THE LONG ARM OF THE EU: THE REACH OF BRUSSELS' DATA PROTECTION REGIME INTO THE UNITED STATES

Patrick A. Wallace[*]

INTRODUCTION

By its very nature, the internet is global. Connecting to the internet all but guarantees that one's data will at some point cross a national border. This raises the much-discussed questions of which country's laws apply to whom and who has the authority to make such a determination. Assuming, for the sake of argument, that the laws of one nation can apply to entities operating outside its borders, the next step is to determine the options a government has for asserting jurisdiction over those entities.

The United States and the European Union take fundamentally different approaches to privacy. The EU Charter of Fundamental Rights recognizes an individual right to have data protected and handled in certain ways.[1] This has translated into two comprehensive legislative enactments aimed at protecting the privacy of individuals living within the EU.[2] In contrast, the United States does not have an explicit right to privacy in its Constitution. Privacy protections for consumers in the US come from a patchwork of sector-specific federal laws,[3] Federal Trade Commission ("FTC") enforcement actions, a handful of common law claims, and various state statutes. There is no comprehensive privacy statute in the United States.

The European Union's General Data Protection Regulation[4] ("GDPR") went into effect in May 2018.[5] It is a comprehensive privacy law that covers private entities in every industry.[6] The GDPR is written to apply even to entities operating outside of the EU.[7] While Europe is no stranger to a comprehensive privacy law, the extraterritorial application of the GDPR is a major

---

[*] Antonin Scalia Law School at George Mason University, J.D. Candidate 2019; Production Editor, George Mason Law Review, 2018–2019. The Author would like to thank his wife Megan for her love and support, and Mebs Dossa and Andrew Konia for their mentorship.

1 2000 O.J. (C 364) 10.

2 These are the General Data Protection Directive and the General Data Protection Regulation. 2016 O.J. (L119) 1–88 (Regulation); 2016 O.J. (L 119) 89–131 (Directive).

3 *See, e.g.*, Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1127; Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

4 2016 O.J. (L 119) 1–88.

5 *Id.* at 87.

6 *See id.* at 32.

7 *Id.* at 32–33.

difference from its predecessor, the General Data Protection Directive (the "Directive").[8]

This Comment considers a tension in the GDPR: Its enumerated territorial scope is broad, but the EU's actual competence to enforce the regulation extraterritorially seems to be quite limited. Thus, while the GDPR casts a big shadow, it is not entirely clear that entities outside of the EU—but subject to the GDPR—will face actual consequences for violations. This tension and its implications are explored at length, specifically for US-based entities.

This Comment proceeds in four parts. Part I explains privacy law in the EU, transatlantic data transfer agreements, and the ability of foreign governments to enforce their laws in the US. A basic understanding of privacy law in the EU provides perspective about the expansive nature of the GDPR. The history of transatlantic data transfer agreements and the weak legal ground on which they are based in part demonstrates how the extraterritorial application of the GDPR became a reality. Part II discusses the avenues the EU could employ to enforce the GDPR in the US. Part III explores when a US entity could be subject to the requirements of the GDPR and proposes steps that could be taken to shield the entity from liability. To demonstrate the far reach of the law, a pair of hypotheticals are developed. Finally, Part IV provides perspective on what the future could hold for GDPR enforcement in the US.

I. BACKGROUND

To understand the implications of the GDPR for the US entities to which it applies, one must understand the history and legal context of privacy in the EU and also understand how the US legal system treats and applies foreign law. In the EU, a fundamental right to privacy flows from its core governing documents.[9] The European Parliament and the European Council have twice given effect to these rights by enacting comprehensive data privacy legislation.[10] In contrast, the US has gradually recognized a right to privacy, arguably beginning with a seminal law review article in 1890.[11] What follows is an in-depth discussion of the fundamental legal principles of EU privacy law, a discussion on transatlantic data transfer, and a discussion on enforcing foreign law in US courts.

---

8 *See* 2016 O.J. (L 119) 89–131.

9 *See* 2012 O.J. (C 326) 55 (granting the right to the protection of personal data and directing the enactment of legislation to give that right full effect.); *id.* at 397 (granting the right to respect of private and family life, home and communications, and the right to the protection of personal data).

10 *See* 2016 O.J. (L 119) 1–88 (Regulation).; 2016 O.J. (L 119) 89–131 (Directive).

11 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

A. *Privacy Law in the EU*

An examination of privacy law in the EU must begin with the Charter of Fundamental Rights of the European Union (the "Charter").[12] Article 7 of the Charter provides "respect for . . . private and family life, home and communications."[13] But the Charter goes beyond simply codifying a general right to privacy.[14] Article 8 guarantees a right to the protection of personal data about an individual.[15] Article 8 further requires that data be "processed fairly for [a] specified purpose[] and on the basis of the consent of the person concerned" or other lawful purpose.[16] The Charter requires that these rights be enforced by an independent authority.[17]

The Treaty on the Functioning of the European Union (the "TFEU")[18] reiterates "the right to the protection of personal data."[19] The TFEU directs the European Parliament and the European Council to enact legislation to give effect to the right to the protection of personal data.[20] The legislation must focus on the processing and free movement of personal data.[21] The TFEU also reiterates the requirement of enforcement by an independent authority.[22]

Based upon the rights enumerated by the Charter and the TFEU, the European Parliament and the European Council enacted the General Data Protection Directive.[23] The Directive was the EU's first comprehensive data protection statute.[24] Many of the key concepts in the GDPR that are discussed below were first expressed in the Directive.[25] The European Parliament and

---

12 2012 O.J. (C 326) 391–407.

13 *Id.* at 397.

14 *See id.*

15 *Id.*

16 *Id.*

17 *Id.*

18 2012 O.J. (C 326) 47–390.

19 *Id.* at 55.

20 *Id.*

21 *Id.*

22 *Id.*

23 2016 O.J. (L 119) 89–131.

24 *Id.* at 89.

25 *Compare* 2016 O.J. (L 119) 107 (defining the term "controller" as "the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law," and the term "processor" as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"), *with id.* at 33 (defining the term "controller" as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law," and the term "processor" as "a natural

the European Council enacted the GDPR to replace the Directive.[26] It went into effect in May 2018.[27] The GDPR is a regulation instead of a directive.[28] In the EU, a regulation is binding law on all member states, while a directive is legislation that requires member states to enact their own domestic legislation to carry it out.[29]

The GDPR maintains a similar framework to that of the Directive but tends to be more comprehensive in its reach and its requirements. The GDPR's definition of "personal data" is more extensive than the Directive's.[30] The GDPR specifies stiff penalties to be assessed for violations while the Directive allowed member states to define their own "effective, proportionate, and dissuasive" penalties for violations.[31] The European Parliament and the European Council have given the GDPR extraterritorial effect.[32] This is a significant departure from the Directive, which expressly excluded data processed during activities that occurred outside of the EU.[33]

From a general standpoint, the GDPR articulates a set of principles by which data should be processed.[34] These principles include: "lawfulness, fairness, and transparency"; "purpose limitation"; "data minimisation"; "accuracy"; "storage limitation"; "integrity and confidentiality"; and "accountability."[35] The GDPR operates from these general principles and gives them effect in the rest of its provisions.[36]

---

or legal person, public authority, agency or other body which processes personal data on behalf of the controller").

26 2016 O.J. (L 119) 1–2.

27 *Id.* at 87.

28 *Id.* at 1.

29 *See Regulations, Directives and Other Acts*, EUROPA, https://europa.eu/european-union/eu-law/legal-acts_en (last visited Aug. 27, 2019).

30 *Compare* 2016 O.J. (L 119) 33 ("'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person . . . ."), *with id.* at 106 ("'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person . . . .").

31 *Compare id.* at 82 (providing for "administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher"), *with id.* at 129 ("Member States shall lay down the rules on penalties applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.").

32 *Id.* at 32–33.

33 *Id.* at 106.

34 *Id.* at 35–36.

35 *Id.*

36 2016 O.J. (L 119) 36–39.

Before one can grasp the workings of the GDPR, one must understand the terms it employs. Perhaps the most important defined term is "personal information." Under the GDPR personal information is

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[37]

The expansive definition of personal information has many notable features. The first is that the GDPR does not apply to persons that are the product of a legal fiction such as corporations.[38] The definition also defines another term within itself—data subject.[39] A "data subject" is the natural person that the personal information describes.[40] Next, one must note that personal information is anything that can identify a person either directly or indirectly based upon attributes "such as a name, an identification number," or "an online identifier."[41] Recital 30 notes than an online identifier can include an IP address.[42] Finally, personal information can also include other pieces of information that reference features of an individual's identity.[43]

After understanding what the GDPR considers to be personal data, one can move to a discussion of how the GDPR defines the possession and use of personal data. The key term is "processing," which the GDPR defines as

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[44]

Processing essentially encompasses anything one can do with data, or in this case, personal information. An entity or natural person is a controller when it or the person "alone or jointly with others, determines the purposes and means of the processing of personal data."[45] A "processor" is an entity or natural person that "processes personal data on behalf of the controller."[46]

With an understanding of the terms the GDPR uses that will be relevant to this discussion, it is now important to understand the scope of the GDPR.

