discussion on the emerging General Data Protection Regulation ("Regulation") and its future impact on organizations operating or conducting business in the EU.

The final segment of this Comment, Part III, will consider the ongoing effect of the Directive and the anticipated effect of the Regulation on the United States ("U.S.") and U.S.-based organizations. Part III will briefly focus on the distinctive methods of handling data protection, primarily on the former International Safe-Harbor Principles, and the subsequent uncertainty brought by the agreement’s invalidation in October 2015.

I. A NEW AGE OF PROTECTION: WHAT IS DATA PROTECTION LAW?

A name, a photograph, an e-mail address, medical records, bank records, a computer’s IP address, and even individual posts on social networking websites, are all considered personal data. Personal data is “any information relating to an individual, whether it relates to his/her private, professional or public life.” The EU data protection rules are appropriately applicable if an individual can be “identified, directly or indirectly, by such data.” Personal data that reveals “racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, and the processing of data concerning health or sex life,” is considered sensitive data, and thus, is afforded more stringent protection under the EU data protection rules.

The most commonly cited description of “privacy” dates back to 1890, in an article by Louis Brandeis and Samuel Warren, in which they defined the term to mean “the right to be let alone,” a notion that sounds awfully familiar to U.S. citizens. In the article, Brandeis and Warren discussed whether the theory of privacy as ownership, “implying that people own the data that relates to them,” is an accurate description. However, it is difficult to view personal data as one’s property, since information may be at many different locations at one time compared to

---

2 Id.
3 Id.
5 Peter Blume, Data Protection and Privacy—Basic Concepts in a Changing World, 56 SCANDINAVIAN STUD. L. 151, 156 (2010).
6 Id. at 156-57.
real estates' stationary position. Furthermore, viewing personal data as property would mean it could be sold, which for obvious reasons, would cause a corrupting landscape under the privacy notion.7

Copyright law presents us with a better interpretation of privacy, in which privacy is viewed as the right to secrecy; parallel to an author's right to possess unlimited rights to his work prior to making it public.8 However, copyright law still fails to capture the true essence of a privacy right, as an author's work has no value unless there is a publication, in contrast to, a right lost as soon as there is a publication. Ultimately, when information leaves an individual's privacy sphere, it is "not private in the true sense of the word but this however does not necessarily imply that it may be freely used" because legal rules may govern the boundaries.9

The previous paragraph presents readers with a perplexing question, what is the difference between data "privacy" and data "protection"? In Europe, mechanisms focusing on protecting privacy and related interests with regards to the processing of personal data are described as "data protection."10 Outside of Europe, the nomenclature tends to be "data privacy" or "information privacy."11 Regardless of these differences in vocabulary, these mechanisms are explicitly "aimed at regulating the processing of data" as related to an individual.12 Data protection originates from the German word "Datenschutz."13 This terminology essentially fails to signify the dominant "interests served by the norms to which it is meant to apply."14 Nonetheless, the term has gained great popularity in Europe and has parallel meaning with principles associated with "data privacy."15

There are three main parties considered when discussing data protection: the data subject, the data controller, and the data processor. Under the Directive, a data subject is defined as "an identifiable person is one who can be identified . . . by reference to an identification number or . . . to his physical, psychological, mental, economic, cultural or social identity."16 The Regulation expanded the definition of a data subject to include "location data and on-line identifiers in the list of factors which may lead to an individual being 'identified or identifiable'" (to be discussed in more detail in Part II).17 Under the Directive, a "data controller" is a

---

7 Id. at 157.
8 Id.
9 Id.
10 Lee A. Bygrave, Privacy and Data Protection in an International Perspective, 56 SCANDINAVIAN STUD. L. 165, 166 (2010).
11 Id.
12 Id.
13 Id. at 168.
14 Id.
15 Id.
17 Executive Briefing Paper: Proposed General Data Protection Regulation, HUNTON & WILLIAMS (2012),
"natural or legal person, public authority, agency or any other body which . . . determines the purposes and means of the processing of personal data."18

In most cases, the data controller is the organization processing the personal data associated with the individual. Finally, the “data processor” is defined as a “natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.”19 Examples of data processors include cloud-computing service providers and franchisors, in cases where the franchisee is considered the controller.

