Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 12 | Issue 1 Article 21

12-12-2017

WHAT ABOUT SMALL BUSINESSES? THE GDPR AND ITS CONSEQUENCES FOR SMALL U.S.-BASED COMPANIES

Craig McAllister

WHAT ABOUT SMALL BUSINESSES? THE GDPR AND ITS CONSEQUENCES FOR SMALL, U.S.-BASED COMPANIES

ABSTRACT

Fast-approaching changes to European data privacy law will have consequences around the globe. Historically, despite having dramatically different approaches to data privacy and data protection, the European Union and the United States developed a framework to ensure that the high-speed freeway that is transatlantic data transfer moved uninterrupted. That framework was overturned in the wake of revelations regarding U.S. surveillance practices, and amidst skepticism that the United States did not adequately protect personal data. Further, the European Union enacted the General Data Protection Regulation (GDPR), a sweeping overhaul of the legal data protection landscape that will take effect in May 2018. The law will impact all companies that process data relating to EU citizens, which will include many U.S.-based ventures, big and small. And while many of the world's large technology companies will have feasible methods of quickly complying with the law, small ventures will not have it so easy. This Note explores the legal landscape of data privacy, discusses what led to the current dynamic between the European Union and the United States, and explains why the current methods for small, U.S.-based ventures attempting to comply with the GDPR are not operationally feasible. This Note then proposes both a short-term and long-term solution to address the significant challenge that small companies in the United States currently face.

INTRODUCTION

Edward Snowden's unveiling of the extent and scope of U.S. surveillance practices caused economic ripples that continue to emanate today.[1] Globalization and the rise of the internet ushered in a new era in which data is collected at an unprecedented pace and transferred all over the globe on a daily basis. Julie Brill, former Federal Trade Commission (FTC) Commissioner, put it best when she said "[t]he Internet has become today's global trade route, and personal data is one of its major currencies."[2] Indeed, the sheer volume of data that is collected and processed in today's economy

1. *See* Klint Finley, *Thank (Or Blame) Snowden for Europe's Big Privacy Ruling,* WIRED (Oct. 6, 2015, 9:06 PM), https://www.wired.com/2015/10/tech-companies-can-blame-snowden-data-privacy-decision/ (explaining that the overruling of Safe Harbor, which occurred in response to arguments relying on information about the NSA's practices leaked by Snowden in 2013, would create headaches for U.S. technology companies).

2. Julie Brill, *Strengthening International Ties Can Support Increased Convergence of Privacy Regimes*, 2 EUR. DATA PROTECTION L. REV. 151, 151 (2016).

is remarkable.[3] While this trend has created growth opportunities for private enterprises, it has also created new risks in the areas of privacy and cybersecurity.

No event shed more light on these new risks than Edward Snowden's revelations regarding the National Security Agency's (NSA) surveillance practices.[4] American data protection laws came under increased scrutiny as an immediate result of Snowden's actions.[5] Around the world, and particularly in Europe, an attitude that perhaps the United States was not adequately protecting consumers' data privacy became commonplace.[6] This movement culminated in a 2015 decision by the European Court of Justice (CJEU) that invalidated the Safe Harbor Framework (Safe Harbor) between the United States and the European Union.[7] Previously, companies in the United States relied on Safe Harbor to lawfully transfer the personal data of EU citizens to the United States. Safe Harbor was necessary under EU data protection law because EU officials deemed the data protection laws of the United States to be inadequate.[8] Without Safe Harbor, companies based in the United States are in need of a new legal solution for transatlantic data transfer.

Meanwhile, Europe was busy creating a new data protection framework of its own.[9] After four years of deliberation, the European Union adopted the General Data Protection Regulation (GDPR) as its new data protection law.[10] The GDPR, set to go into effect in 2018, will replace the current EU data privacy law and apply directly in each member state.[11] The GDPR will provide a unified body of data protection law and a more harmonized administration,[12] while also introducing an entirely new set of obligations for companies looking to transfer personal data outside of the European Union.[13]

3. *See* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 4 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

4. *See* Finley, *supra* note 1.

5. *See* Courtney M. Bowman, *US-EU Safe Harbor Invalidated: What Now?*, THE NAT'L L. REV. (Oct. 7, 2015), http://www.natlawreview.com/article/us-eu-safe-harbor-invalidated-what-now.

6. *See* Angelique Carson, *Safe Harbor-Compliant Companies Seeking Contracts: Facing an Uphill Battle in the EU*, THE INT'L ASS'N OF PRIVACY PROF.: THE PRIVACY ADVISOR (May 20, 2014), https://iapp.org/news/a/safe-harbor-compliant-companies-seeking-contracts-facing-an-uphill-battle-i/.

7. Bowman, *supra* note 5.

8. *Id.*

9. *See* ALLEN & OVERY, THE EU GENERAL DATA PROTECTION REGULATION (2016), http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf.

10. *See id.* at 2.

11. *See id.*

12. Commission Regulation 2016/679, 2016 O.J. (L 119) 1 [hereinafter Commission Regulation].

13. *See* ALLEN & OVERY, *supra* note 9, at 3.

Further, the GDPR largely came about as a result of public debate around how large technology companies handle personal data, and the practice of domestic governments monitoring such data for investigative purposes.[14] Paradoxically, many of the U.S.-based companies that relied on Safe Harbor were small and medium sized enterprises.[15] Accordingly, much uncertainty remains with respect to how these small technology companies should operationalize their data transfers in light of recent regulatory developments.[16]

Part I of this Note provides a brief historical overview of European data privacy law and how it has traditionally differed from that of the United States. Part II discusses the GDPR and what it will mean for companies looking to compete in the global digital economy. Part III addresses the current options in place for companies—both large and small—looking to lawfully transfer personal data out of the European Union and into a third country, and explains why these methods are not operationally feasible for small ventures. Finally, Part IV proposes both a short-term and a long-term solution. In the near-term, this Note proposes that Congress enact a federal tax credit for small, U.S.-based companies looking to have a digital footprint in the European Union. As a more lasting solution, this Note recommends that Congress pass data privacy legislation to address growing privacy concerns in the United States and abroad, and to streamline transatlantic data transfers by bringing data protection laws in the United States to the level observed in the European Union.

I. DATA PRIVACY LAW IN EUROPE

Privacy is seen as a fundamental right in Europe, and includes the right to protection with respect to the processing of personal data.[17] Consequentially, European culture espouses a greater expectation of privacy than what exists in the United States.[18] Traditionally, the law protecting this

14. *See* Glyn Moody, "*Privacy Shield" Proposed to Replace US-EU Safe Harbor, Faces Skepticism*, ARS TECHNICA (Feb. 29, 2016, 9:04 AM), http://arstechnica.com/tech-policy/2016/02/privacy-shield-doomed-from-get-go-nsa-bulk-surveillance-waved-through/.

15. *See* Julie Brill, U.S. Fed. Trade Comm'r, Two-Way Street: U.S.-EU Parallels Under the General Data Protection Regulation, Keynote Address at Ghostery/Hogan Lovells Data Privacy Day 9 (Jan. 21, 2016) (transcript available at https://www.ftc.gov/system/files/documents/public_statements/910663/160121hoganghostery_dpd.pdf).

