Boston College Law Review

Volume 59 | Issue 4 Article 9

4-26-2018

The Face-Off Between Data Privacy and Discovery: Why U.S. Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information

Samantha Cutler
Boston College Law School, samantha.cutler@bc.edu

THE FACE-OFF BETWEEN DATA PRIVACY AND DISCOVERY: WHY U.S. COURTS SHOULD RESPECT EU DATA PRIVACY LAW WHEN CONSIDERING THE PRODUCTION OF PROTECTED INFORMATION

Abstract: When foreign parties involved in U.S. litigation are ordered to produce information that is protected by EU data privacy law, they are caught in an unfortunate "Catch-22." Historically, U.S. courts have pointed to the unlikelihood of sanctions for data privacy law violations to justify these orders. EU data privacy law, however, has recently undergone several shifts in favor of tougher rules and significantly increased sanctions. Additionally, EU regulators are now more vigilant and active in enforcing these laws. These developments, combined with the benefits of international judicial respect and the intrinsic value of privacy, mean that U.S. courts should more strongly consider EU data privacy law in discovery deliberations. This Note argues that courts should more heavily weigh the interests of foreign nations and the hardship on foreign litigants when contemplating discovery orders and, when appropriate, order discovery to be conducted through the Hague Evidence Convention rather than by the foreign party.

INTRODUCTION

As technology develops and more information is stored and accessible online, the risks regarding the security of that information increase, requiring the law to keep up.[1] In recent years, several major shifts have occurred in EU data privacy law that affect companies in the United States and around the world.[2] These changes have occurred in tandem with an increased EU vigilance for data privacy and for pursuing those who threaten it.[3]

---

[1] *See* SEDONA CONFERENCE, THE SEDONA CONFERENCE COMMENTARY ON PRIVACY AND INFORMATION SECURITY: PRINCIPLES AND GUIDELINES FOR LAWYERS, LAW FIRMS, AND OTHER LEGAL SERVICE PROVIDERS 11 (2015), https://iapp.org/media/pdf/resource_center/Sedona_Privacy_InfoSec_Law-firms.pdf [https://perma.cc/CY5L-VFDE] (observing that data privacy laws have developed in response to massive data breaches); Morgan A. Corley, *The Need for an International Convention on Data Privacy: Taking a Cue from the CISG*, 41 BROOK. J. INT'L L. 721, 721–22 (2016) (noting that technological advances and the increased movement of personal information has resulted in a rise in data breaches); *Protection of Personal Data*, EUR. COMM'N, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en [https://perma.cc/57JG-F3BG] (pointing out that individuals entrust their personal information to third parties for everyday actions).

[2] *See* McKay Cunningham, *Complying with International Data Protection Law*, 84 U. CIN. L. REV. 421, 421 (2016) (explaining how businesses with even negligible foreign relationships may

In U.S. litigation, discovery orders often run up against data privacy laws.[4] Foreign litigants can find themselves in a quandary when they are ordered to produce information that is protected by foreign data privacy laws.[5] U.S. courts have frequently dismissed the consequences of ordering litigants to violate EU data privacy laws by pointing to the unlikelihood of their enforcement.[6]

This Note discusses the increasing importance of EU data privacy law in discovery deliberations.[7] Part I provides a brief history of EU data privacy law, including the development of more stringent rules and sanctions.[8] It then highlights the recent increase in EU enforcement actions for data privacy violations.[9] Part II discusses the conflict between EU data privacy law and U.S. discovery procedures.[10] Part III argues that U.S. courts should adjust their approach to discovery orders that contravene EU data privacy law by more strongly considering the hardship placed on foreign litigants, as well as the intrinsic value of privacy.[11]

I. THE DEVELOPMENT OF DATA PRIVACY LAW IN THE EUROPEAN UNION

Data privacy law governs the collection, use, processing, preservation, and divulgence of personal information.[12] Personal information is defined broadly, so data privacy law applies to most U.S. businesses.[13] Rather than a

---

be subjected to or impacted by foreign data privacy law); Sam Schechner, *Ireland's Privacy Cop Picks Up the Beat: Irish Data-Protection Chief Helen Dixon Sets Pace for EU Monitoring of Global Tech Giants*, WALL STREET J. (Dec. 27, 2016), https://www.wsj.com/articles/irelands-privacy-cop-picks-up-the-beat-1482855575 [https://perma.cc/XTC7-QA27] [hereinafter Schechner, *Ireland's Privacy Cop*] (quoting Irish Data Privacy Commissioner Helen Dixon who said that EU data privacy laws will serve as a benchmark for the rest of the world).