The legal systems of many countries contain a variety of rules that “embody elements of the basic principles typically found in data protection instruments or which can otherwise promote these principles.”20 However, only a few have adopted rule-sets that are directly concerned with stimulating data protection or have appointed independent agencies explicitly charged with overseeing the implementation and advancing development of these rule-sets.21 Member states of the EU, which make up a majority of those countries, have become global leaders in data protection laws, while other countries’ attempt to emulate their rule-sets.22 Thus, it is beneficial to grasp a comprehensive understanding of the EU’s data protection laws that make them such a stimulus for other countries.

II. DATA PROTECTION IN EUROPE

Protecting the personal information of citizens has always been a priority for member states of the EU, which has the oldest and most comprehensive data protection laws.23 Historical significances include invasions of privacy at the core of certain World War II abuses and a tradition of prospective law-making that seeks to guard against future harms, particularly those where social issues are concerned (discussed more in Part III).24 In alignment with the EU’s bureaucratic history, it has prioritized the development of data protection laws since the early 90s, when unprotected personal data first proved to be an issue, with the employment of the Directive in 1995.25 The Directive continues to serves as the current body of law concerning data protection, but as a result of a rapid growth in digital innovation, could be replaced with the Regulation

19 Id. (emphasis added).
20 Lee A. Bygrave, Privacy and Data Protection in an International Perspective, 56 SCANDINAVIAN STUD. L. 165, 180 (2010).
21 Id.
22 See id. (“All of these provisions give an impression that the E.U., in effect, is legislating for the world.”).
23 Id. at 188.
24 See id. at 176.
25 See id. at 182.
within the coming years.\textsuperscript{26}

A. THE DATA PROTECTION DIRECTIVE 95/46/EC

The E.U. Directive 95/46/EC has become the leading innovator and standard for data protection around the world.\textsuperscript{27} The Directive operates under the “dual purpose of ensuring the free movement of personal data . . . throughout the EU [internal market and guaranteeing a uniformly high level of privacy protection for data subjects.\textsuperscript{28} Today, the Directive is considered the world’s most aspiring and comprehensive data privacy initiative of the high-technology era.\textsuperscript{29} As a result, its underlying objectives and eight definitive principles are foundational to developing future data protection laws and amendments, including the Regulation, within the EU, as well as, outside of the European domain.

1. General Discourse of Directive 95/46/EC

The Directive, which mainly focuses on the actions of the data controller rather than those of the data subject, generally sets out a “high level of normative density with the result that EU member states cannot go beyond or fall short of the proposed standards.”\textsuperscript{30} Member states are committed to translate “the minimum requirements prescribed by the Directive into national legislation.”\textsuperscript{31} However, member states have the possibility to introduce additional requirements, as long as, these are in compliance with the Directive’s procedures.\textsuperscript{32} The considerable margin of choice for transposition of the Directive into national law causes national deviations arising from differing interpretations of the laws by supervisory authorities, which is amongst the reasons for the Regulation reform.

2. Foundational Principles of Directive 95/46/EC

The minimum procedural requirements of the Directive are set out through eight principles, which encompass various aspects associated with the protection of personal data.\textsuperscript{33} Though the Directive is today considered a legal framework that has struggled to remain relevant in an age of mass information sharing, it is still foundational. Thus, it is crucial to grasp a thorough understanding of its principles and their reasoning.

\begin{thebibliography}{9}
\bibitem{}\textsuperscript{26} See id.
\bibitem{}\textsuperscript{27} See id. at 187.
\bibitem{}\textsuperscript{29} Id. at 940.
\bibitem{}\textsuperscript{30} Id.
\bibitem{}\textsuperscript{32} Id.
\end{thebibliography}
i. Transparency

The principle of transparency embodies the notion that "[t]he individual person must have a real possibility of knowing how personal data are being processed, for what purpose and by whom." Furthermore, the Directive indicates that an individual must be informed about others having access to the data and any disclosure of it. The Directive requires businesses to retain detailed information concerning the data's use and to respond swiftly to all inquiries concerning it. This demands personnel and time to review and revise all company practices, retain records, and respond to client information requests.