16. *See U.S.-EU Safe Harbor Framework Before the H. Energy and Trade Subcomm. on Com, Mfg. and Trade and Commerce & Tech.* (Nov. 3, 2015) [hereinafter Testimony of Edward Dean] (testimony of Edward M. Dean, Deputy Assistant Sec'y for Serv., Int'l Trade Admin., U.S. Dep't of Commerce), *available at* http://docs.house.gov/meetings/IF/IF16/20151103/104148/HHRG-114-IF16-20151103-SD012.pdf.

17. *See Article 29 Data Protection Working Party Opinion 8/2014 on the Recent Developments on the Internet of Things*, at 3 (WP223) (Sept. 16, 2014).

18. *See* Phil Lee, *How Do EU and US Privacy Regimes Compare?* FIELDFISHER: PRIVACY, SECURITY, AND INFO. L. (Mar. 5, 2014, 10:29 PM), http://privacylawblog.fieldfisher.com/2014/how-do-eu-and-us-privacy-regimes-compare/.

right in Europe was the 1995 Directive (the Directive).[19] Among other things, the Directive forbade the transfer of personal data to a country outside the European Economic Area (EEA) unless that country had adequate protection measures in place.[20] Because of the stark difference in privacy protection laws between Europe and the United States, European Data Protection Authorities (DPA) deemed the United States' laws to be inadequate.[21]

While this may appear to have constituted a major obstacle to the functioning of the global digital economy, the United States and the European Union overcame this by forming the Safe Harbor Pact.[22] Under Safe Harbor, American companies could self-certify that they complied with the Safe Harbor data protection principles.[23] A self-certification essentially meant that the company publically attested that it complied with certain European privacy standards.[24] Once a company self-certified, it could transfer personal data from the EEA to the United States without running afoul of the Directive.[25] Safe Harbor, therefore, provided U.S.-based companies with a relatively accessible method of ensuring compliance with the more stringent privacy laws of the EEA while also enabling the continuous flow of personal data from the EEA to the United States.[26] As of 2015, approximately 4,400 companies participated in the Safe Harbor.[27]

In a single decision in 2015, the CJEU changed all of that.[28] In *Schrems v. Data Protection Commissioner*, the CJEU ruled that national regulators in the European Union had the authority to override the fifteen year-old framework, as it violated the privacy rights of Europeans by exposing them to unlawful surveillance by the U.S. government.[29] The case began in 2013 when Max Schrems, Austrian privacy advocate, filed a complaint regarding

19. *See generally* Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

20. *See* Bowman, *supra* note 5.

21. *See* Peter Sayer, *EU Court Rules US Privacy Protection Inadequate*, INFOWORLD (Oct. 6, 2015), http://www.infoworld.com/article/2988851/privacy/eu-court-rules-us-privacy-protection-inadequate.html.

22. *See* Bowman, *supra* note 5.

23. *See id.* These principles included notice, choice, onward transfer, security, data integrity, access, and enforcement. *See* PRIVACYTRUST, SAFE HARBOR CERTIFICATION, https://www.privacytrust.com/guidance/safe_harbor.html (last visited Nov. 11, 2017).

24. *See Bowman*, *supra* note 5.

25. *See id.*

26. *See id.*

27. Testimony of Edward Dean, *supra* note 16. Dean described Safe Harbor as "a cornerstone of the transatlantic digital economy enabling growth and innovation in the United States and in Europe." *Id.*

28. *See generally* Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 1-1, *available at* http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN.

29. *See id.*

Facebook's compliance with EU data privacy laws.[30] The complaint, filed with the Irish Data Protection Commissioner (DPC),[31] claimed that revelations brought to light by former NSA contractor, Edward Snowden, showed that Facebook was not sufficiently protecting users' data, since the data was subject to mass surveillance in the United States.[32] Procedurally, Mr. Schrems was venturing into uncharted territory.[33] The Irish DPC initially rejected the complaint on grounds that it was bound by the Safe Harbor Pact.[34] Mr. Schrems then appealed to an Irish Court, which requested an answer from the CJEU on whether a national regulator had the authority to disregard a pact that applies across the entire European Union.[35] The court held that the Irish DPC not only had the authority to investigate, but that it had a duty to do so.[36]

The result was sweeping.[37] To Mr. Schrems, the decision was a victory for privacy.[38] "The message is clear," he said, "that mass surveillance isn't possible against fundamental rights in Europe."[39] Experts disagree, however, on the validity of the premise upon which the court's decision relied.[40] According to Edward M. Dean, former Deputy Assistant Secretary for Services in the International Trade Administration of the Department of Commerce, Safe Harbor was the unfortunate scapegoat of broader geopolitical revelations with regard to surveillance.[41] Mr. Dean noted that "[s]ince Safe Harbor had become linked to the surveillance disclosures, it became a target for continued criticism largely based on misunderstanding and false assumptions about its purpose and operation and the important privacy benefits it provided."[42] At the core of the criticism, Mr. Dean said, were "false accusations that the United States was engaged in 'mass, indiscriminate surveillance' of the data transferred to the United States under Safe Harbor."[43]

Regardless of whether the criticism was well-founded, the implications of the court's decision were significant.[44] Billions of dollars of trade in the online advertising industry relied upon Safe Harbor for its compliance with

30. *See* Natalia Drozdiak and Sam Schechner, *EU Court Says Data-Transfer Pact with U.S. Violates Privacy*, WALL ST. J. (Oct. 6, 2015), http://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361.
31. Sayer, *supra* note 21.
32. Drozdiak & Schechner, *supra* note 30.
33. Sayer, *supra* note 21.
34. Drozdiak & Schechner, *supra* note 30.
35. *Id.*
36. *See id.*
37. *See id.*
38. *See* Sayer, *supra* note 21.
39. Drozdiak & Schechner, *supra* note 30.
40. *See* Testimony of Edward Dean, *supra* note 16; *see also* Carson, *supra* note 6.
41. *See* Testimony of Edward Dean, *supra* note 16.
42. *Id.* at 2.
43. *Id.*
44. *See* Sayer, *supra* note 21; *see also* Drozdiak & Schechner, *supra* note 30.

EU privacy law.[45] Furthermore, myriad companies relied on Safe Harbor when transferring human-resource related data about European employees.[46] "Losing Safe Harbor would be hugely disruptive to all sorts of businesses," said one official at a U.S.-based technology company that provides cloud services.[47] Similarly, former Secretary of Commerce Penny Pritzker commented that "we are deeply disappointed in [the Safe Harbor decision]," as it "puts at risk the thriving transatlantic digital economy."[48]

Many feel that the decision will hurt small businesses most, since they do not have the legal resources necessary to adopt other data-transfer methods, or defend against potential complaints that may stem from such methods.[49] "We expect that a suspension of Safe Harbor will negatively impact Europe's economy, [and] hurt small and medium-sized enterprises, and the consumers who use their services, the most," said Christian Borggreen, International Policy Director for the Computer & Communications Industry Association.[50] Similarly, Mike Weston, CEO of Data Science Consultancy Profusion, described the development as bad news for small and medium-sized companies transferring data from the European Union to the United States, as "American companies are going to have to restructure how they manage, store and use data in Europe and this will take a lot of time and money."[51] Mr. Dean's testimony before the House Energy and Commerce Subcommittees on Commerce, Manufacturing and Trade and Communications & Technology bolstered this sentiment.[52] Mr. Dean described a specific instance in which a small enterprise was hurt by the suspension of Safe Harbor:

> A small company, which provides support services relevant to clinical research trials, has already lost significant business across Europe. The company's clients are suspending and shutting down projects, while its EU-based main competitor has reached out to other existing clients recommending they switch providers in light of the court ruling.[53]

Cases like this raise the question of how a small, digitally-oriented, U.S.-based enterprise can achieve a global footprint in light of these recent legal developments.