---

37 *Id.* at 33.
38 *Id.* at 3, 33.
39 *Id.* at 33.
40 *Id.*
41 *Id.*
42 2016 O.J. (L 119) 6.
43 *Id.* at 33.
44 *Id.*
45 *Id.*
46 *Id.*

Article 2 lays out the material scope of the GDPR.[47] It applies to "the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."[48] Paragraph 2 of Article 2 provides four exceptions to the applicability of the GDPR to the processing of personal information.[49] Two of the exceptions are relevant to law enforcement and national security interests.[50] The other two are for information processed in activities that fall outside of the scope of EU law and for data processed "by a natural person in the course of a purely personal or household activity."[51]

The territorial scope of the GDPR is laid out in Article 3 and is considerably more nuanced than the material scope.[52] There are three instances that fall under the territorial scope of the GDPR: (1) the establishment of a controller or processor operating within the EU, (2) processing data about data subjects residing within the EU, and (3) the processing of personal data by a controller outside of the EU, but where an EU member state's law applies by virtue of international law.[53]

Instance 1 is relatively straightforward in its application. If an entity seeks to establish a controller or processor within the EU, the GDPR applies regardless of where the processing takes place.[54] In other words, if one starts a company in the EU that will possess personal data, the GDPR applies.[55] If said company outsources one of its functions that involves the processing of personal information (human resources, payroll, etc.), then the GDPR applies to those functions as well.[56] The GDPR has extraterritorial effect in situations where the outsourced function occurs outside of the EU.[57]

Instance 3 is mostly beyond the scope of this Comment but is worth mentioning briefly. The GDPR envisions instances where an EU member state's domestic law applies in countries that are outside of the EU.[58] The example given in Recital 25 is when a controller is established in an EU member state's diplomatic mission or consular post located in a country outside of the EU.[59]

Instance 2 presents a bit of a bedeviling situation. For controllers or processors not within the EU, the GDPR applies when the data subjects are

---

47 *Id.* at 32.
48 2016 O.J. (L 119) 32.
49 *Id.*
50 *See id.*
51 *Id.*
52 *Id.* at 32–33.
53 *Id.*
54 2016 O.J. (L 119) 32.
55 *See id.* at 4, 32.
56 *See id.*
57 *See id.* at 32.
58 *Id.* at 32–33.
59 *Id.* at 5.

located within the EU and the processing activities are related to "(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of [the data subject located within the EU's] behaviour as far as their behaviour takes place within the Union."[60] This language has potentially wide-ranging consequences for internet-connected entities located outside of the EU.

The offering of goods or services to data subjects within the EU, irrespective of payment, potentially covers a wide range of online activity. Recital 23 states that the determination of whether a controller or processor offers goods or services to data subjects in the EU will turn on if "it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union."[61] At first glance, this appears to be a simple test that looks at the intent of the controller or processor, but the guidance on how this language will be interpreted is thin. However, the Oxford Dictionary defines "envisage" as to "[c]ontemplate or conceive of as a possibility or desirable future event."[62] Thus, the test does not necessarily reflect the intent of a controller or processor, but merely the foreseeability of a person residing within the EU using its service or purchasing a product.

Recital 23 further explains the test for determining whether goods or services were offered to data subjects residing within the EU.[63] The "mere accessibility" of a website in the EU, the availability of an email address or contact information, and the use of a language or currency in use in an EU member state are, each taken separately, "insufficient" to determine whether goods or services are offered.[64] But the recital takes care to note that the use of a certain language or currency or the mention of users or customers in the EU may evidence that the controller or processor envisaged offering goods or services in the EU.[65] It is not clear whether the GDPR contemplates an objective or subjective test as to what the controller or processor envisages.

Looking to the second half of Instance (2), the class of data controllers or processors located outside of the EU that process data of data subjects related to the monitoring of behavior that occurs within the EU seems to be quite broad. To determine whether the processing of data is related to monitoring behavior, Recital 24 counsels determining "whether natural persons are tracked on the internet."[66] It also points towards determining whether data have a potential subsequent use to profile an individual or to predict future behavior.[67]

---

60 2016 O.J. (L 119) 33.

61 *Id.* at 5.

62 *Envisage*, OXFORD ENGLISH LIVING DICTIONARY (2019), https://www.lexico.com/definition/envisage.

63 *See* 2016 O.J. (L 119) 5.

64 *Id.*

65 *Id.*

66 *Id.*

67 *Id.*

Now in possession of a general sketch of important defined terms in the GDPR and a sense of both its material and territorial scope, the discussion turns to a brief overview of the requirements placed on an entity subject to the GDPR. The GDPR requires controllers and processors to abide by the principles articulated in Article 5, as discussed above.[68] Chapter IV places a more concrete set of responsibilities on controllers and processors.[69]

The GDPR requires controllers and processors to implement measures aimed at achieving compliance with its principles in a risk-conscious manner weighed against costs.[70] This is not a one-time discrete responsibility, but an ongoing one.[71] Controllers and processors are expected to be able to demonstrate compliance with the principles and provisions of the GDPR at all times.[72] Compliance requires that controllers and processors maintain records[73] of the actions taken that relate to the processing of personal information.[74]

The GDPR also codifies in European law the concept of "[d]ata protection by design and by default."[75] This is defined in the regulation as:

---

68 *See id.* at 36.

69 *See* 2016 O.J. (L 119) 47–60.

70 *Id.* at 14–15, 47–48.

71 *See id.* at 47 ("Th[ese] measures shall be reviewed and updated where necessary.").

72 *Id.* at 15, 47–48.

73 The GDPR requires that the following information related to processing activities be recorded by controllers:

> (a) [T]he name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
> (b) the purposes of the processing;
> (c) a description of the categories of data subjects and of the categories of personal data;
> (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
> (e)where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
> (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Id. at 50–51. Processors are further required to maintain records that include:

> (a) [T]he name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
> (b) the categories of processing carried out on behalf of each controller;
> (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
> (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Id. at 51.

74 2016 O.J. (L 119) 16, 50–51.

75 *Id.* at 48.

> [B]oth at the time of the determination of the means for processing and at the time of the processing itself, implement[ing] appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing . . . .[76]

The regulation goes further in defining the concept, requiring entities to

> implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.[77]

Looking beyond mere privacy, the GDPR requires regulated entities to adopt "appropriate technical and organisational measures" to bolster data security.[78] Such measures are intended to be implemented in light of the current state of the art and with regard to the costs of implementation balanced with the risks involved.[79] The GDPR specifically mentions steps that might be taken, including:

> (a) [T]he pseudonymisation[80] and encryption of personal data;
>
> (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
>
> (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
>
> (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[81]

Outsourcing of processing functions is specifically contemplated by the GDPR.[82] A controller or processor may only use a third-party processor if that processor has provided sufficient guarantees that it has implemented appropriate technical and organizational measures to ensure that the processing

---

76 *Id*.

77 *Id*.

78 *Id*. at 51–52.

79 *Id*.

80 The GDPR defines "pseudonymisation" as:

> [T]he processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

2016 O.J. (L 119) 33.

81 *Id*. at 51–52.

82 *See id.* at 49.

of data occur in compliance with the GDPR.[83] Third-party processing must be done under an enumerated contract that contains stipulations[84] specified in the text of the GDPR.[85] A third-party processor that wishes to have another party process personal information must inform the original controller or processor of its intent to do so.[86] Any such additional processing is subject to the same requirements to which the original outsourcing was subject.[87]

In situations where a controller or processor is located outside of the EU and either offers goods or services to those residing within the EU or collects personal information for the purposes of monitoring behavior occurring within the EU, the controller or processor must designate in writing a representative to the EU.[88] Entities are exempt from this requirement if the data processing is (1) occasional, (2) does not include processing on a large scale special categories of personal data[89], or (3) involves processing data about criminal convictions.[90] A representative must be located within an EU member state which is home to individuals about who personal information is processed.[91] The representative effectively serves as the liaison between the

---

83 *Id.* at 49.

84 The contract must stipulate that the processer:

> (a) [P]rocesses the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
> (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
> (c) takes all measures required pursuant to Article 32;
> (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
> (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
> (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
> (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
> (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Id. at 49.

85 *Id.*

86 2016 O.J. (L 119) 49.

87 *Id.* at 50.

88 *Id.* at 48.

89 Special categories of personal data include "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation . . . ." *Id.* at 38.