The Directive also requires data controllers to notify the member states’ Data Protection Authorities ("DPAs") before executing any automatic processing. "The data controller or his representative must notify the appropriate national supervisory authority before carrying out any automatic data processing operation" (each authority in which the controller processes data). This notification must include:

- The name and address of the controller and his representative; the purpose or purposes of the processing; a description of the categories of data subjects and of the categories of data relating to them; the categories of recipients to whom the data may be disclosed; the proposed transfers of data to third countries; and a general description of the measures taken to ensure security of processing that will allow the supervisory authority to make a preliminary assessment of their appropriateness.

The notification procedure clearly illustrates one aspect of the Directive’s burdensome, costly nature. An alternative to this notification requirement involves the national authority making it a requirement for data controllers to appoint a data protection officer.

Modern information technology has created complexity in this aspect and has made it difficult for the organizations to know exactly when an individual’s data is being collected. Thus, the aspect of transparency has gained great importance and is addressed more broadly and concisely in the Regulation.

ii. Right of Access

The right of “access, rectification and opposition” encompasses the data subject's rights “to obtain copies of all data relating to him or her that

---

35 Id.
38 Id.
39 Id.
40 Id.
are processed, to rectify inaccurate data, and to object to processing in certain situations.\textsuperscript{42} Thus, individuals are enabled to trace which third parties hold personal information about them, verify how they are using it, and enjoin uses that do not conform to those specified in the controller's initial notice.\textsuperscript{43} Furthermore, the data subject may "object to the processing of his data at any time based on 'compelling legitimate' grounds relating to his particular situation."\textsuperscript{44} Where the objection is "justified," the controller must halt all processing of the data.\textsuperscript{45} In other words, in order for an organization to stop processing personal data, the burden of proof initially falls on the data subject to provide a legitimate reason to end the processing.

The right of access is restricted where the processing of data is essential to national security, public safety, criminal investigations, or other important economic or financial reasons associated with the member state.\textsuperscript{46} This notion is one of the main areas in which the Directive and Regulation differ, as the burden of proof switches to the controller in this respect (discussed in more detail below).\textsuperscript{47}

iii. Legitimate Purpose

Under the Directive, personal data must be processed "fairly and lawfully" indicating that personal data may only be processed for "specified, explicit, and legitimate purposes."\textsuperscript{48} Further, data may only be processed and used for the purpose specified, so that enterprises are prohibited from collecting unnecessary information.\textsuperscript{49} However, the Directive provides exceptions to this requirement if data is processed for "historical, statistical or scientific purposes," as long as, the member state has appropriate safeguards in place.\textsuperscript{50}

An example of a legitimate purpose that justifies the processing of data under the Directive is implied consent.\textsuperscript{51} If an organization has acquired the implied consent of a subject, it has obtained a legitimate purpose for collecting the personal data.\textsuperscript{52} Other legitimate purposes include those related to a "public interest."\textsuperscript{53}

\textsuperscript{43} Id. at 979.
\textsuperscript{44} Id. at 962.
\textsuperscript{45} Id.
\textsuperscript{46} See id. at 959.
\textsuperscript{47} See id. at 974.
\textsuperscript{49} See id.
\textsuperscript{50} Id.
\textsuperscript{52} Id.
\textsuperscript{53} Id. at 29.
iv. Quality and Proportionality

The Directive additionally indicates that in collecting data, the information must be:

'adequate, relevant and not excessive' given the purposes for which it is being acquired. It must be accurate and, where necessary, 'kept up to date'. Every reasonable step must be taken to ensure that inaccurate or incomplete information is either erased or rectified. Finally, data must be kept in a form which permits identification of the data subject for 'no longer than necessary' for the purposes for which it was collected or processed.\(^{54}\)

Thus, ensuring the accuracy of the collected data and incorporating a type of retention program to monitor unnecessary data, is critical for organizations operating in the EU.

v. Security

The fifth principle of the Directive, security, ensures that the data controller takes "technical and organizational security measures" appropriate to the risks of the processing.\(^{55}\)

Security measures include implementing security software systems, preforming consecutive internal audits, reciting data protection information to all employees and executives, and other tasks generally associated with an effective data protection compliance program.\(^{56}\)