45. Drozdiak & Schechner, *supra* note 30.
46. *Id.*
47. *Id.*
48. *Id.*
49. *See id.*
50. *Id.*
51. Sayer, *supra* note 21.
52. *See* Testimony of Edward Dean, *supra* note 16, at 3–4.
53. *Id.*

II. THE GENERAL DATA PROTECTION REGULATION: AN AGGRESSIVE STEP FORWARD FROM THE DIRECTIVE

After four years of discussion, the European Commission adopted the GDPR.[54] The GDPR will replace the Directive when it goes into effect on May 25, 2018.[55] Companies that process personal data would be wise to take this time to review the GDPR in detail to ensure that their organizations are prepared for the significant impact that the law will surely have.[56]

The European Commission pushed the GDPR forward as an overall update to EU data protection law for several reasons.[57] First, the GDPR will provide an overall harmonization of data protection laws across the EEA.[58] Under the Directive, enforcement of data protection laws required local implementation of national legislation by each individual member state.[59] Under the GDPR, the regulations will take immediate effect in each individual member state, without the need for states to enact national legislation.[60] This method of implementation will likely lead to a more uniform, turnkey application of the GDPR across the EEA.[61] Along those same lines, the GDPR will create a "One Stop Shop," a term adopted by the European Commission to describe an improvement to what proved to be a frustrating component of the Directive.[62] Under the Directive, companies could be subject to enforcement by any of the individual member state DPAs, each of whom could have potentially taken a varying approach to enforcement of the Directive and its principles.[63] With the GDPR, companies will have a single supervisory authority based on the company's location or, if the company has multiple locations, its "main establishment."[64] This will likely reduce the headache and confusion companies experienced when corresponding with DPAs across the EEA.[65]

Additionally, and perhaps more importantly for companies, the GDPR will have an extra-territorial effect.[66] Currently, under the Directive, data

54. *See* ALLEN & OVERY, *supra* note 9, at 2.
55. *Id.*
56. *See id.* at 9.
57. *See id.* at 2.
58. *See* § 11:2 PROPOSED GEN. DATA PROTECTION REG., 2 DATA SEC. & PRIVACY LAW § 11:2 (Westlaw through 2017) [hereinafter PROPOSED DATA PROTECTION REG.].
59. *Id.*
60. *Id.*
61. *See id.*
62. *Id.*
63. *See id.*
64. *See id.* The idea is that companies will only have to correspond with one supervisory authority, and this will be the supervisory authority in the member state in which the company has its "main establishment." The main establishment is wherever the most processing activities take place. *Id.* at 2. For example, if a company stations the majority of its engineers in one location, this will likely be the company's main establishment.
65. *See id.*
66. Commission Regulation, *supra* note 12, at 32–33 ("Territorial scope"); *see also* PROPOSED DATA PROTECTION REG., *supra* note 58.

controllers that are established in the European Union or make use of data processing equipment located in the European Union are subject to the data protection laws of the Directive.[67] The GDPR, however, will apply to data controllers and processors *outside* the European Union whose processing activities relate to (1) the offering of goods or services to data subjects in the European Union, or (2) the monitoring of their behavior in the European Union.[68] The GDPR provides details with regard to what business activities fall under this provision, stating that the offering of goods or services, in order to be subject to the GDPR, must be more than simply providing access to a website or email address.[69] Such goods or services might take the form of using the language or currency generally used in one or more member states with the possibility of purchasing goods or services there, or monitoring the behavior of data subjects in member states.[70] Moreover, this monitoring of behavior provision applies to situations in which data subjects are tracked on the internet by methods that apply a profile to the subject in order to make decisions and predictions about the subject's personal preferences.[71] The result will be that many non-EU businesses—and in particular internet companies—will now be subject to the GDPR, a break from the current situation under the Directive.[72] The GDPR, therefore, carries sweeping implications for American companies of all sizes looking to process data related to citizens in the EEA in 2018 and beyond.[73]

The changes do not stop there. Not only will the GDPR claim jurisdiction over thousands of non-EU companies, it will also impose a host of new obligations on businesses.[74] First, the GDPR requires that companies generally implement appropriate data protection policies.[75] The GDPR lays out extremely detailed compliance requirements for both data controllers and data processors, and mandates that companies take measures to demonstrate compliance with the law.[76] Additionally, the GDPR introduces the concepts of data protection "by design and by default."[77] This obligates businesses to incorporate privacy and data protection as part of the organization's DNA from the start of any product design process, maintain such an approach throughout the processing activity's life-cycle, and appropriately assess all risks to data protection and privacy before launching new products.[78]

67. PROPOSED DATA PROTECTION REG., *supra* note 58.
68. ALLEN & OVERY, *supra* note 9, at 3.
69. *See* Commission Regulation, *supra* note 12, at para. 23.
70. *See id.* at para. 24.
71. *See* ALLEN & OVERY, *supra* note 9, at 3; *see also* Commission Regulation, *supra* note 12.
72. *See* ALLEN & OVERY, *supra* note 9, at 3.
73. *See* Sayer, *supra* note 21.
74. *See* ALLEN & OVERY, *supra* note 9, at 3.
75. *See* Commission Regulation, *supra* note 12, at 47; *see also* PROPOSED DATA PROTECTION REG., *supra* note 58.
76. *See* PROPOSED DATA PROTECTION REG., *supra* note 58.
77. *Id.*
78. *Id.*

Notwithstanding the time that companies have to prepare for the GDPR, the requirement to update fundamental approaches to product design is daunting, time consuming, and expensive.[79] Roy Smith, the CEO of PrivacyCheq, lamented that "the GDPR will be particularly hard on software-as-a-service[80] (SaaS) legacy products," as they were "put in place without consideration of privacy, encryption, user consent, [and the] right to be forgotten."[81] The effort required to update these products, Smith said, will be akin to that of "changing an engine on a plane in midflight."[82]

Additionally, the GDPR will emphasize the concept of data minimization and the principle of necessity.[83] These concepts will require companies to establish and maintain adequate technical and organizational measures to effectively ensure that, "by default, only personal data which are necessary for each specific purpose of the processing are processed."[84] Along similar lines, the GDPR will also require organizations to maintain significant internal records.[85] The GDPR puts forth a list of data that must be included in these records which, in many cases, is more onerous than the previous requirements for registration under the Directive.[86] Furthermore, the GDPR will require that, in many cases, organizations appoint a Data Protection Officer (DPO) to oversee data protection within the organization and manage compliance with the relevant supervisory authority.[87] The GDPR will also require that companies perform data protection impact assessments where the processing is "likely to result in a high risk to the rights and freedoms" of

79. *See* Sayer, *supra* note 21.

80. Software as a service (SaaS) simply refers to a method of providing programs over the internet as a service. SaaS provides the benefit of simplicity and accessibility, since it frees customers from dealing with complicated software and hardware. *SaaS: Software as a Service*, SALESFORCE, https://www.salesforce.com/saas/ (last visited Aug. 23, 2017).

81. Ricci Dipshan, *The GDPR Reckoning: How the Upcoming Regulation is Already Changing Privacy in Tech*, LEGAL TECH. NEWS (Sept. 21, 2016) https://www.law.com/legaltechnews/almID/1202767963049/.