90 *Id.* at 48.

91 2016 O.J. (L 119) 49.

supervisory authorities and the controller or processor and is subject to enforcement actions by any authority.[92]

To help ease the burden of compliance, an enumerated goal of the GDPR is the creation of codes of conduct that, when followed, would assist an organization in adhering to the principles of the GDPR.[93] The implementation by a controller of an approved code of conduct may be used as evidence that an entity is complying with the GDPR but is not dispositive.[94] A process for approving codes of conduct is laid out in Article 40.[95]

All of the rights and responsibilities laid out in the GDPR are not without an enforcement mechanism. The GDPR builds upon the supervisory authority model created by the Directive for the enforcement of its provisions by vesting the authorities with additional powers and giving greater specificity to those powers.[96] Each EU member state is required to establish an independent supervisory authority that is tasked with overseeing the implementation of, and compliance with, the GDPR.[97] Member states are given some latitude to determine the structure of their supervisory authority, with the GDPR outlining broad rules on the appointment of members and other functions necessary to the establishment of an authority.[98] Supervisory authorities have investigative, corrective, advisory, and enforcement authority.[99]

To ensure the consistent application of the GDPR across the member states, the GDPR created the European Data Protection Board.[100] The board consists of the European Data Protection Supervisor[101] and the head of a

---

92 *Id.* at 16, 49.

93 *See id.* at 19, 56.

94 *E.g.*, *id.* at 16, 50, 52.

95 *Id.* at 56–58 (requiring codes of conduct to be submitted to member state supervisory authorities that issue an opinion on the validity of the code and then submitting the draft code the European Commission for approval).

96 *Compare, e.g.*, *id.* at 69 ("Each supervisory authority shall have all of the following investigative powers: (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; (b) to carry out investigations in the form of data protection audits; (c) to carry out a review on certifications issued pursuant to Article 42(7); (d) to notify the controller or the processor of an alleged infringement of this Regulation; (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law."), *with id.* at 126 ("Each Member State shall provide by law for each supervisory authority to have effective investigative powers. Those powers shall include at least the power to obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks.").

97 2016 O.J. (L 119) 65.

98 *See id.*at 65–67.

99 *Id.* at 69–70.

100 *See id.* at 76.

101 The European Data Protection Supervisor is an existing independent supervisory authority created by the European Parliament and the European Council in 2001. *See* 2001 O.J. (L 8) 18.

supervisory authority from each of the EU member states.[102] It is not vested with any enforcement authority; its role is limited to issuing guidance.[103]

Entities subject to the GDPR have a large incentive to comply with the legislation. The GDPR allows for administrative penalties of up to €10 million or two percent of an entities' yearly turnover, whichever is greater.[104] Individuals injured by violations of the GDPR may bring action against a controller or processor to recover damages.[105] Article 79 creates a private right of action for individuals against controllers and processors notwithstanding any administrative proceedings that may also be undertaken against that processor or controller.[106] Jurisdiction to hear the complaint is granted to the courts in the member state in which the controller or processor has an establishment or where the data subject has a "habitual residence."[107]

B. *Transatlantic Data Transfer*

Data often crosses borders without regard for the laws of the jurisdiction from which it originated or the jurisdiction at which it arrives. The EU places limits on data being transferred to countries outside of the EU. The United States, with its generally laissez faire approach to privacy, essentially has no restrictions outside of a few sector-specific laws.[108] As this Comment focuses on data being transferred between the EU and the US, this discussion will be limited to the legal implications of that transfer.

1. Transfers Under the GDPR

Both the Directive and the GDPR place restrictions on the circumstances under which data may be transferred to a country outside the EU.[109] In GDPR parlance, transferring data to a country outside of the EU is referred to as transferring data to a "third country."[110]

Data may be legally transferred to a third country under one of four bases: (1) pursuant to an adequacy decision of the European Commission, (2) subject to appropriate safeguards, (3) under binding corporate rules, or (4) under one of several derogations.[111] The European Commission is empowered under the GDPR to determine that a third country provides an "adequate

---

102 2016 O.J. (L 119) 76.
103 *See id.* at 76–78.
104 *Id.* at 82.
105 *Id.* at 81.
106 *Id.* at 80.
107 *Id.*
108 *See supra* note 3 and accompanying text.
109 2016 O.J. (L 119) 60, 120.
110 *See Id.* at 60–61.
111 *Id.* at 61–64.

level of protection,"[112] and thus data may flow freely into that third country without "any specific authorisation."[113] Adequacy decisions are monitored on an ongoing basis and all decisions and revocations of adequacy are published in the EU Official Journal.[114]

Transfers may be made to a third country that is not the subject of adequacy decision on the basis of appropriate safeguards that provide "enforceable data subject rights and effective legal remedies for data subjects."[115] Appropriate safeguards can include: binding corporate rules (as discussed below), standard contractual clauses sanctioned by both a supervisory authority and the European Commission, approved codes of conduct, and approved certification methods.[116] The use of appropriate safeguards allows data to be transferred to third countries without any addition authorization.[117]

Binding corporate rules are a subset of appropriate safeguards but receive additional treatment in the GDPR.[118] As the name suggests, binding corporate rules are rules with legal effect that are developed within an organization or a group of organizations.[119] Binding corporate rules must be approved by a supervisory authority and allow for data to be transferred to a third country without any additional authorization.[120]

Member-state data protection authorities have taken steps to enforce EU privacy law dating back as far as 1996.[121] These steps include onsite audits of

---

112 *Id.* at 61. The GDPR gives the European Commission some latitude in making an adequacy determination, but the regulation requires the Commission to specific take account of the following factors:

> (a) [T]he rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

Id.

113 *Id.*

114 *Id.*

115 2016 O.J. (L 119) 62.

116 *Id.*

117 *Id.*

118 *Id.* at 62–63.

119 *See id.* at 62.

120 *Id.* The GDPR lays out minimum specifications for Binding Corporate Rules that are beyond the scope of this discussion. *See id.* at 63.

121 *See* Dan Jerker B. Svantesson, *The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on U.S. Businesses*, 50 STAN. J. INT'L L. 53, 74–75 (2014).

facilities in the US.[122] In one instance, a German data protection authority performed an onsite audit of a US subsidiary of a bank.[123] The audit was performed with the consent of the bank and not under the auspices of any formal law enforcement agreement between German and American authorities.[124]

2. Safe Harbour and EU-US Privacy Shield

Due to the perceived importance of data transfer between the US and the EU, the two jurisdictions have negotiated a number of data transfer agreements. The first of these was the ill-fated International Safe Harbour Privacy Principles ("Safe Harbour").[125] Safe Harbour was invalidated by the Court of Justice of the European Union in *Schrems v. Irish Data Protection Commissioner*.[126]

In *Schrems*, the Court found that Safe Harbour did not provide EU citizens with the privacy rights to which they were entitled under the EU Charter and under the Directive.[127] It noted that Safe Harbour only bound the private organizations that voluntarily agreed to adopt its principles and did not apply to governmental entities.[128] Further, the Court noted that under the agreement, factors such as law enforcement and national security took precedence to the Safe Harbour principles.[129] Thus, when a private entity faced a conflict between the Safe Harbour principles and complying with an order from the US authorities to turn over data, the entity would be required to turn over the data.[130] In the view of the Court, this created a direct route for data about EU residents to be transferred to entities not bound by Safe Harbour.[131]

The Court took issue with two aspects of US law: first, in its view, the access US authorities had to personal information was not proportional to the scope of national security and law enforcement interests, and second, US law did not provide administrative or judicial redress for EU residents.[132] Specifically, on the issue of proportionality, the Court asserted, "United States authorities were able to access the personal data transferred from the [EU] Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security."[133]

---

122 *See id.*
123 *Id.*
124 *See id.*
125 2000 O.J. (L 215) 7–47.
126 Case C-362/14, Schrems v. Irish Data Prot. Comm'r, 2015 E.C.R. I-650, ¶ 98.
127 *Id.* ¶ 87–98.
128 *Id.* ¶ 80–82.
129 *Id.* ¶ 86.
130 *Id.* ¶ 85.
131 *See id.* ¶ 87.
132 *Schrems*, 2015 E.C.R. ¶ 93–95.
133 *Id.* ¶ 90.