The security principle also requires that data processors, acting under the authority of the data controller, process data only upon receiving instructions from the controller.\(^{57}\) Ultimately, "controllers are responsible for ensuring that their processors provide sufficient guarantees of adequate technical and organizational measures for the processing."\(^{58}\)

vi. Sensitive Data

The sixth principle of the Directive requires that additional protections be applied to "sensitive data, data used for marketing purposes, or data subject to automated processing."\(^{59}\) As stated earlier, sensitive data is personal data that discloses "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and . . . health or sex life."\(^{60}\)

Data of this type may only be processed "if the data subject gives 'explicit consent' to processing."\(^{61}\) Without this explicit consent, processing may occur:


\(^{55}\) *Id.* at 963.

\(^{56}\) *Id.*

\(^{57}\) *Id.*

\(^{58}\) *Id.*

\(^{59}\) *Id.* at 959.

\(^{60}\) *Id.* at 965.

\(^{61}\) *Id.*
only if it is necessary to carry out the obligations and rights of the controller as authorized by national law; to protect the vital interests of the data subject; if the data have been made public by the data subject; if the processing is carried out in the course of legitimate activities by a non-profit-seeking body; or to establish, exercise, or defend legal claims.62

vii. Transfer

The transfer principle encompasses the requirements for transferring personal data to a third country. A third country is a term used in legislation to define countries outside of the EU.63 Article 25 of the EU Directive indicates that the European Commission ("Commission") may decide, upon a majority vote of approval from the member states, to ban "all data transfers to a third country, including the United States, if the Commission finds that the third country does not ensure 'an adequate level of protection' of data privacy rights."64

This transfer restriction guarantees that controllers sending data abroad for processing will not undermine the level of protection in the Community.65 Examples of countries that are considered to have an "adequate" level of protection include Canada, New Zealand, and the United States only under a Safe-Harbor Certification (discussed in Part III).66

viii. Remedies, Liability, and Sanctions

The eighth and final principle of the Directive encompasses the remedies afforded to data subjects, a data controller’s liability, and sanctions imposed on the data controller for violation.67 Article 22 indicates that member states shall provide each individual with a judicial remedy for any breach of the rights guaranteed to that individual by the national law applicable to the processing.68 Furthermore, the Directive requires that member states entitle each data subject to compensation from the data controller for any damage suffered as a result of an unlawful processing operation.69 However, the controller may be exempt from this liability if it proves that it was not responsible for the unlawful processing.70 Finally, the

62 Id.
66 Id.
67 Boyd, supra note 27, at 988.
68 See id. at 965.
69 Id.
70 Id.
Directive indicates that member states shall adopt suitable measures to ensure the full implementation and enforcement of the Directive provisions, and impose sanctions in cases of infringement.\textsuperscript{71}

The Directive provides the EU with a foundation highlighting the basic requirements for protecting individual data. However, with today's growing digital advancements, having a body of law encompassing solely the basics, is not enough. Thus, reform was needed by the Commission, which led to the development of the General Data Protection Regulation.

**B. THE GENERAL DATA PROTECTION REGULATION**

The Commission's proposed Regulation remedies two main problems. First, the Directive's principles do not sufficiently address rapidly progressing technological advancements, "especially the growth of Internet-based business services."\textsuperscript{72} Second, "previous EU and national regulations created a patchwork of rules" that lacked uniformity, which hampered business growth and "did not protect individual privacy sufficiently."\textsuperscript{73} Regulation was necessary to create a more consistent, steady structure of laws that apply the same data protection to all facets of EU activity.\textsuperscript{74} Many of the provisions of the Regulation have been adopted from the Directive, with an eye towards "strengthening consumer rights and promoting efficiency."\textsuperscript{75} The differences between the Directive and the Regulation are increased harmonization, more user control, increased data controller accountability, and relaxed transfer restrictions to ensure trans-border data flow.