82. *Id.*

83. *See* Commission Regulation, *supra* note 12, at para. 156 ("[S]afeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation.").

84. *Id.* at art. 25; *see also* PROPOSED DATA PROTECTION REG., *supra* note 58.

85. *See* Commission Regulation, *supra* note 12, at art. 57; *see also* PROPOSED DATA PROTECTION REG., *supra* note 58.

86. *See* PROPOSED DATA PROTECTION REG., *supra* note 58.

87. *See* Commission Regulation, *supra* note 12, at arts. 37–39. Pursuant to Article 37, examples of cases that require the appointment of a DPO include where "the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;" or "the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 [governing the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union members, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation] and personal data relating to criminal convictions and offences referred to in Article 10."

individuals,[88] and companies will be held directly liable under the GDPR for the security of personal data processing activities.[89]

Additionally, consent will become significantly more difficult to use as a justification for processing personal data under the GDPR.[90] Companies would be wise to review the GDPR's language closely to ensure that the data subject's consent is specific, informed, and unambiguous.[91] Furthermore, data controllers must be able to prove that they obtained the requisite consent, and consent will not be valid under the GDPR if a significant imbalance between the parties exists.[92] For example, such an imbalance may exist between an employer and employee if there is an apparent disparity in bargaining power.[93]

Lastly, and perhaps most importantly, the GDPR will significantly increase fines for violations of data protection laws.[94] Fines under the Directive vary based on national law and tend to be relatively low.[95] For example, the maximum fine under the Directive in the United Kingdom is £500,000.[96] Under the GDPR, however, punishment will be uniform throughout the EEA and maximum fines will increase substantially, with the maximum fine increasing to €20 million, or 4% of annual worldwide turnover, whichever is greater.[97]

Given the significant changes to the European data privacy regime, as well as the myriad new obligations under the GDPR, companies must take

---

88. *See id.* at art. 35. Article 35, para. 3 expounds on the meaning of "high risk to the rights and freedoms of natural persons," stating that:

> A data protection impact assessment . . . shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1) [relating to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or a natural person's sex life or sexual orientation] or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.

Id.

89. *See* PROPOSED DATA PROTECTION REG., *supra* note 58.

90. *See id.*

91. *See* Commission Regulation, *supra* note 12, at para. 32.

92. *See id.* at paras. 42–43 ("the controller should be able to demonstrate that the data subject has given consent to the processing operation. . . ." and "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller. . . ."); *see also* PROPOSED DATA PROTECTION REG., *supra* note 58.

93. *See* PROPOSED DATA PROTECTION REG., *supra* note 58.

94. *See id.*

95. *See id.*

96. *See id.*

97. Commission Regulation, *supra* note 12, at art. 83.

preparatory measures now to ensure they are able to comply.[98] For small, U.S.-based enterprises that relied on Safe Harbor under the Directive, the future of data privacy compliance in the European Union remains nebulous.

III. AVAILABLE OPTIONS FOR TRANSATLANTIC DATA TRANSFER UNDER THE GDPR DO NOT ADEQUATELY ADDRESS THE NEEDS OF SMALL COMPANIES

The enhanced territorial reach of the GDPR and the plethora of obligations that will go into effect in 2018 will leave many U.S.-based companies looking for legally sound methods of transferring data out of the European Union. The GDPR allows companies to transfer data out of the EEA if the data is moving to a country with data protection laws that are deemed adequate by the European Commission.[99] The European Commission has not declared the laws of the United States adequate.[100] The result is that companies in the United States that are looking to transfer data out of the EEA will need to transfer by way of appropriate safeguards, as provided by Article 46 of the GDPR.[101] For various reasons, however, the menu of available options for transferring personal data out of the EEA under the GDPR are complex and expensive, and likely not operationally feasible for most small enterprises, and thus the current landscape leaves these companies in a bind.[102]

A. CODES OF CONDUCT

First, companies can lawfully transfer data from the European Union to a third-party country through adherence to an approved code of conduct.[103] To do so, the parties processing or controlling the data must submit to a contract that governs the subject matter and duration of the data processing, the purposes of the processing, and the type of data and categories of data subjects.[104] The code must take into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk for the rights and freedoms of the data subject.[105]

98. *See* Dipshan, *supra* note 81.

99. *See* Anna Myers, *Top 10 Operational Impacts of the GDPR: Part 4 – Cross-Border Data Transfers*, THE INT'L ASS'N OF PRIVACY PROF.: THE PRIVACY ADVISOR (Jan. 19, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/.

100. *See* Bowman, *supra* note 5.

101. *See* Myers, *supra* note 99.

102. FTC Commissioner Julie Brill acknowledged that Standard Contractual Clauses and Binding Corporate Rules are each "expensive, complicated, and may not be appropriate for all data transfers." *See* Boris Segalis & Kathryn Linksy, *FTC Commissioner Julie Brill Comments on EU-US Privacy Shield*, DATA PROTECTION REP. (Feb. 4, 2016), http://www.dataprotectionreport.com/2016/02/ftc-commissioner-julie-brill-comments-on-eu-us-privacy-shield/.

103. *See* Myers, *supra* note 99.

104. *See* Commission Regulation, *supra* note 12, at para. 81.

105. *See id.*

Although binding codes of conduct provide an alternate mechanism to transfer data out of the EEA, utilizing this method is operationally cumbersome.[106] The GDPR claims to take "account of the specific needs of micro, small, and medium-sized enterprises,"[107] and yet, utilizing codes of conduct as a method of transferring data under the GDPR requires companies to appeal directly to supervisory authorities in EU member states.[108] The supervisory authority then gives "an opinion on whether the draft code . . . complies with [the] Regulation."[109] This process could take years, according to Harriet Pearson, a partner at the law firm Hogan Lovells and a former Chief Privacy Officer for IBM.[110] Implicit in the inclusion of this mechanism is the assumption that most codes of conduct will be drafted by trade associations or other organizations representing data processors, and will be written with the many aspects and obligations of the GDPR in mind.[111] Prominent industry trade groups, however, tend to represent large technology companies and, thus, binding codes of conduct as a mechanism for transatlantic data transfer do not help small businesses, since they do not have the legal resources necessary to adopt such an onerous method.[112]

B. STANDARD CONTRACTUAL CLAUSES

A second option for an appropriate safeguard under the GDPR is the use of standard data protection contractual clauses.[113] In essence, companies can use contract language approved by the European Commission or a member state DPA in order to transfer data out of an EU member state and into a country lacking an adequacy status.[114] Companies looking to employ ad hoc contractual clauses must obtain approval from the appropriate supervisory authority prior to doing a deal, thereby making the mechanism less operationally feasible.[115] Furthermore, former FTC Commissioner Julie Brill acknowledged that standard contractual clauses are "expensive, complicated, and may not be appropriate for all data transfers."[116] For small businesses, therefore, standard contractual clauses likely fall short of providing a feasible method of data transfer.

106. *See* Drozdiak & Schechner, *supra* note 30.
107. Commission Regulation, *supra* note 12, at para. 13.
108. *See id.* at art. 40(5).
109. *Id.*
110. *See* Drozdiak & Schechner, *supra* note 30.
111. *See* Myers, *supra* note 99.
112. *See* Drozdiak & Schechner, *supra* note 30.
113. *See* Myers, *supra* note 99.
114. *See id.*
115. *See id.*
116. Segalis & Linksy, *supra* note 102.