[3] *See infra* notes 67–84 and accompanying text.

[4] SEDONA CONFERENCE, INTERNATIONAL PRINCIPLES ON DISCOVERY, DISCLOSURE & DATA PROTECTION: BEST PRACTICES, RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING THE PRESERVATION DISCOVERY OF PROTECTED DATA IN U.S. LITIGATION 2 (Amor A. Esteban ed., 2011), https://theedonaconference.org/system/files/sites/sedona.civicactions.net/files/private/drupal/filesys/publications/International%20Litigation%20Principles_Transitional%20Ed_Jan%202017.pdf [https://perma.cc/SUL4-7PV8] [hereinafter INTERNATIONAL PRINCIPLES ON DISCOVERY].

[5] Steven C. Bennett, *EU Privacy Shield: Practical Implications for U.S. Litigation*, 62 PRAC. L. 60, 60 (2016).

[6] *Id.* at 63.

[7] *See infra* notes 12–188 and accompanying text.

[8] *See infra* notes 12–65 and accompanying text.

[9] *See infra* notes 67–84 and accompanying text.

[10] *See infra* notes 85–142 and accompanying text.

[11] *See infra* notes 143–169 and accompanying text.

[12] Brian M. Gaff et al., *Privacy and Data Security*, 2012 COMPUTER 9, 9, http://www.edwardswildman.com/files/upload/March%202012.pdf [https://perma.cc/QB4N-N3ZD].

[13] *Id.*; *101: Data Protection*, PRIVACY INT'L, https://privacyinternational.org/explainer/41/101-data-protection [https://perma.cc/8H37-E28Q]. Personal information includes any type of information that can be used to identify someone. Gaff et al., *supra* note 12. It can encompass simple

single law, a continually broadening assemblage of statutes, regulations, common law duties, contractual commitments, industry norms, and international obligations govern U.S. data privacy practices.[14] Agreements between the United States and the European Union are an important source of data privacy law.[15]

Despite differing approaches to protecting personal information, the United States and the European Union have deliberately and continuously endeavored to cooperate with one another.[16] As an economic region with significant market power and a hub for U.S. trade and investment, the European Union has substantial negotiating power on data privacy matters.[17] U.S. businesses with operations in the European Union rely on EU-U.S. information exchanges, so any possible limitations on those exchanges are highly consequential.[18]

Despite the European Union's strong position, the United States persists as a powerful adversary at the negotiating table because the U.S. economy is the largest international arena for EU companies.[19] Both the United States and the European Union had good reason to negotiate a solution to

---

data like names, birth dates, and contact information, or more obscure data like financial or health information, fingerprints, license plate numbers, or Internet Protocol ("IP") addresses. *101: Data Protection*, *supra*. A person can be "identified"—even if a data collector does not know his or her name—by singling them out, tracking their activity, and creating a detailed profile. *Id.*

[14] *See* U.S. DEP'T OF COMMERCE, U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE II, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg [https://perma.cc/93XY-ZV8Q] [hereinafter PRIVACY SHIELD] (governing data transfers from the European Union to the United States); Gaff et al., *supra* note 12, at 9–10 (explaining that U.S. federal data privacy law specifically regulates the financial and healthcare sectors, but various other laws require the provision of data security for personal information in all areas of business); *see, e.g.*, 15 U.S.C. §§ 6801–6802 (2012) (imposing a duty on financial institutions to safeguard their clients' private personal information and governing the disclosure of such information); 210 MASS CODE REGS. 17.03 (2018) (requiring every data processor in possession of personal information regarding a Massachusetts resident to facilitate a complete data privacy security system).