1. **Procedural Differences**

A directive is defined as "a legislative act which sets out a goal that all EU countries must achieve."\textsuperscript{76} However, it is up to the individual countries to decide how the goals are achieved. A directive includes a set of orders listing objectives to be completed and is directed toward national governments, who must then take action to incorporate the orders into national law.\textsuperscript{77}

On the contrary, a regulation is defined as a "binding legislative act that must be applied in its entirety across the EU."\textsuperscript{78} Many data protection regimes in the EU are moving towards participatory control mechanisms,

\textsuperscript{71} See id at 965-66
\textsuperscript{73} Id.
\textsuperscript{74} Id.
\textsuperscript{75} Id. at 631.
\textsuperscript{76} Legal framework: General Data Protection Regulation (EU), ADMINISTRATIVE DATA RESEARCH NETWORK (April 2016), https://adrn.ac.uk/protection-privacy/legal/eu/.
\textsuperscript{77} Lee A. Bygrave, Privacy and Data Protection in an International Perspective, 56 SCANDINAVIAN STUD. L. 165, 182 (2010).
\textsuperscript{78} Legal framework: General Data Protection Regulation (EU), supra note 76.
which aim to regulate citizens directly, rather than through data protection agencies.  

2. Increased Harmonization and Consistency

Enforcement of the Directive depends on each member state, resulting in an inconsistent and highly complex application, which hampers business growth and leaves many individuals under-protected. Commissioner Viviane Reding explained at a convention in Brussels, "Take those 60 pages and multiply by 27 member states, and you'll get an idea of what the term "regulatory complexity" means in practice." Reding, who revealed the new Regulation draft in 2012, said the objective was to "replace that complexity with a single ninety-one-article law" that incorporates all of Europe: "One continent, one law", in the interest of simplicity and opening a market. A single set of rules on data protection, valid across the EU, would make it easier for companies to know and understand the rules.

Increased harmonization is the reasoning behind the Regulation’s proposed notion of a “One-Stop-Shop.” Under the EU Data Protection Directive, organizations are required to notify the DPAs in each member state in which they operate, wasting their resources and time and those of the DPAs. These unnecessary administrative burdens are eradicated under the Regulation. “In the new regime, organizations would only have to deal with a single national data protection authority in the EU country where they have their main establishment.” Likewise, people would be able to refer to the data protection authority in their country, even when a company based outside the EU processes their data.

The “one-stop-shop” principle is a significant component of the harmonization of the EU legal agenda for data protection. The Commission proposed the concept in order to, increase the steady application, provide legal certainty and reduce excessive organizational burden for data controllers and data processors that have a presence in

79 Id. at 190.
81 Id. at 270. (talking about the twelve page long Directive being implemented in Germany with sixty pages).
82 Id.
85 Id. at 635.
86 GILBERT, supra note 88, at 817—818.
87 Id. at 817.
88 See ROTENBERG & JACOBS, supra note 89.
more than one member state. It is important to enable organizations to deal with only one supervisor instead of 28 national regulators, hence the name “one-stop-shop.”

3. More User Control

While the Directive provides data controllers and data processors with the most control over data, the Regulation does the exact opposite and gives data subjects maximum control. It seems that adopting the Regulation’s approach to control distribution is more justified, since, after all, it is the subject’s personal data, and not the controller’s that is being collected.

i. More Stringent Consent Requirements

One of the significant differences between the Directive and the Regulation is the strengthened consent notion. Currently under the Directive, there is only a requirement for implied consent. For example, in many member states, “an individual who uses a website is often assumed to have agreed to the privacy policy of that website,” thus implying his or her consent.

Under the Regulation, when consent is considered the legitimate purpose for processing, it will have to be “specific, informed, and explicit.” The controller bears the burden of demonstrating that the data subjects’ consented to the processing of their personal data for identified purposes. For corporations, this means they may be forced to discover means of keeping consent records “from their customers, users, visitors and other data subjects, or will be forced to ask for this consent each time the company receives any data.”

Though the additional notion of “explicit consent” seems stringent, for web-based services, the Regulation is flexible enough to be satisfied with a clear affirmative action, such as the checking or unchecking of a box.