C. CERTIFICATION MECHANISMS

As another form of appropriate safeguard, the GDPR encourages the "establishment of certification mechanisms, data protection seals and marks," such that data subjects are able to quickly assess the level of data protection of relevant products and services.[117] Similar to codes of conduct and standard contractual clauses, the implementation of certification mechanisms, seals, and marks require additional action by the European Data Protection Board.[118] In the future, the Board may develop a common European Data Protection Seal and oversee the publishing of information about certification registrants in a publically available directory.[119] Whether this type of action happens, and whether it presents a viable method of certification, remains to be seen.

Still, the United States and the European Union recently adopted the Privacy Shield Framework in an effort to provide a new transatlantic data transfer framework.[120] The European Commission adopted the arrangement in an effort to "impose stronger obligations on U.S. companies exchanging data with EU states" in the wake of the Safe Harbor invalidation.[121] While at face value the agreement appears to serve as a replacement for Safe Harbor and, therefore, allow for uninterrupted data flows, analysts and industry officials are not convinced.[122] Datacenter Dynamics described the agreement as "controversial" and suggested that it would be the subject of further appeals and subsequent revisions.[123] Similarly, Julie Brill acknowledged that with Privacy Shield, there is much conversation around "whether European courts, Member States, and data protection authorities will find the protections surrounding these data transfers to be adequate."[124] The viability of Privacy Shield as a framework for transatlantic data transfer is thus clouded by uncertainty, with experts doubting its longevity, and one concluding that it will "suffer the same fate as the Safe Harbor scheme it has been designed to replace."[125] Accordingly, without additional legal clarity, the recently adopted framework does not provide small businesses with a reliable mechanism for data transfer.

117. Commission Regulation, *supra* note 12, at art. 42(1).
118. *See* Myers, *supra* note 99.
119. *See id.*
120. *See* Michael Hurley, *Europe Could be up for Grabs*, DATACENTERDYNAMICS (Oct. 20, 2016), http://www.datacenterdynamics.com/content-tracks/colo-cloud/europe-could-be-up-for-grabs/97160.fullarticle.
121. *Id.*
122. *See* Moody, *supra* note 14.
123. Hurley, *supra* note 120 ("The controversial agreement . . . leaves many observers unconvinced . . .").
124. Brill, *supra* note 2, at 154.
125. Moody, *supra* note 14.

D. HOW DO LARGE TECHNOLOGY COMPANIES COMPLY?

It is worth noting that large technology companies based in the United States can comply with the GDPR by simply keeping their data within the EEA, thereby negating the need for use of the aforementioned appropriate safeguards.[126] The resources available to these industry-leading companies enable them to comply by relocating their data centers to the EEA, or building new ones, which they are doing.[127] For example, Apple, Microsoft, and Google are investing in Irish, Dutch, and Scandinavian facilities, and, in general, large U.S. providers and enterprises are bolstering their presence closer to their data subjects across the Atlantic.[128] Google also expanded the size of its center in Belgium, and built a new data center in the Netherlands.[129] Moreover, Amazon plans to add a new data center in Sweden in 2018, giving Amazon a total of five cloud services locations in Europe.[130] Amazon's founder and CEO, Jeff Bezos, also met with the Italian Prime Minister, Matteo Renzi, in July of 2016 to discuss opportunities in Italy.[131] This interaction sheds light on the recent trend of politicizing the construction of data centers, a pattern that could increase with the evolution of data protection regulation, coupled with the obvious incentives for political figures to attract technology investment to their countries.[132] And while it may be easy to see why large U.S. technology companies would look to invest in data centers across the EEA and ingratiate themselves with relevant political figures, this movement clouds the landscape for small businesses in the evolving digital economy.[133]

Indeed, small, U.S.-based technology companies looking to compete across the EEA are currently caught "between a rock and a hard place."[134] Purely from an operational perspective, the obligations placed on companies by the GDPR are extensive.[135] According to Ryan Costello, operations manager at eTERA Consulting in Europe, the GDPR will require that many companies conduct "a complete revamping of their software, which small companies don't have the resources or time to be able to do."[136] This is the case, Mr. Costello explained, because these companies may have expended

126. *See* Drozdiak & Schechner, *supra* note 30.
127. *See id.*
128. *See* Hurley, *supra* note 120.
129. Drozdiak & Schechner, *supra* note 30.
130. Barb Darrow, *Amazon Web Services to Open Cloud Data Centers in Sweden,* FORTUNE (Apr. 4, 2017), http://fortune.com/2017/04/04/aws-swedish-data-center/.
131. Hurley, *supra* note 120.
132. *See id.*
133. *See* Drozdiak & Schechner, *supra* note 30.
134. Carson, *supra* note 6 (Phil Lee of Field Fisher Waterhouse described U.S. companies seeking to transfer data out of the EU as being "stuck between a rock and a hard place," largely due to the distrust related to U.S. surveillance.).
135. *See supra* Part II.
136. Dipshan, *supra* note 81.

all their capital and effort creating a specific product.[137] Mr. Costello believes that while most of the large and midsized companies will be able to meet the regulation by 2018, "small companies are the ones that will get hurt the most."[138] Indeed, many companies may find that the burden of complying with the new data protection regulations by 2018 will simply be too much of a burden to bear. According to former FTC Commissioner Julie Brill, "small and medium enterprises—which made up around 60 percent of Safe Harbor membership—stand to lose the most from the *Schrems* decision."[139] Ms. Brill explained that, similar to the biggest companies that are frequently the subject of public debates in Europe, small and medium-sized enterprises depend on the free flow of information to sell goods and services globally, to build global workforces, and to take advantage of low-cost cloud computing resources.[140] Unlike those big technology companies, these small and medium enterprises "do not have the resources to get [binding corporate rules] approved or put model contractual clauses in place."[141] The result: these small ventures are left in a bind.

IV. ADDRESSING THE PREDICAMENT THAT SMALL, U.S. INTERNET COMPANIES FACE IN THE GDPR WORLD

The GDPR, as described above, will provide a unified, harmonized body of data protection laws that align with Europe's comparatively stringent views of data privacy. Given the progression of technology and data processing, however, the GDPR's principles leave a wide gap between the state of digital commerce today and the world the Commission envisions. With the GDPR, Europe will enhance its data privacy regime to a point which will require data processors to reexamine their approaches to product design and overall operations.[142] This happens at a time when thousands of non-EU companies are left without a good option for transferring personal data out of the European Union as part of their operations.[143]

With no Safe Harbor, and a more onerous European data privacy regime, the transatlantic digital economy is likely headed toward a business climate in which very few small, U.S.-based companies are able to comply with EU law.[144] It is also worth noting that many business leaders are currently unaware of the requirements that the new regulation will impose on their organizations.[145] A recent study by Amárach Research, completed on behalf

137. *See id.*
138. *Id.*
139. Brill, *supra* note 15.
140. *See id.*
141. *Id.*
142. *See* Sayer, *supra* note 21.
143. *See* Brill, *supra* note 15.
144. *See supra* Part III.
145. *See Study: Only 28 Percent of CFOs are Aware of the GDPR*, THE INT'L ASS'N OF PRIVACY PROF.: EUROPE DATA PROTECTION DIGEST, Nov. 17, 2016, LEXIS [hereinafter *Study*].