The issue of the absence of redress is addressed even more sharply. Article 47 of the EU Charter asserts a fundamental right to an effective remedy and to a fair trial. In the words of the Court, "data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased."[134] Thus the court found that:

> [L]egislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection . . . . The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the very existence of the rule of law.[135]

EU-US Privacy Shield ("Privacy Shield") is the current transatlantic data transfer agreement, which replaced Safe Harbour.[136] Like Safe Harbour, Privacy Shield is predicated on the fact that the EU does not consider the US to provide an adequate level of data protection as required by either the Directive or the GDPR.[137] The agreement recreates the Safe Harbour system where US companies voluntarily agree to be bound by a set a privacy principles subject to enforcement and oversight by the United States Department of Commerce.[138]

The Article 29 Working Party, an EU body responsible for providing guidance on privacy and data protection matters, recently conducted its first review of Privacy Shield.[139] The Working Party recognized that Privacy Shield provided improvements in data protections for EU citizens over Safe Harbour.[140] At the same time, the Working Party outlined numerous concerns regarding the operational aspects and implementation of privacy shield, data collection practices of the US government, and judicial remedies available to EU nationals.[141] The report noted that the "prioritized concerns need[ed] to be resolved by 25 May 2018," the same date the GDPR went into effect.[142] Privacy Shield remains in effect.[143]

---

134 *Id.*

135 *Id.* ¶ 95.

136 *See* 2016 O.J. (L 207) 2.

137 *See Id.*

138 *Id.* at 3; 2000 O.J. (L 215) 7–8.

139 Data Prot. Working Party, *EU–U.S. Privacy Shield – First Annual Joint Review*, at 2 (Nov. 28, 2017), https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782.

140 *See id.* at 4, 7.

141 *See generally id.* at 7–12, 14–19.

142 *Id.* at 20.

143 *See Welcome to the Privacy Shield*, U.S. DEP'T OF COMMERCE (last visited Nov. 17, 2019) https://www.privacyshield.gov/welcome.

C. *European Data Protection Board Guidance*

On November 16, 2018, the European Data Protection Board released guidelines on the territorial scope of the GDPR.[144] The guidelines were aimed at clarifying the extent to which Article 3 of the GDPR placed entities outside of the EU under the GDPR's data protection regime.[145] In reality, the guidelines were mostly just a restatement of the GDPR as it was enacted. They focused on the previously mentioned three instances in which a controller or processor might find itself under the coverage of the GDPR: (1) establishing the data controller or processor within the EU, (2) targeting individuals within the EU, and (3) applying EU law by virtue of international law.[146] The section briefly examines the establishment guidelines and the targeting guidelines, as the application of EU law by virtue of international law is largely beyond the scope of this Comment.

Looking to the establishment of a controller or processor within the EU instance in which the GDPR may apply, the EUDP recommended a "three-fold" approach.[147] The first consideration is whether the controller or processor has an establishment within the EU.[148] The threshold for this seems to be quite low, as the guidelines state:

> In order to determine whether an entity based outside the Union has an establishment in a Member State, both the degree of stability of the arrangements and the effective exercise of activities in that Member State must be considered in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet. The threshold for "stable arrangement" can actually be quite low when the centre of activities of a controller concerns the provision of services online. As a result, in some circumstances, the presence of one single employee or agent of the non-EU entity may be sufficient to constitute a stable arrangement if that employee or agent acts with a sufficient degree of stability.[149]

The guidelines note that while the "notion of establishment is broad, it is not without limits."[150] The only concrete limit provided is that simple web accessibility of an entity does not constitute an establishment.[151]

The next consideration in the establishment analysis is determining whether the processing of personal data occurs "in the context of the activities" of the establishment.[152] For this inquiry, the EUDP provided the

---

144 *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)*, EUROPEAN DATA PROT. BD. 1 (Nov. 16, 2018), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf [hereinafter *Guidelines 3/2018*].

145 *See id.* at 3.

146 *See id.*

147 *Id.* at 4.

148 *See id.*

149 *Id.* at 5.

150 *Guidelines 3/2018*, *supra* note 144, at 5.

151 *See id.*

152 *Id.* at 6.

recommendation that organizations determine whether personal data is being processed and then determine whether there are links between the processing and the activities of presence the organization has within the EU.[153] If such a link is found, the inquiry will turn upon whether the link to EU activities involves a relationship to an entity within the EU and the raising of revenue within the EU.[154]

The final consideration in the threefold analysis is essentially a directive to disregard where the processing takes place and the geographical locations of the individuals about whom the data is processed.[155] This means that the GDPR can apply to entities outside of the EU if they meet the first two considerations in the threefold analysis for establishment of data controller or processor.[156] This also means that the GDPR can apply to processing of data that is about individuals that are neither EU residents nor citizens.[157]

In introducing the discussion on targeting individuals within the EU, the guidelines note that the targeting criteria established within Article 3 of the GDPR represent a greater widening of the territorial scope beyond what is provided for in the establishment criteria.[158] The guidelines state that the inquiry under this portion of the territorial scope of the GDPR focuses on the specific process activities and must be performed on a "case-by-case basis."[159] The EDPB recommended a two-fold approach, one that first considers whether the personal data is related to data subjects residing within the EU and then considers whether the processing relates to the offering of goods and services within the EU.[160]

The first consideration under the targeting analysis is whether the personal data is about data subjects within the EU.[161] This analysis is not limited to nationality or legal status of the data subject in question.[162] Rather the inquiry turns on whether or not the data subject is within the EU at the time that the data processing occurs.[163] While this seems to be very open-ended, the guidelines note that this is limited by the second inquiry.[164]

The guidelines split the second inquiry into two subparts: (1) targeting in the context of offering goods or services, regardless of whether a payment is provided and (2) tracking of behavior that occurs within the EU.[165] The

153 *See id.*
154 *See id.* at 6–7.
155 *See id.* at 8–9.
156 *See Guidelines 3/2018*, *supra* note 144, at 8–9.
157 *See id.* at 9.
158 *See id.* at 12.
159 *Id*. at 13.
160 *See id.*
161 *See id.*
162 *See Guidelines 3/2018*, *supra* note 144, at 13.
163 *See id.*
164 *See id.* at 14.
165 *See id.* at 14, 17.

guidelines suggest that the following factors may be useful in determining whether goods or services are offered within the EU:

> * The EU or at least one Member State is designated by name with reference to the good or service offered;
>
> * The data controller or processor pays a search engine operator for an internet referencing service in order to facilitate access to its site by consumers in the Union; or the controller or processor has launched marketing and advertisement campaigns directed at an EU country audience[;]
>
> * The international nature of the activity at issue, such as certain tourist activities;
>
> * The mention of dedicated addresses or phone numbers to be reached from an EU country;
>
> * The use of a top-level domain name other than that of the third country in which the controller or processor is established, for example ".de", or the use of neutral top-level domain names such as ".eu";
>
> * The description of travel instructions from one or more other EU Member States to the place where the service is provided;
>
> * The mention of an international clientele composed of customers domiciled in various EU Member States, in particular by presentation of accounts written by such customers;
>
> * The use of a language or a currency other than that generally used in the trader's country, especially a language or currency of one or more EU Member states;
>
> * The data controller offers the delivery of goods in EU Member States.[166]

None of these factors are dispositive, and many will have to be considered in light of—and in combination with—each other.[167]

In determining whether or not behavior within the EU has been tracked, the EDPB recommends a similar multifaceted analysis.[168] The guidelines note that there is no intent requirement written into the GDPR in reference to the behavioral monitoring provision, but state that a consideration of intent is a natural part of the analysis.[169] It goes on to say that monitoring of behavior could "encompass a broad range of monitoring activities, including in particular:"[170]

> * Behavioural advertisement;
>
> * Geo-localisation activities, in particular for marketing purposes;
>
> * Online tracking through the use of cookies or other tracking techniques such as fingerprinting;
>
> * Personalised diet and health analytics services online;
>
> * CCTV;
>
> * Market surveys and other behavioural studies based on individual profiles;

---

166 *Id.* at 15–16.
167 *See id.* at 16.
168 *See Guidelines 3/2018*, *supra* note 144, at 17–18.
169 *See id.* at 18.
170 *Id.*

* Monitoring or regular reporting on an individual's health status.[171]

D. *Enforcement of Foreign Law in the US*

With the enactment of the GDPR, the EU codified its intention that its privacy regulatory regime apply outside of the territory of the EU. While EU member-state courts are clearly competent to enforce the provisions of the GDPR within the boundaries of the member states of the EU, how may the EU through its member states enforce the provisions of the GDPR outside of the EU, specifically in the United States? This Section discusses methods by which a foreign jurisdiction such as an EU member state may seek to enforce its law on entities in the United States.