89 See supra text accompanying note 93.
90 See supra text accompanying note 93.
93 See ROTTENBERG & JACOBS, supra note 96.
95 Id. (emphasis added).
96 Id.
97 Id.
However, "consent is not valid where there is an imbalance between the data subject and the [data] controller," such as in an employment context. With a stronger consent requirement, controllers will be forced to take more responsibility, whilst obtaining personal data of individuals, and subjects are in turn provided with more control over their personal data.

ii. Expanded Right to Object and Right to Erasure

The Directive contains a right to object to the processing of personal data. Article 19 of the Regulation would provide this right, but the "burden of proof would switch to the data controller, while it is currently on the data subject." Under the Regulation:

the data subjects would have the right to object at any time to the processing of personal data that has been made without their consent allegedly for (i) the protection of their vital interests, (ii) the performance of a task carried out in the public interest or in the exercise of official authority vested in the [data] controller, or (iii) the legitimate interests of the [data] controller.

The controller has to "demonstrate that there are compelling legitimate grounds for the processing that override the interests or fundamental rights and freedoms of the data subject." In general, the Regulation "expands the right to object and shifts the burden to justify processing to the data controller."

The right to erasure, originally in Article 12(b) of the Directive, would be significantly strengthened. In the current regime, individuals may obtain the erasure of their data only in limited circumstances. Through stronger rights to erasure, the Regulation establishes a "right to be forgotten" under which an individual will be able to demand that organizations erase records of their personal information where "no
legitimate reason" for the data to be retained exists.\(^ {107} \) If a data controller stores personal data, it should consider the legitimate grounds for its retention — it will be the data controller’s burden to prove that legitimate grounds outweigh the interests of the data subject.\(^ {108} \)

Furthermore, the Regulation adds a “limiting qualification: Controllers may only pursue legitimate interests ‘which meet the reasonable expectations of the data subject based on his or her relationship with the controller.’”\(^ {109} \) Additionally, the data controller responsible for the disclosure of personal data into the public realm has to “inform third parties of the data subject’s request to erase any links to the personal data and any copy or replication of the personal data.”\(^ {110} \)

4. More Accountability/ Responsibility for Data Controller

Parallel to the Directive, the Regulation affects all data controllers “based in the EU or which offer services and products to individuals based in the EU.”\(^ {111} \) However, unlike the Directive, the Regulation shifts the burden of accountability and responsibility from data subjects to data controllers.\(^ {112} \) As a result, data controllers will not only have to comply with substantive principles and data subject’s rights, but also take all appropriate measures to ensure compliance, and to verify and demonstrate that those measures exist and continue to be effective.\(^ {113} \) A data controller’s additional responsibilities include “conducting privacy impact assessments, . . . comply with individual requests to exercise their ‘right to be forgotten,’ and to notify [DPAs] and individuals in the event of a security breach.”\(^ {114} \)

5. Increased Supervision and Enforcement

In addition to payment for damages undergone by data subjects, violating entities may be subject to “a fine up to 100,000,000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater.”\(^ {115} \)

\(^{107}\) Id. at 632—633.

\(^{108}\) MITCHELL-REKRUT, supra note 109.

\(^{109}\) See supra text accompanying note 113.


\(^{112}\) Id. at 632.

\(^{113}\) GILBERT, supra note 115, at 819.

\(^{114}\) See supra text accompanying note 118.

Furthermore, Articles 35 through 37 of the Regulation "require data controllers and data processors to appoint a data protection officer." This rule applies to the "public sector, and, in the private sector, to enterprises employing more than 250 employees, or where the core activities of the controller or processor consist of processing operations that require regular and systematic monitoring of the data subjects."

With the currently rapid rate of technological advancements, the GDPR is sorely needed. When implemented, the Regulation will reveal the uninterrupted integration of the European member countries, the progress of contemporary technology and business practices, and the insights derived from the post-War efforts to preserve the fundamental human right to privacy.

III. EUROPEAN DATA PRIVACY REGULATIONS EFFECT ON THE U.S.

The current U.S. environment is very friendly to organizations collecting data on individuals with limited exceptions when the data has certain properties (health and financial records). "Many businesses and industries rely on the regulatory environment continuing to favor companies." The EU's chief concern with data protection in the United States is the absence of a "horizontal law" similar to the Directive, "which would cover any sort of processing of personal data." Despite the lack of over-arching data protection laws, "the United States does not, to paint matters in broad strokes, simply value privacy less than Europe does. For historical and cultural reasons, the concept has nonetheless evolved differently on either side of the Atlantic."