of BT Ireland, revealed that "63 percent [of financial decision makers working in organizations with an average of 800 employees] were unaware of the requirements or penalties associated with the EU's General Data Protection Regulation."[146] Additionally, the report revealed that, despite Irish Chief Financial Officers (CFO) being more likely than Chief Information Officers to be in control of large-scale IT investments, approximately two-thirds of the CFOs surveyed were completely unaware of key privacy regulations, such as Privacy Shield.[147] This report puts the current regulatory landscape in perspective, as it underscores the question recently posed by BT Communications Ireland Managing Director Shay Walsh: "[A]re boardroom decision makers aware of the penalties associated with a data breach?"[148] Walsh emphasized that CFOs and board members "need to understand the impact of their tech spend, and ensure they have clear procedures, policies and compliance in place, in preparation for the changes coming in May 2018."[149]

Looking ahead, the regulatory landscape under the GDPR could go one of two ways. On the one hand, the climate could be one in which few companies comply, and consistent enforcement across the EEA of all data protection infringements is a pipe dream. On the other hand, the situation could be one in which European DPAs significantly increase enforcement of data protection infringements to an extent that could seriously jeopardize U.S.-based companies' ability to compete throughout the EEA. For small American companies, the latter scenario is not optimal, and it bears noting that U.S.-based companies will, in theory, be the ones falling behind. Companies based in the EEA will benefit from a streamlined approach to data privacy enforcement and compliance.[150] Such regulatory renovations may, in time, prove beneficial for companies in the European Union, a result the European Commission is undoubtedly counting on. Indeed, with the Commission creating a "One Stop Shop" mechanism to harmonize enforcement of the GDPR,[151] the hope is that imposing an extra-territorial effect will raise the data privacy standards globally.[152]

Evidence of this can already be found in various pockets of the world. For example, in the Philippines, one Senator who authored a recently enacted data protection law cited business and investment interests as a primary

146. Charlie Taylor, *CFOs in the Dark on Data Legislation,* IRISH TIMES, Nov. 17, 2016, at 5.
147. *See id.*
148. *See Study*, *supra* note 145.
149. *See* Taylor, *supra* note 146.
150. *See supra* Part II.
151. *See supra* Part II.
152. *See* Marc Rotenberg & David Jacobs, *Privacy, Security, and Human Dignity in the Digital Age: Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J.L. & PUB. POL'Y 605, 642 (2013).

motivator for basing the law on the EU Data Protection Directive.[153] "By establishing such a policy framework, we actually protect Internet freedoms while making sure the Web remains safe," the Senator explained.[154] "In this way, we reduce the risk for true harm to be inflicted and heighten the opportunity for our digital space to be a truly productive and collaborative venue."[155] The Philippines' government thus hoped to encourage investment in their information technology and Business Process Outsourcing (BPO) industries by mimicking the privacy framework of the European Union.[156] This development lends credence to the idea that the European Union will raise global data protection standards by enacting the GDPR.

By not passing data privacy legislation, the United States risks falling behind the global standard for data privacy and further eroding citizens' trust in the processing of personal data by U.S.-based companies. Despite conversations amongst top officials in the United States and the European Union being described as "healthy talks about U.S. efforts to make ongoing improvements to the framework,"[157] the United States and the European Union are clearly at a crossroads. While the European Union just passed a sweeping regulation that will empower citizens to better understand and control their personal data while also providing a streamlined mechanism of enforcement, the United States is essentially in the same place it was when Safe Harbor was invalidated. Indeed, "the EU in general still strongly mistrusts the U.S. to keep its data safe."[158] Even prior to Safe Harbor's invalidation, the issue of trust seemed to have an effect both on individual citizens' choices as well as those of European companies. Not surprisingly, the two appear to be inextricably linked. Emmannuelle Bartoli, former Chief Privacy and Security Legal Counsel at Atos in Paris, described the market for data transfer from Europe to the United States as "very tough because the customers are always questioning the security . . . . Self-certification in Europe is not something people trust."[159]

On the other hand, some experts feel the attitudes around the prior self-certification regime are unwarranted. Phil Lee, Certified Information Privacy Professional (Europe)(CIPP/E) of Field Fisher Waterhouse, described Safe Harbor as the "low-hanging fruit," because the framework was a "little unfairly singled out."[160] Mr. Lee explained that "[o]f all the data-export solutions, the most enforcement has happened around Safe Harbor."[161]

153. *See Senate Approves Data Privacy Act on 3rd Reading*, ABS-CBN NEWS (Mar. 20, 2012), http://news.abs-cbn.com/business/03/20/12/senate-approves-data-privacy-act-3rd-reading.
154. *Id.*
155. *Id.*
156. *See id.*
157. Carson, *supra* note 6.
158. *Id.*
159. *Id.*
160. *Id.*
161. *Id.*

Furthermore, Mr. Lee pointed out that there had been "no enforcement of model [contract] breaches, no enforcement of binding corporate rules breaches."[162] Mr. Lee concluded that, "in many senses, Safe Harbor is the most robustly enforced."[163] To that end, the FTC had shown a willingness to enforce data privacy prior to Safe Harbor's invalidation.[164] Indeed, between November 2013—when the European Commission published thirteen recommendations for how to improve Safe Harbor—and May 2014, the FTC reached settlements with more than twelve companies regarding alleged infringements related to Safe Harbor.[165]

Such a push in enforcement actions could be seen as a genuine attempt by the FTC—and the United States in general—to ramp up their privacy enforcement regime, thereby pushing the standard closer to that of the European Union. On the other hand, it could also be seen as a desperate attempt to salvage the only legal framework for transatlantic data flow that U.S. companies utilized on a widespread basis. The continuing distrust on the part of the European Union seems to suggest the latter. Mr. Lee described a conversation he had with a German company which, at the time, was in discussions with a U.S.-based vendor.[166] Mr. Lee, with hopes of facilitating a deal, tried to persuade the German company that the U.S. company had done its due diligence, and that Safe Harbor was the optimal legal solution upon which to base the deal.[167] The German company responded, "[T]hat may be the case, but it's not safe."[168] Further, the German company explained that while they recognized everything Lee was saying, they simply did not "like it at the end of the day."[169] To Mr. Lee, this reaction showed that the "emotional perception" of the United States' privacy approach was ultimately driving the decisions around whether those who were self-certifying were adequately protecting data privacy.[170]

A. SHORT-TERM SOLUTION: FEDERAL TAX CREDIT FOR SMALL INTERNET BUSINESSES

Aside from the alleged merits of EU citizens' distrust toward U.S. privacy laws, the misgivings certainly seem to stem from the Snowden

162. *Id.*
163. *Id.*
164. *See id.*
165. *Id.* The European Commission recommended thirteen specific improvements to Safe Harbor. These included that self-certifying companies should disclose all data-sharing relationships with third parties, various modifications to the dispute-resolution process, and a more stringent reading of the "national security exception" that allowed companies to derogate from the privacy rules. Many of the FTC's settlements centered on charges that the self-certifying companies had not met their obligation to recertify annually, despite claiming to be Safe Harbor compliant. *See id.*
166. *See id.*
167. *See id.*
168. *Id.*
169. *Id.*
170. *Id.*

revelations.[171] As Mr. Dean of the Department of Commerce testified, Safe Harbor originally became a target for criticism because it "had become linked to the surveillance disclosures."[172] Whether this link was valid or not, the revelations brought to light by Snowden created distrust across the European Union and the overall perception that the United States was "engaged in 'mass, indiscriminate surveillance'" of personal data of EU citizens.[173] Indeed, "Mr. Schrems' claimed allegations . . . by Snowden showed Facebook wasn't sufficiently protecting users' data because it is subject to mass surveillance in the U.S."[174] The NSA's surveillance practices, therefore, played a significant role in producing the predicament that small, U.S.-based internet companies looking to compete across the Atlantic now face. Without the revelations regarding the surveillance of personal data, particularly the personal data of non-U.S. citizens derived from large internet and social network companies, EU citizens would have less of a reason to distrust the United States, and small, U.S.-based internet companies would face fewer obstacles when transferring data. Although the events likely will not pose prohibitive obstacles for companies like Amazon or Facebook, small enterprises are left searching for practical solutions, or perhaps not even concerning themselves with compliance in the first place. To address this predicament, Congress should adopt short-term measures to help small, U.S.-based internet companies expand globally in a regulatory climate that, practically speaking, discourages such growth.