A discussion about the applicability of one state's law in another state must necessarily begin with a discussion about jurisdiction. Jurisdiction is a term that has many meanings. In domestic law, jurisdiction is the competency of a state organ over a certain matter.[172] Even just within the international context, the term "jurisdiction" has multiple meanings.[173] The broadest of these meanings is the "right to regulate," or the right of one state in relation to another state.[174] Jurisdiction can also mean the physical territory of a state.[175] Finally, jurisdiction can mean the right of a court to hear an international dispute.[176]

Notwithstanding the concrete conceptions of jurisdiction is the more theoretical idea of what Professor Dan Jerker Svantesson refers to as the distinction of "bark jurisdiction" versus "bite jurisdiction."[177] This distinction recognizes that there are some jurisdictional claims that are not likely to be carried out in the real world.[178] Those jurisdictional claims are "bark jurisdiction."[179] Jurisdictional claims that are likely to be carried out in the real world are "bite jurisdiction."[180] Svantesson argues that while bark jurisdiction might seem like regulatory overreach or an act of futility, it can still have practical effects.[181]

Understanding the basic definitions of jurisdiction, the next step is to understand the judicial doctrine of comity. Comity in American law is best defined as "deference to foreign government actors that is not required by

---

171 *Id.*
172 *See* UTA KOHL, JURISDICTION AND THE INTERNET 14 (2007).
173 *See id.*
174 *Id.*
175 *See id.*
176 *See id.*
177 Svantesson, *supra* note 121, at 58–59.
178 *Id.*
179 *Id.*
180 *Id.*
181 *Id.* at 59.

international law but is incorporated in domestic law."[182] It can serve as the basis for applying foreign law or recognizing foreign judgments in US Courts.[183] The rule was laid down in *Hilton v. Guyot*,[184] where the Court noted:

> "Comity," in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens, or of other persons who are under the protection of its laws.[185]

Professor William Dodge observes that there are three types of comity in American law.[186] The first is prescriptive comity, which is best defined as one nation applying the laws of another nation in its courts in recognition of the other nation's jurisdiction to set rules for the event or transaction in question.[187] The next type is adjudicative comity, defined "in American law through the rules for recognizing foreign judgments."[188] Finally, there is sovereign party comity which allows sovereign states to sue in US courts.[189]

In considering the application of foreign law in US courts via the doctrine of comity, it is important to consider the distinction between public and private law. Private law is the set of obligations which arise from or are enforced under contract, tort, property law, and other civil matters.[190] Public law refers to criminal, tax, regulatory, administrative, and other types of law that are laid down by the state and represent an obligation placed on private citizens.[191]

The distinction between private and public law is found in American jurisprudence on foreign relations. The Restatement (Third) of the Foreign Relations Law of the United States provides a different set of rules for recognizing foreign judgments and for recognizing and enforcing foreign and penal judgments.[192] Generally, the judgments of foreign courts granting or denying recovery of money, relating to the status of a person, or determining property interests are entitled to recognition in US courts.[193] This largely

---

182 William S. Dodge, *International Comity in American Law*, 115 COLUM. L. REV. 2071, 2078 (2015).

183 *Id.* at 2089.

184 159 U.S. 113 (1895).

185 *Id.* at 163–64.

186 *See* Dodge, *supra* note 182, at 2079.

187 *Id.* at 2100.

188 *Id.* at 2105.

189 *Id.* at 2116.

190 *See* KOHL, *supra* note 172, at 19.

191 *Id.*

192 *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES §§ 481, 483 (AM. LAW. INST. 1987) [hereinafter RESTATEMENT (THIRD) FOREIGN RELATIONS].

193 *Id.* § 481.

follows the standard laid down in *Hilton v. Guyot*.[194] The entitlement to recognition is subject to certain limits.[195] Conversely, US courts are not required to recognize or enforce judgements for "the collection of taxes, fines, or penalties rendered by the courts of other states."[196]

Underlying the distinction between public and private law in regards to the recognition of foreign judgments is the long-held rule in Anglo-American law that courts will not enforce foreign penal statutes.[197] This rule first appeared in a 1789 English case, *Folliott v. Ogden*,[198] which somewhat ironically related to a confiscation order issued by the American revolutionary government.[199] In American law, the rule was laid down by Chief Justice John Marshall in *The Antelope*,[200] where he simply stated that "the Courts of no country execute the penal laws of another."[201] There does not appear to be any United States cases addressing the issue of enforcing foreign penal judgments in US courts.[202] The Supreme Court in *Huntington v. Attrill*[203] held that a judgment was penal when its only purpose was to compensate the state in its role as the representative of society for a public wrong and not when the judgment aided individuals.[204]

---

194 *See* 159 U.S. 113, 167–68 (1895) (listing the types of judgments that are "valid everywhere" and including those relating to title to property, those about marriage, and those resulting in money damages).

195 *See Id.* at 202–03. The Restatement details when United States courts may or need not recognize foreign judgments:

> (1) A court in the United States may not recognize a judgment of the court of a foreign state if:
> (a) [T]he judgment was rendered under a judicial system that does not provide impartial tribunals or procedures compatible with due process of law; or
> (b) the court that rendered the judgment did not have jurisdiction over the defendant in accordance with the law of the rendering state . . . .
> (2) A court in the United States need not recognize a judgment of the court of a foreign state if:
> (a) the court that rendered the judgment did not have jurisdiction of the subject matter of the action;
> (b) the defendant did not receive notice of the proceedings in sufficient time to enable him to defend;
> (c) the judgment was obtained by fraud;
> (d) the cause of action on which the judgment was based, or the judgment itself, is repugnant to the public policy of the United States or of the State where recognition is sought;
> (e) the judgment conflicts with another final judgment that is entitled to recognition; or
> (f) the proceeding in the foreign court was contrary to an agreement between the parties to submit the controversy on which the judgment is based to another forum.

RESTATEMENT (THIRD) FOREIGN RELATIONS, *supra* note 192, at § 482.

196 RESTATEMENT (THIRD) FOREIGN RELATIONS, *supra* note 192, at § 483.

197 *See* Thomas B. Stoel, Jr., *The Enforcement of Foreign Non-Criminal Penal and Revenue Judgments in England and the United States*, 16 INT'L & COMP. L.Q. 663, 664–65 (1967).

198 Folliott v. Ogden, [1789] 126 Eng. Rep. 75 (Ct. Com. Pl. 1789), *aff'd*, [1790] 100 Eng. Rep. 825 (Ch.).

199 *See* Stoel, *supra* note 197, at 664.

200 23 U.S. (10 Wheat.) 66 (1825).

201 *Id.* at 123.

202 Stoel, *supra* note 197, at 667.

203 146 U.S. 657 (1892).

204 *See id.* at 664–65.

II. ENFORCEMENT OF THE GDPR IN THE US

With an understanding of the GDPR, the legal issues surrounding data transfer in and out of the EU, and the applicability of foreign law within the US, this Comment shifts to a discussion of the how the GDPR might be applied in the US. The EU has the option of attempting to have judgments rendered by its member-states' courts recognized by US courts. The EU also has the option of using Privacy Shield as a way to coax US authorities into cooperating with EU data protection authorities. The upshot is that the EU has a limited set of legal options for pursuing compliance.

Building on Svantesson's concept of "bark" and "bite" jurisdiction, the EU may find itself in what could be called a "dog's fence" scenario. Picture this: a family with a dog wants to let the dog outside to roam about the yard but does not want to have to accompany the dog with a leash or build a fence. Many families solve this problem by purchasing an electric fence. This "electric fence" is a buried wire that, as the dog approaches, causes a special collar worn by the dog to make a sound, and if the dog crosses the buried wire, delivers a small electric shock to the dog. The dog is trained via positive (and at times, negative) reinforcement to not cross this invisible barrier.

Squirrels and rabbits that the dog loves to chase, via trial and error, soon learn that there is an invisible barrier the dog will not cross. They soon begin to sit just across the electric fence line where they know the dog cannot get them. The dog barks itself hoarse but is powerless to chase the squirrels and rabbits. In the scenarios contemplated by this Comment, the EU is the dog and US companies without an EU footprint are squirrels and rabbits sitting on the opposite side of the electric fence, the borders of the United States.

A. *Judicial Enforcement of the GDPR*

The EU could seek to enforce the GDPR via the US judicial system. This could take a number of forms. An EU citizen could seek to have a judgment rendered under the GDPR's private right of action recognized in a US court. An EU data protection authority could seek to have its penalties recognized by US courts. Finally, an EU member state as a sovereign could attempt to bring suit against a private entity in the US.

To consider the EU's options for enforcing the GDPR in the US via the courts, one first needs to determine the nature of the fines assessed by the GDPR. Are they penal? Are they compensatory to the individual harmed by the violation of the regulation? As discussed above, the nature of the fines is at the heart of the legal analysis for whether foreign law can be enforced in the United States.[205]

---

205 *See* Stoel, *supra* note 197, at 665–67.