A. DIFFERENCES

Legal protection of personal data in the United States "falls short in significant respects of the protection levels in many other countries, especially the member states of the [EU]. . . . This variation, though, need

---


117 Id.


120 Id. at 969.

121 Id. at 968.

not reflect differences between countries’ respective levels of support for privacy.”\textsuperscript{123} Rather, it can be partially attributable to historical differences. In essence, the wide-ranging governmental nature of data protection regulation in Europe undeniably is a reflection of sufferings from fairly recent, personal experience of totalitarian oppression, i.e., World War II. In contrast, in North America, the scarcity of first-hand domestic experiences of totalitarian oppression tends to make the countries’ regulatory policies in the field comparatively lenient.\textsuperscript{124}

B. SAFE-HARBOR INVALIDATION AND AVAILABLE ALTERNATIVES

The U.S.’s response to the 1995 Directive is embodied in the former International Safe Harbor Privacy Principles (“Safe-Harbor”), an initiative intended to resolve the trade conflict by allowing U.S. companies to self-certify that they meet an "adequacy" requirement for E.U. privacy protection.\textsuperscript{125} The Safe-Harbor permitted the flow of personal data from the EU to U.S.-based companies, who willingly agreed to abide by a set of “fair information” principles that were loosely based on the EU Directive.\textsuperscript{126}

On October 6th, 2015 the European Court of Justice (“ECJ”) invalidated the Safe Harbor, leaving U.S. companies scrambling for alternatives in order to continue data flows from their EU counterparts.\textsuperscript{127} Max Schrems, an Australian citizen and avid Facebook user, lodged a complaint with the Irish DPA pointing out the insufficiencies of U.S. laws and practices in protecting individuals from U.S. government surveillance of data transferred to that country.\textsuperscript{128} In what would come to be known as the ‘Schrems’ decision, the ECJ determined that the Safe Harbor no longer served as a sufficient method of ensuring the protection of data regarding EU citizens.\textsuperscript{129} Consequently, the Commission and U.S. authorities began negotiations to form a new, adequate agreement. On February 2, 2016, the Commission announced the creation of a “Safe Harbor 2.0” giving it the critiqued name of the “EU-US Privacy Shield (“Shield”).\textsuperscript{130}

\begin{itemize}
  \item \textsuperscript{123} Lee A. Bygrave, \textit{Privacy and Data Protection in an International Perspective}, 56 \textit{SCANDINAVIAN STUD. L.} 165, 176 (2010).
  \item \textsuperscript{124} See id.
  \item \textsuperscript{126} Id. at 337—39.
  \item \textsuperscript{128} See id. at 262.
  \item \textsuperscript{129} See id. at 270.
\end{itemize}
The Commission has done no more than merely announce the creation of the Shield. The agreement still needs to adopt a formal "adequacy decision," which is impossible without consultation and approval from the Article 29 Working Party and others in the Commission. From the little information we have about the Shield, it is evident that it encompasses stronger restrictions on U.S. mass surveillance, effective redress options for EU citizens, increased obligations to maintain transparency between U.S. companies and data subjects, and binding assurances from the U.S. authorities—all critical elements not accounted for in the former Safe Harbor.

As a result of uncertainty, it is necessary for U.S. companies to implement alternatives in order to maintain their data flow. Standard contractual clauses and binding corporate rules, two alternatives to the Safe Harbor, were always an option for companies, and are still deemed sufficient for transatlantic data flow. Thus, in the midst of the developing uncertainty, U.S. companies are left with two options: (i) implement one of the alternatives, or (ii) take a risk and await the Shield’s approval.

1. Standard Contractual Clauses

Standard contractual clauses, more commonly referred to as model clauses, are four sets of contract clauses that have been pre-approved by the Commission for the purpose of establishing safeguards in the transfer of personal data between the EU and U.S. The Commission has deemed model clauses to be the main fallback for companies, primarily because they can be implemented quickly and can be used for intracompany transfers or transfers to third parties.