Such legislative measures could take the form of a federal tax credit made available to small internet companies that previously relied on Safe Harbor for their transatlantic data transfers, as well as new companies that fit a similar description. The credit would, in theory, help level the playing field for U.S.-based internet companies. Requirements for obtaining approval for the credit would include: (1) that the company employs less than 300 employees; (2) that the company's annual revenue is under $7.5 million;[175] (3) that the processing of personal data of EU citizens is substantially related to the functioning of the company's business; (4) that the company does not already belong to a trade or industry group that could implement binding corporate codes of conduct or standard contractual clauses; and (5) that the

171. *See* Drozdiak & Schechner, *supra* note 30.

172. Testimony of Edward Dean, *supra* note 16.

173. *Id.*

174. Drozdiak & Schechner, *supra* note 30.

175. The Small Business Administration (SBA) defines small businesses in the following sectors as those with revenue under $15 million: Advertising Agencies; Media Buying Agencies; Other Services Related to Advertising; Marketing Research and Public Opinion Polling; and All Other Professional, Scientific and Technical Services. *See* U.S. SMALL BUS. ADMIN., TABLE OF SMALL BUSINESS SIZE STANDARDS MATCHED TO NORTH AMERICAN INDUSTRY CLASSIFICATION SYSTEM CODES (2017), https://www.sba.gov/sites/default/files/files/Size_Standards_Table_2017.pdf. For the purposes of this tax credit, the revenue cap could be reduced further, to $7.5 million, or even lower, to ensure that only companies that do not have robust legal support would benefit from the program.

company has previously complied and will continue to comply with the privacy standards promulgated by the FTC.

With the credit program, Congress could maintain its own form of annual certification. Under such a program, companies would work with the FTC to apply annually for certification. As long as organizations remain in the small enterprise category, maintain an internet-based business that relies on data processing in order to function, and comply with the relevant data privacy and data protection standards set forth by the FTC, companies would remain in good standing and continue to benefit from the tax credit. The program would help small companies like the one Mr. Dean described,[176] as the financial assistance would enable them to either invest in data centers abroad or partner with appropriate cloud computing vendors in the European Union. The former route would enable small companies to more easily comply with the GDPR, as they could avoid transfers of personal data to third-party countries outside of the EEA. The latter option would achieve a similar result in that it would enable small companies to keep any data they collect within the confines of the EEA. This option could also prove beneficial for small companies in that a sophisticated cloud computing partner would likely bring compliance expertise to the company's data processing activities. By helping small companies afford a partnership with this type of vendor, the tax credit would, to some extent, level the playing field with the larger technology companies that already have the means to invest in data centers abroad.

B. LONG-TERM SOLUTION: FEDERAL DATA PRIVACY & PROTECTION LEGISLATION

If the United States wants its businesses to compete globally, the government needs a long-term solution. While the above tax credit would do much to help remedy the predicament largely created by the U.S. government itself, a more sustainable privacy framework that allows for seamless data transfers across borders is optimal. To that end, Congress should enact legislation that raises the data privacy standards in the United States, assuages the concerns of foreign nations regarding data protection, and ultimately earns the United States an "adequate" label from the European Commission.

1. The 2012 Consumer Privacy Bill of Rights: A Worthy Model with Similarities to the GDPR

Congress should look to the 2012 Consumer Privacy Bill of Rights, released by the Obama administration, as a useful framework for such legislation.[177] The overall goal of the initiative was to strike the ideal balance

176. *See* Testimony of Edward Dean, *supra* note 16.

177. *See* EXEC. OFFICE OF THE PRESIDENT, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*

between strengthening consumer protections with respect to data privacy and allowing companies to innovate effectively both in the operation of their businesses and in the implementation of privacy protection.[178] Along those lines, President Obama described the importance of enhanced privacy protection when he said that:

> Even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever.[179]

The Consumer Privacy Bill of Rights outlined seven key rights that an enhanced privacy framework should emphasize.[180] The guidelines pertain to the relevant consumers, as well as the companies that process the data as part of their business operations.[181] Not surprisingly, the seven-point framework and the framework provided by the GDPR have plenty in common. The key points are: (1) individual control; (2) transparency; (3) respect for context; (4) security; (5) access and accuracy; (6) focused collection; and (7) accountability.[182]

The enhanced privacy framework would give individual consumers more control over their personal data. Specifically, it would empower citizens to control what data is collected, what is stored, and how it is used.[183] This measure is not unlike the GDPR provisions requiring companies to account for the right to correct and the right to be forgotten.[184] Next, the Consumer Privacy Bill of Rights would impose the concept of transparency on digital companies.[185] This would require companies to provide consumers with an easy and accessible way of viewing the types of data collected and the purposes of collection, a timeline of data processing, and whether their data would ever be shared with third parties.[186] These concepts almost directly mirror the GDPR's transparency obligations outlined in Article 12.[187]

The third component would require that companies only process personal data in ways that are "consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the

(2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [hereinafter *Consumer Data Privacy*].

178. *See* Rotenberg & Jacobs, *supra* note 152, at 649.

179. *Consumer Data Privacy*, *supra* note 177.

180. *See* Rotenberg & Jacobs, *supra* note 152, at 649.

181. *See id.*

182. *See* Press Release, Office of the Press Secretary, White House, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012).

183. *See Consumer Data Privacy*, *supra* note 177, at 11.

184. *See* Commission Regulation, *supra* note 12, at art. 54.

185. *See Consumer Data Privacy*, *supra* note 177, at 10.

186. *See* Rotenberg & Jacobs, *supra* note 152, at 649.

187. *See* Commission Regulation, *supra* note 12, at art. 12.

data . . . ."[188] Here, again, the proposed framework is consistent with the GDPR's requirements in Article 40 discussing data minimization and restricting data processing to the purpose of its original collection.[189] This component of the framework would, therefore, move the United States closer to the European Union's privacy standard.

The fourth component of the framework pertains to data protection.[190] Companies would be required to implement adequate procedures to safeguard against data breaches, data loss, data destruction, data modification, and improper disclosure.[191] These concepts are reminiscent of the GDPR's requirement of data protection "by design and by default."[192] Both privacy regimes would, therefore, require companies to incorporate appropriate procedures—throughout both the product design life-cycle, as well as the overall operation of the business—to ensure adequate data security.