The GDPR has a number of avenues for penalizing data controllers and processors who violate its requirements. The GDPR creates a private right of action for individuals who have been harmed by a violation of the regulation.[206] Action can be brought in member-state courts under the GDPR and processors are held jointly and severally liable for the damage caused by the violation of the regulation.[207] Supervisory authorities are empowered to impose administrative fines against entities found in violation of the GDPR.[208] Finally, member states are directed to enact rules for "other penalties" for violating the GDPR.[209]

The best chance the EU has for the GDPR being enforced in US courts is through individuals bringing suits under the private right of action the GDPR creates. An EU national would bring a suit against a US entity under the GDPR in a member-state's court. The US entity could either appear or not appear and allow default judgment to be entered. The EU national could then seek to have the judgment enforced in US court.

Assuming the matter was appropriately adjudicated in the EU member states' court system, an EU national could ask a US court to look to the doctrine of adjudicative comity to enforce the judgment. The judgment rendered under the GDPR's private right of action is essentially a matter of private law and relates to the granting or denial of recovery for money. This falls within the comity doctrine enunciated by both The Restatement (Third) of Foreign Relations Law of the United States and *Hilton v. Guyot*.[210] Thus, absent prudential determinations made by a judge, it is plausible that an EU national could recover a judgment against a US entity made in EU court under the GDPR's private right of action.

The outlook for data protection authorities seeking to enforce the GDPR is less sunny. A primary mode of enforcement for data protection authorities is the significant administrative penalties that can be levied. In seeking to enforce the GDPR in the US by levying administrative penalties, the important determination to be made is whether the GDPR is a "penal statute" as referenced in *The Antelope* and *Huntington v. Attrill*.[211] If the GDPR is a penal statute, then a US court will not enforce it.

From a plain reading of the GDPR, it is difficult to see how a US court would not characterize it as a penal statute. Using the terminology from the definition of a penal statute in *Huntington v. Attrill*,[212] the purpose of administrative penalties is to compensate the data protection authorities in their role

---

206 2016 O.J. (L 119) 81–82.

207 *Id.* at 82.

208 *Id.*

209 *Id.* at 83.

210 *See* 159 U.S. 113, 163–64 (1895); RESTATEMENT (THIRD) FOREIGN RELATIONS, *supra* note 192, § 481.

211 *See* 146 U.S. 657, 666 (1892); The Antelope, 23 U.S. (10 Wheat.) 66, 123 (1825).

212 *See Huntington*, 146 U.S. at 673–74 ("The question . . . depends upon . . . whether its purpose is to punish an offense against the public justice of the state, or to afford a private remedy to a person injured by the wrongful act.").

as the representative for society for the public wrong of violating the privacy rights of EU citizens. The administrative penalties do not serve the purpose of compensating individuals; that is the role of the private right of action. Since the administrative penalties are simply a punitive measure that compensate the state, a US court would likely consider the GDPR to be a penal statute in that context and therefore would not enforce it within the US.

An EU member state could look to the doctrine of sovereign party comity to enforce the GDPR in US courts. This has a low chance of success. It is not clear what cause of action could be brought that would not implicate the rule from *The Antelope* of not enforcing foreign penal statutes. For example, seeking to enjoin a party from violating the GDPR is just a backdoor to enforcing a foreign penal statute. Additionally, it is not likely that a court would allow an EU sovereign to bring a cause of action based upon a private right of action in EU law. The private right of action is clearly reserved for private parties and not extended to the sovereign.

B. *Privacy Shield as a Bargaining Chip*

Considered as a whole, enforcement of the GDPR in the US is as much a legal question as it is a diplomatic one. The EU would be none too thrilled at the US harboring bands of internet scofflaws who refuse to comply with EU data protection regulations while processing and storing data about EU nationals. On the other hand, the US would be none too thrilled at the prospect of European data protection authorities harassing US-based businesses with only minimal or coincidental contacts in the EU.

Both the EU and the US must engage in a balancing exercise. For the US, it becomes an exercise in balancing the interest in preserving sovereignty and maintaining a positive relationship with one of the largest economic blocs in the world. For the EU, it becomes an exercise in balancing the interest of upholding the rule of law and maintaining a positive relationship with the country that is home to almost all of the internet giants.

In analyzing the issue of enforcing the GDPR in the US, a primary consideration is the leverage which the two parties possess. The US is home to Facebook, Google, LinkedIn, Twitter, Amazon, Microsoft, Apple, and an almost endless number of online platforms used every day by millions of Europeans. This is a double-edged sword for the US. On the one hand, the EU has an interest in ensuring its citizens and companies have access to these platforms that make EU commerce possible. On the other hand, the US has an interest in ensuring that its largest corporations have access to an enormous market. The question is: which party is more likely to blink first?

The EU has sent mixed signals as to its negotiating position on privacy law in the US. The replacement of Safe Harbour with Privacy Shield in the wake of *Schrems* seems to signal that the EU is willing to "look the other way" in regard to the US's comparatively lax approach to privacy. The reality is that Privacy Shield is basically a rebranding of Safe Harbour with a couple

of minor concessions from the US. One of the core issues at the heart of *Schrems*, the National Security Agency's bulk collection of telephone records, is largely the same now as when *Schrems* was decided.[213] Conversely, its recent aggressive moves in the areas of competition policy signal that the EU may be taking a new, more assertive approach to what it sees as "bad behavior" by US companies.[214]

The leverage the EU seems to have over the US is Privacy Shield. Since Privacy Shield is a political agreement between the two jurisdictions, it is subject to larger political considerations. The EU could take the position that repeated violations of the GDPR by companies that do not have an EU presence threatens the validity of Privacy Shield's underlying adequacy decision. This would then predicate the viability of Privacy Shield as a means for legal data transfer in and out of the EU on the US effectively policing companies that were subject to the GDPR's requirements.

A concession the EU could likely get from the US would be more coordination and cooperation in the enforcement of the GDPR by EU data protection authorities. For the EU to obtain this concession, the US would have to recognize that the EU has a valid jurisdictional claim over the companies doing the processing. The theoretical underpinning for this jurisdictional claim could come from what Svantesson calls "market sovereignty."[215] Market sovereignty is based on a sovereign's ability to take "market destroying measures" on the market in which conduct occurs.[216]

While market sovereignty provides a good theoretical underpinning for a claim that the GDPR should be enforced on US entities without an EU presence, the US could simply recognize the prudential issues at play. The EU is a very large market in which many US companies have substantial customer bases. The deeper political issues and how they might play out is beyond the scope of this Comment, but the important takeaway is that the legal issue of GDPR enforcement outside of the EU does not exist in a vacuum.

III. WHEN A US ENTITY IS SUBJECT TO THE GDPR

US-based entities have an important strategic decision to make. The GDPR, by design, has a potentially global reach. Depending on the type of data an organization processes, compliance—and its cost—may range from a minor annoyance to a majorly disruptive undertaking. Multinational

---

213 While Congress enacted the USA FREEDOM Act, the changes it made were minor and did nothing to address the issues at the heart of the Schrems case. *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

214 *See, e.g.*, Mark Scott, *Google Fined Record $2.7 Billion in E.U. Antitrust Ruling*, N.Y. TIMES (June 27, 2017), https://www.nytimes.com/2017/06/27/technology/eu-google-fine.html.

215 *See* Svantesson, *supra* note 121, at 99.

216 *Id.*

corporations with a presence in the EU will have no choice but to comply. But when the size of an entity decreases and its corporate footprint does not extend to the EU, the calculus changes. This Section sketches a pair of hypotheticals and uses them to discuss the implications of the GDPR for US-based companies.

A. *A Deep South Small Business and a Silicon Valley Startup*

Consider this scenario: Boone and his wife Margaret have a small business that they run out of their home in Mobile, Alabama. Boone is a general contractor and does remodeling and additions to residential homes. Margaret is an architect and designer. She designs the remodeling projects and additions that Boone builds. Their business activities are limited to South Alabama and the parts of Florida and Mississippi that are within about an hour's drive.

Wanting to build their business and attract more customers, Boone and Margaret decide to get a website. They know a teenager from church who knows the technical jargon like HTML and search-engine optimization. They pay her to build a rudimentary, noninteractive website for their business. The website contains photos of past projects, profiles of both Boone and Margaret, and a form for submitting a request for a quote. The teenager also sets up a backend log file analyzer, AWStats, for the site. AWStats processes the log files generated by webservers into graphs and other useful tools for analyzing web traffic.[217]

Helmut lives a few miles outside of Munich, Germany. He comes across Boone and Margaret's site in a Google Search. He clicks the link in the search results and is on the site for no more than ten seconds before he realizes it is irrelevant. In that ten seconds, his IP address was recorded in a log file on the server hosting Boone and Margaret's website. Curious about her website's traffic, Margaret downloads to her computer a .CSV of the information collected by AWStats. This .CSV file contains the information collected in the webserver log files, including IP addresses.[218]

Consider another scenario: Piper and Riley are friends from their college days. They both have a passion for coding apps. After barely finishing their undergraduate degrees, they both moved to Silicon Valley with the hopes of being the next Facebook. After several grueling months of nonstop coding, Piper and Riley have workable beta for their ingenious social media platform.