However, model clauses are not always fit for purpose where a more complex web of processing exists, especially in a world of advancing cloud-based technology. Additionally, for a larger company, implementing model clauses is time-consuming and rather ineffective as a result of its larger customer-base and vendor-base (each customer and vendor would need to sign and return the model clauses). Consequently, larger, more developed corporations tend to turn to the only other approved alternative to maintain their data flow, binding corporate rules.

131 Id.
132 Id.
134 Id. at 272.
136 See id.
137 See id.
2. Binging Corporate Rules

Binding corporate rules are guidelines developed and adopted internally by a multinational company, similar to a Code of Conduct or Best Practices Guide. These guidelines define a company's global policy regarding the transfer of personal data within the same corporate group to entities in countries that do not maintain an adequate level of protection.\(^\text{138}\)

Once the Commission and DPAs of member states approve a company's binding corporate rules, the company is able to transfer data freely between its entities without having to worry about signing a contract for every single transfer, as opposed to the model clauses alternative.\(^\text{139}\) Binding corporate rules harmonize data protection practices amongst a group and also generally embed the significance of data protection in a company's culture.\(^\text{140}\)

However, there are two reasons many companies shy away from implementing binding corporate rules: (i) they are expensive and (ii) approval can take up to 18 months.\(^\text{141}\) It is for these reasons that binding corporate rules are more appealing to larger organizations such as Intel, eBay and JPMorgan Chase, which have recently received approval for and finalized their binding corporate rules.\(^\text{142}\)

The real trouble lies for the medium-sized companies that are too large to sign contractual clauses with each customer and supplier, but are too small to afford the implementation of binding corporate rules. Thus, these companies are left to take the intimidating risk of awaiting guidance from the Commission. Hopefully, the development of the Shield is one relatively small step in the right direction.

Though the United States may fall behind in the race to have the most effective data protection regime, a lack of horizontal, federal data protection regulations may be in its favor.\(^\text{143}\) "In the words of Google CEO Eric Schmidt: 'High tech runs three times faster than normal businesses. And the government runs three times slower than normal businesses. So we have a nine-times gap,' and the only way to fix the problem is 'to make sure that the government does not get in the way and slow things down.'


\(^{140}\) Id.

\(^{141}\) Id.

\(^{142}\) See McLellan, supra note 140.

down.”  

Essentially, Schmidt believes that regulation hampers real innovation.  Keeping that scrutiny in mind, it becomes a question as to whether widespread regulation will actually be achievable in the future, considering the “tension with innovation, as well as the significant influence of companies that have a reason to oppose it.”

CONCLUSION

It seems that the “age of privacy as we knew it in the time of Warren, Brandeis, and their Right to Privacy—one still characterized by secluded spaces in which we can reasonably expect to be let alone—will soon” completely diminish.  In an interview on surveillance drones in the city, New York City Mayor, Michael Bloomberg, stated, “‘You can’t keep the tides from coming in.”  Our personal data is everywhere, and there is little that individuals can do to keep it protected and controlled.

Directive 95/46/EC has been a major “driving force in the adoption of data protection laws throughout the world.” Numerous countries outside of the EU, such as “Switzerland, Peru, Uruguay, Morocco, Tunisia, or the Dubai Emirate (in the Dubai International Financial District) have adopted data protection laws that closely follow the terms of Directive 95/46/EC.”

With the new General Data Protection Regulation, the European Union has taken the foundational principles from the Directive 95/46/EC, and reframed that body of law to achieve the goal of increased data protection. If the current provisions survive the final draft, the Regulation will increase the rights of individuals and the power of the authorities. While the Regulation would create additional responsibilities and accountability requirements for organizations, the adoption of a single rule throughout the EU will help streamline the governance of information, procedures, record keeping, and other requirements for companies.

With regard to data protection in the United States, a few fundamental questions remain unanswered: Is the United States going to adopt the European mindset of privacy as dignity and autonomy, and will the American people demand legislation that gives them more control of their data? Or, will privacy become obsolescent in a future in where they willingly yield, in the interest of accessibility and connectedness, the

---

144 Id. at 281.
145 Id.
146 Id.
147 Id. at 286.
148 Id.
150 Id.
expectation that they can ever, anywhere, truly be “let-alone?”  