The framework would next require that companies provide consumers with access—in usable formats—to their data so that they can correct any inaccuracies.[193] The format must be easily digestible, and it must provide an appropriate manner of correcting, deleting, or limiting the use of such data. Moreover, companies must consider the "scale, scope, and sensitivity of the personal data that they collect or maintain and the likelihood that its use may expose consumers to financial, physical, or other material harm."[194] Again, the concern around inaccuracies and their potential impact on citizens' lives is something expressly contemplated by the GDPR in paragraph 71.[195] In this sense, the two regimes express clear concern for the potentially discriminatory effects of data processing and present rules to which companies must adhere.

The sixth element in the proposed framework pertains to the "reasonable limits on the personal data that companies collect and retain."[196] This proposed framework bears similarities with the GDPR's principles of data minimization and data by necessity. Under each, companies should not collect excessive amounts of data, but rather collect the minimum amount of data consistent with the context principle.[197] Finally, the Consumer Privacy Bill of Rights would require accountability, which obligates companies to properly train their employees, regularly evaluate their data privacy and

188. *Consumer Data Privacy*, *supra* note 177, at 47.
189. *See* Commission Regulation, *supra* note 12, at art. 40.
190. *See Consumer Data Privacy*, *supra* note 177, at 48.
191. *See id.*
192. *See* PROPOSED DATA PROTECTION REG., *supra* note 58.
193. *See* Rotenberg & Jacobs, *supra* note 152, at 649–51.
194. *Consumer Data Privacy*, *supra* note 177, at 48.
195. *See* Commission Regulation, *supra* note 12, at para. 71.
196. *Consumer Data Privacy*, *supra* note 177, at 48.
197. *See* Commission Regulation, *supra* note 12, at art. 5(1)(c).

protection procedures, and where appropriate, perform audits.[198] This would encourage a similar standard imposed by the GDPR, which requires companies to maintain adequate internal records,[199] implement adequate organizational procedures,[200] and, in some cases, conduct data protection impact assessments to ensure the proper standard of data privacy and security.[201]

2. Putting Federal Data Privacy Legislation in Context

Similarities notwithstanding, this framework is still not law. In 2012, President Obama promised that his administration would "work to advance these principles and work with Congress to put them into law."[202] Five years and a new administration later, the United States is without Safe Harbor, has not formally enacted data privacy legislation, and relies primarily on Privacy Shield—a framework that many feel will be invalidated—for cross-border transfers. Moreover, in early 2016, the Obama administration moved to expand the sharing of data that the NSA collects with other agencies.[203] The administration had the authority to take such measures under domestic law because the NSA collects the data through surveillance methods that Congress did not include in the Foreign Intelligence Surveillance Act (FISA), the main law governing wiretapping.[204] In the absence of express statutory limits, the NSA's surveillance programs are primarily governed by rules set by the White House under a previous Executive Order.[205] Such a move will likely further erode trust of U.S. data protection policy in the European Union and around the globe. Such unfettered discretion is precisely what gave rise to the high level of distrust in the first place and, therefore, must be checked.

To that end, the much-needed federal data privacy legislation should explicitly codify the boundaries of the NSA's surveillance authority, both in terms of the personal data of Americans and that of foreign citizens. With due consideration to the concerns of national security, the legislation could mimic some of the language of the GDPR in terms of data minimization, necessity, and appropriate safeguards. Specifically, the legislation should require "appropriate technical and organizational measures . . . to safeguard

198. *See Consumer Data Privacy*, *supra* note 177, at 48.
199. *See* Commission Regulation, *supra* note 12, at art. 30.
200. *See* Commission Regulation, *supra* note 12, at arts. 5 and 22.
201. *See* Commission Regulation, *supra* note 12, at art. 35.
202. Rotenberg & Jacobs, *supra* note 152, at 652.
203. *See* Charlie Savage, *Obama Administration Set to Expand Sharing of Data That N.S.A. Intercepts*, N.Y. TIMES (Feb 26, 2016), https://www.nytimes.com/2016/02/26/us/politics/obama-administration-set-to-expand-sharing-of-data-that-nsa-intercepts.html.
204. *See id.*
205. Executive Order 12333, a directive from President Reagan's administration, governs the NSA's surveillance programs that are not implicated by the Foreign Intelligence Surveillance Act. *See id.*

the rights and freedoms of the data subject."[206] Lawmakers could achieve this by explicitly specifying the purposes for which the agency could monitor data, setting limits on the amount of time that data could be stored, and by codifying the technical and organizational measures that would ensure that fundamental rights, such as privacy, are not abused. Such legislation would do much in the way of bringing U.S. surveillance practices out of the shadows and instilling trust throughout the international community.

Such comprehensive legislation would dramatically update the data privacy and data protection laws in the United States. This move forward for the United States would bode well for transatlantic data transfers and the digital economy overall. In the context of the European Union, this legislation would put the United States in a position to earn an adequacy categorization from the European Commission. Having an adequacy categorization would effectively free up small, U.S.-based internet companies to transfer data across borders with ease, thereby presenting a solution to the problem that the government played a key role in creating. Privacy legislation would also provide consumers—both in the European Union and the United States—with increased confidence that their data is being processed safely and responsibly. Moreover, such legislation would be an important step toward securing the more than $240 billion in digitally deliverable services traded between the United States and Europe.[207] Accordingly, Congress should promptly enact such legislation.

CONCLUSION

Revelations regarding the NSA's surveillance practices shed light on the risks to privacy in a digital world unchecked by proper privacy law. These revelations sowed distrust around the world with respect to the treatment of personal data in the United States. Europe's treatment of data privacy as a fundamental right separates it from the United States and positions the European Union as a leader in the realm of data protection law in the digital economy. With the GDPR taking effect in May 2018, companies around the globe need to be aware of the upcoming changes, and take measures to ensure compliance with the GDPR if they want to compete globally. Given the severe penalties associated with data protection infringements under the GDPR, ignoring the sweeping regulation would be a grave mistake. And while it may be operationally feasible for large American technology companies to comply right away, small, U.S.-based ventures face a challenging road ahead.

The process of adjusting to the GDPR world will surely be iterative and gradual, but given its massive scope, the U.S. government surely has a role to play. Moreover, because the U.S. government was at least partly

206. Commission Regulation, *supra* note 12, at art. 5(1)(e).
207. *See* Testimony of Edward Dean, *supra* note 16.

responsible for producing the aforementioned distrust amongst the international community, Congress should be proactive about addressing the inequities that small, U.S.-based companies currently face. Congress should adopt both short-term and long-term measures to level the playing field for small businesses in the United States. In the short term, Congress should enact a federal tax credit containing an annual certification mechanism to assist small, U.S.-based internet companies seeking a global footprint. In the long run, Congress should pass federal data privacy legislation that raises the data privacy and protection standards in the United States, assuages the concerns of foreign nations regarding treatment of personal data in the United States, and ultimately positions the United States to earn an adequacy ruling from the European Commission. These measures would mitigate the challenges many small American companies currently face, thereby helping them compete in the global economy, and in the GDPR world.

Craig McAllister[*]

* B.A., Villanova University, 2011; J.D. Candidate, Brooklyn Law School, 2018. Thank you to Kieran Meagher, Drita Dokic, Michael Kumar, and the entire Brooklyn Journal of Corporate, Financial & Commercial Law staff for their help preparing this note for publication. Also, special thanks to Professor Jonathan Askin for listening to me ramble on about data privacy, and encouraging me to consider the small business community. Finally, thank you to my parents, Tom and Jeanne, for encouraging life-long learning.