To register and use the platform, a user must provide his name and email address. He also has the option of providing his date of birth, geographic location, and various other pieces of data about his interests and background,

---

217 *See What Is AWStats*, AWSTATS OFFICIAL WEB SITE, https://awstats.sourceforge.io/ (last visited Aug. 7, 2019).

218 *See id.*

but none of this information is required. The platform allows users to trade messages with each other in private and public.

The social media platform does not have a specific audience. It is written in English and operates on the internet, so it is available to anyone with an internet connection. Piper played around with a couple of code libraries that will translate the site into a handful of foreign languages, but she has no idea if the function actually works or just produces gibberish. To make the platform sound sophisticated, Piper and Riley often refer to it as a "global" platform when promoting it to their family and friends. Like almost every other social media platform, it is free to use.

Piper and Riley have not put much thought into the legal ramifications of operating a social media platform beyond Piper using LegalZoom to form a limited liability company and Riley finding some generic terms of service for the website. The generic terms of service have a few things about privacy in them, but they are as boring as the iTunes agreement Riley has never read, so he does not read his site's terms either.

With most of the coding done and the beta live, Piper and Riley are now in the process of recruiting users. The ultimate goal is for the site to go viral and for venture capitalists to flood Piper and Riley with offers for funding. So far, their attempts at making the site go viral have not worked. Their user base is limited to family, friends, and some acquaintances from college.

Thousands of miles away, in Amsterdam, the Netherlands, Sophie is an American expat who works for a multinational consultancy. She had a few classes with Riley in college and generally thought well of him. They are Facebook friends, and she saw him post about the platform. In a show of support for her old friend, Sophie decides to sign up. After only a few days of use, Sophie thinks that the platform is fantastic. She convinces a number of her American expat friends and a few friends from Europe to sign up for it.

B. *Reach of the GDPR*

The discussion now turns to whether the activities of the companies sketched above implicate EU law. In both scenarios, the fictitious companies are in possession of data about EU nationals. Boone and Margaret have Helmut's IP address and could possibly have the IP addresses of other EU nationals who happen to stumble upon their site. Piper and Riley run a social media platform that has collected the names and email addresses of many EU nationals and private messages between EU nationals are being created at a steady rate each day.

1. Data Controllers and Processors

Looking first to Boone and Margaret, we must determine whether their company is a data controller or processor. To perform this inquiry, they must determine whether they possess data that is personal information under the GDPR and whether the activities that Boone and Margaret are performing are processing under the GDPR.[219] Examining the facts leads to the conclusion that Boone and Margaret's company is both a data controller and processor.

In this scenario, Boone and Margaret's company is in possession of the IP address of Helmut, an EU national, and operates a web server that collects the IP addresses of EU nationals like Helmut. IP addresses are explicitly considered personal information under the GDPR.[220] The personal information is being processed because it is, at least, being collected and stored.[221] Boone and Margaret's company is a data controller because it determines the purposes and means of data processing.[222] It was the company's decision to establish the website and to set up the analytics page. The company is also a data processor because it is processing the personal information by collecting, structuring it, and storing it.[223]

Looking now to Piper and Riley's company, it must also be determined if it is a data controller or processor. Piper and Riley's company is in possession of at least the names and email addresses of several EU nationals. Names and email addresses are personal information under the GDPR because names are specifically mentioned in the definition of personal information and because email addresses are a basic example of an online identifier.[224] The personal information in question is being processed because it is, at a minimum, being collected, structured, stored, and disseminated. The company is also a data controller because it designed, implemented, and operates and maintains the platform. These are clear examples of exercises in determining the means and purposes of processing, as it is defined in the GDPR.[225] Finally, the company is a data processor because it is the entity that is processing the data by collecting, storing it, and disseminating it.[226]

---

219 *See* 2016 O.J. (L 119) 33.
220 *See id.* at 6, 33.
221 *See id.* at 33.
222 *See id.*
223 *See id.*
224 *See id.*
225 *See* 2016 O.J. (L 119) 33.
226 *See id.*

2. Scope of the GDPR

Now that it has been determined that both entities are data processors and controllers, it must be determined whether they fall under the scope of the GDPR. This inquiry first requires making a determination about the material scope of the GDPR in relation to both entities, followed by a determination about the territorial scope in relation to the entities. The analysis leads to the conclusion that the activities of both Boone and Margaret's company and Piper and Riley's company would fall under the material and territorial scope of the GDPR.

The analysis for determining whether Boone and Margaret's company and Piper and Riley's company are within the material scope of the GDPR is relatively straightforward. The GDPR materially applies to the processing of personal information wholly or partially by automated means.[227] Based on the determinations made above regarding whether both companies qualify as data controllers, it is clear that they are processing personal information by automated means. Further, neither company is subject to any of the exceptions to the territorial scope of the GDPR.[228] Therefore, the activities of both companies are within the material scope of the GDPR.

The analysis for determining whether either company fits within the territorial scope of the GDPR is a bit more nuanced. As laid out in Article 3 of the GDPR, there are three instances that fall within the territorial scope of the GDPR.[229] Two of them—sections 1 and 3—do not apply to the companies sketched out here,[230] leaving section 2 as the only reasonable way that either Boone and Margaret's company or Piper and Riley's company could be within the territorial scope of the GDPR.

Section 2 includes the processing of personal information about data subjects within the EU by data processors or controllers outside of the EU.[231] It has already been determined that both entities in the discussion are data controllers and processors under the GDPR, so section 2 could potentially

---

227 *Id.* at 32.

228 *See id.* (exempting from the GDPR's material scope activities occurring outside of the scope of EU, activities related to certain law enforcement and national security, and data that is collected for personal household use).

229 This include activities related to the establishment of a controller or processor within the EU, the processing of personal data about data subjects residing within the EU by data controllers outside of the EU in certain instances, and situations where EU member state law applies by virtue of international law. *See id.* at 32–33.

230 Neither Boone and Margaret's company nor Piper and Riley's company are attempting to set up a data controller or processor within the EU, so Article 3 section 1 does not apply. In regard to section 3, which provides that the GDPR applies where EU member state law "applies by virtue of public international law," the GDPR does not seem to contemplate that in the instance of either company. *See id.* at 5, 33. Recital 25 provides as an example, a member state's diplomatic outpost. *Id.* at 5. There does not seem to be any principle of public international law that applies to either situation envisioned in this discussion, nor is a diplomatic outpost involved, so section 3 does not apply.

231 2016 O.J. (L 119) 33.

apply. But section 2 limits its applicability to instances where processing is related to the offering of good services to data subjects within the EU, even if payment is not required, and to instances where the processing is used to monitor behavior of EU data subjects that occurs within the EU.[232]

Starting with Boone and Margaret's company, it is not clear whether their company's processing activities fall within the scope of section 2. The company is located outside of the EU and is processing data about a data subject within the EU. Their company is clearly not offering goods or services to anyone within the EU, including Helmut. But the question remains as to whether or not the processing activity related to website analytics constitutes monitoring behavior that occurs within the EU. Recital 24 notes that the determination is based on whether natural persons are tracked on the internet including whether the processing can help predict future behavior.[233]

The basic purpose of website analytics is to track a person's online activity. One could argue that the purpose is not to track *individuals*, but to detect larger behavioral patterns of groups of people. Further, one could also argue that the best reading of Recital 24 would be for activities that go above and beyond a simple log file and basic web analytics. Neither of these arguments, when taken in light of the fact that the GDPR explicitly expanded the definition of personal information to include IP address, seems to be persuasive. The EU's intent in enacting the GDPR was clearly to place limitations on the ability of data controllers and processors to track online activities. Absent a clear statement within the GDPR itself, or by the Article 29 Working Party, or a member state court, there is no reason to doubt that website analytics are not covered by the GDPR. Therefore, it is at least plausible that Boone and Margaret's company could fall within the territorial scope of the GDPR.

Turning to Piper and Riley's company, it is more likely that their company's processing activities would fall within the territorial scope of the GDPR. As determined above, the company is both a data controller and processor. It is located outside of the EU and, due to its growing user base in Amsterdam, has personal information about individuals within the EU.

It is quite plausible that an EU court would find that Piper and Riley's company tracks the behavior of data subjects in the EU. To use the social media platform, users are required to register. As with any social media platform, users record their activities on the platform via postings and messages to others. Further, any site with a login capability likely uses cookies, which track the online behavior of users, even if only limited to activity within the same site.[234] Therefore, it is likely that Piper and Riley's company falls within the territorial scope of the GDPR.

---

232 *Id.*

233 *Id.* at 5.

234 *HTTP Cookies*, MOZILLA DEVELOPER NETWORK, https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies (last visited Jan. 9, 2020).

An additional question to consider is whether Piper and Riley's company is offering a service to the data subjects that are within the EU. Pursuant to Recital 23, this seems to turn on whether an entity "envisages offering services to data subjects in one or more Member States in the Union."[235] Thus, the question is whether or not it was foreseeable that the social media platform would attract users within the EU. While the mere availability of the site in the EU and the use of the site by EU residents is not sufficient to show intent, the availability of other languages on the site may show that a company considered the possibility that it would be offering services in the EU.[236]

A court could plausibly find that Piper and Riley's company envisaged offering services to data subjects in the EU. The site had a built-in translation service. Riley posted on his Facebook page that the site had an international reach, and the website described itself as a global social media platform. These are all factors that demonstrate that the company was aware that it could reasonably be offering services to data subjects within the EU. Thus, the company could also potentially fall within the territorial scope of the EU based on this part of Article 3.[237]

C. *Proactive Steps to Avoid EU Liability*

Boone and Margaret's company and Piper and Riley's company could take proactive measures to ensure they do not fall within the scope of the GDPR. These measures fit within two categories: technical measures and legal measures. Neither type of measure presents an overly attractive option for either company.

The most obvious technical measure either company could take is to block any traffic from within the EU. There are a number of services available that allow a website owner to block internet traffic based on its country of origin.[238] But this is not foolproof. Blocking internet traffic from a country is typically done by blocking all IP addresses from that country.[239] If the list is not accurate or up to date, internet users in the EU could still access the site. Further, there could be instances where a user's IP address does not actually reflect his geographic location such a through a virtual private network, a proxy, or while using a network that uses network address translation.

A technical remedy unavailable to Boone and Margaret's company but available to Piper and Riley's company would be to require users to disclose from what country they are using the platform and simply not allow people

---

235 2016 O.J. (L 119) 5.

236 *See id.*

237 *See id.* at 32–33.

238 *See, e.g.*, *Block or Allow Network Access By Country*, COUNTRY IP BLOCKS, https://www.countryipblocks.net/ (last visited Jan. 9, 2020); *Block Visitors by Country Using Firewall*, IP2LOCATION, https://www.ip2location.com/free/visitor-blocker (last visited Jan. 9, 2020).

239 *See Block Visitors by Country Using Firewall*, *supra* note 238.

within the EU to sign up for the service. This is unattractive for two reasons. First, it closes off a very large market for Piper and Riley's company. Second, it depends on users being honest about the country from which they are using the platform.

Other options both companies could pursue include the derogations or carve outs that GDPR provides to entities in countries that do not provide an adequate level of protection or a certification under Privacy Shield. Either of these options has the potential to be time consuming and costly for small and fledgling businesses. This is an especially impracticable solution for a small business like Boone and Margaret's that has no interest in doing business with entities within the EU. But this is simply the reality of the GDPR: a regulation that spans the globe and potentially covers every entity with a digital presence.

IV. WHERE DO WE GO FROM HERE?

This Comment contains a long and somewhat arduous discussion of the GDPR and its applicability to a couple of very different small businesses located within the US and totally outside of the EU. The underlying point is to illustrate that the GDPR is an ambitious legislative project undertaken by the EU. It is almost cliché to remark that the internet is a global phenomenon, but it is nonetheless true. The GDPR's extraterritorial applicability merely recognizes that fact.

In enacting the GDPR and attempting to give it extraterritorial effect, the EU made a decision, either consciously or unconsciously, to create a de facto global privacy standard. While that may not have been the intent of the EU, that is likely the practical effect. Multinational companies effectively have no choice but to comply with the GDPR. As demonstrated above, virtually any company that has any potential international contacts should consider taking steps to achieve GDPR compliance. Absent walling itself off from the whole of the EU, any company with an internet presence faces potential liability.

While it is true that any internet-connected company could face liability under the GDPR, the real question is the likelihood of consequences. It is highly likely that a multinational company with an EU presence would face an enforcement action if it has violated the GDPR. But thinking back to Boone and Margaret, it is not likely that their company would ever face an enforcement action. Data protection authorities have limited time and limited resources. Going after a couple of small business owners in a state most people in Europe have never heard of simply does not make sense.

Having answered the questions of what is likely to happen to big, international companies and what is likely to happen to small, purely domestic ones, the question remains about every company between those two extremes. There are likely thousands of companies like Piper and Riley's that have a purely domestic presence but have the potential to reach into

international markets. Any solution will require both the EU and the US to make concessions to each other.

The EU and the member states' data protection authorities will have to decide how aggressively GDPR violations by companies outside of the EU will be policed. In practice, the EU will have to draw a line between de minimis violations and substantive violations. An economic approach could be employed that weighs the cost of enforcing a given violation against the putative injury it caused. When the latter is greater by a satisfactory margin, the EU should attempt to bring an enforcement action against the US company.

Prudential factors should also be considered. While whether an entity was knowingly courting European business is a part of some of the analysis in determining whether an entity is a data controller or processor, as demonstrated above, there are situations where an entity could be a data controller or processor and not even know it. The EU should decline to bring enforcement actions on these types of cases. The GDPR also grants supervisory authorities with certain powers to remedy violations of the GDPR before resorting to penalties.[240] Wherever possible, the European authorities should use these measures against US companies instead of penalties. The aim is for the EU and its member states' data protection authorities to exercise a type of prosecutorial discretion that effectively protects the privacy of EU nationals while respecting US sovereignty.

The US will have to assist the EU in enforcing the GDPR by cooperation. The US has already taken steps to cooperate with the EU's enforcement of its data protection regime via Safe Harbour and Privacy Shield. Given that both of those agreements were enacted when the Directive was the operative privacy law in the EU, it follows logically that a transatlantic data transfer agreement should be updated to reflect the operation of the GDPR.

While Svantesson's idea of economic sovereignty provides a good theoretical underpinning for the EU to assert jurisdiction over US entities processing GDPR data, practical considerations limit its usefulness. US comity doctrine greatly limits a foreign state's ability to enforce any type of administrative penalties in US courts.[241] It is also not clear that companies in the US that have no EU presence would voluntarily consent to a European court's jurisdiction. Further, this concept of sovereignty completely displaces the classic notion of sovereignty that has been enshrined in law for centuries. While economic sovereignty is an elegant solution to a messy problem like jurisdiction over activities that occur purely on the internet, it is difficult to see such an ancient and bedrock idea like sovereignty be changed so quickly.

Professor Svantesson also argues that under the doctrine of economic sovereignty, technology allows those who wish not to be subject to a certain jurisdiction to wall themselves off from that jurisdiction.[242] While this is true, US companies refusing to do business with EU nationals is an outcome that

---

240 *See* 2016 O.J. (L 119) 69–70.

241 *See* Dodge, *supra* note 182, at 2078–79.

242 *See* Svantesson, *supra* note 121, at 99–100.

both jurisdictions would likely want to avoid. The EU is a large market and the US has been a breeding ground for many online companies that are a part of many Europeans' everyday lives. A more flexible approach as discussed above is preferable to an all or nothing approach where US-only companies are subjected to the full brunt of European law or choose to not do business with Europe at all.

Economic sovereignty also blurs the distinction between an entity that has consciously availed itself of customers within a jurisdiction and one that has not. An entity that has actively sought customers in the EU made a conscious decision to do so and thus implicitly consents to be bound by the laws of that jurisdiction. But, as in the case of both Boone and Margaret's company and Piper and Riley's company, there are many instances where contact with the data of an EU national happened not because of the actions of the company, but by the actions of the EU national. A foreign government attempting to assert jurisdiction over a US entity based on the contacts an EU national made with the US entity, of which the US entity was not even aware occurred at the time, would be a bizarre and antidemocratic outcome. Ignorance of the law may be no excuse, but ignorance of which country's citizen's actions will subject you that country's jurisdiction should be.

CONCLUSION

Globalization is here, and it is here to stay. Data will continue to flow between the EU and the US. Given the economic implications, policymakers in both jurisdictions likely do not want to countenance a scenario where each jurisdiction walls off the internet from the other. Recognizing this, the US has an interest in allowing the EU to protect rights of its citizens as they are enumerated in the Charter, and the EU has an interest in not taking a heavy-handed approach to enforcement of the GDPR.

The GDPR has the potential to cover every company in the world that is connected to the internet. It carries a hefty set of penalties and opens companies to potential liability from private suits. The EU must recognize the size and scale of regulatory regime it has created and the potential impacts it will have outside of its borders. While the EU has a responsibility to its citizens to protect their privacy, it must not overstep the sovereignty of other nations like the US. At the same time, the US must recognize that activities that physically occur within its boundaries digitally affect citizens in other countries. This Comment calls for cooperation between sovereign states and the larger international organization of which they are members using proven existing diplomatic and legal frameworks.