[15] *See infra* notes 28–52 and accompanying text (explaining the EU-U.S. Safe Harbor Privacy Principles ("Safe Harbor") and the subsequent EU-U.S. Privacy Shield ("Privacy Shield")).

[16] Corley, *supra* note 1, at 726.

[17] Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards*, 25 YALE J. INT'L L. 1, 39 (2000). The European Union is the United States' largest trading partner and the locus of most international investment and overseas production by U.S. businesses. *Id*. Additionally, EU member states significantly increased their bargaining power relative to the United States when they shifted their negotiating power for international data privacy issues to the European Commission. *Id*. at 41. Because the EU member states decided to act together, the impact of a EU data transfer ban became much more serious and led the United States to act more cautiously than it might have against individual member states. *Id*.

[18] *Id*. at 41. U.S. companies rely on information exchanges with many outside entities such as suppliers, clients, advisers, and advertisers, as well as their internal associates, branches, and subsidiaries. *Id*.

[19] *Id*. at 41, 44.

their dispute regarding the adequacy of data privacy protections.[20] Consequently, from 1998 to 2000, officials engaged in negotiations to construct a legal framework by which U.S. entities could satisfy the EU Data Protection Directive's ("EU Directive") standards.[21]

This Part explores the evolution of EU data privacy law.[22] Section A provides a summary of the EU Directive and the EU-U.S. Safe Harbor Privacy Principles ("Safe Harbor") framework.[23] Section B explains the impact of *Schrems v. Irish Data Protection Commissioner* on the data privacy law landscape.[24] Section C describes the EU-U.S. Privacy Shield ("Privacy Shield") framework.[25] Section D highlights some of the changes the General Data Protection Regulation ("GDPR") will bring.[26] Section E highlights examples of the recent increase in EU enforcement actions for data privacy violations.[27]

A. Safe Harbor: A Solution to the EU Directive

The EU legislature issued the EU Directive in 1995.[28] The EU Directive governs data movement into and out of the European Union.[29] It also forbids transfers of personal information to non-EU countries unless the country guarantees an "adequate level of protection."[30]

The European Union found that the United States did not provide "adequate" data privacy protection for EU citizens and prohibited personal data transfers to the United States.[31] In 2000, the United States and the European Union agreed to Safe Harbor, which the European Commission deemed com-

---

[20] *See id.* at 44–45 (explaining how economic interests persuaded the U.S. and EU governments to solve their data privacy disagreement).

[21] *See* Bennett, *supra* note 5, at 61 (indicating that the Safe Harbor agreement was brokered from 1998 to 2000); Corley, *supra* note 1, at 747 (explaining that, faced with the limitations of the EU Data Protection Directive ("EU Directive"), EU and U.S. representatives started to discuss a solution).

[22] *See infra* notes 28–84 and accompanying text.

[23] *See infra* notes 28–34 and accompanying text.

[24] *See infra* notes 35–41 and accompanying text.

[25] *See infra* notes 43–51 and accompanying text.

[26] *See infra* notes 51–65 and accompanying text.

[27] *See infra* notes 67–84 and accompanying text.

[28] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 50 [hereinafter EU Directive]. A directive is one of the four types of EU legislation and is a law adopted by the EU legislature, setting a certain policy goal, but allowing member states to devise their own means of achieving it. DIRECTORATE-GEN. FOR COMMC'N, EUROPEAN COMM'N, THE EUROPEAN UNION EXPLAINED: HOW THE EU WORKS 5 (2014).

[29] Kristina Daugirdas & Julian Davis Mortenson, *European Union and United States Conclude Agreement to Regulate Transatlantic Personal Data Transfers*, 110 AM. J. INT'L L. 360, 361 (2016).

[30] EU Directive, *supra* note 28, at 45.

[31] Bennett, *supra* note 5, at 61.

pliant with the EU Directive's requirements.[32] Safe Harbor embodied seven core principles for U.S. organizations to adhere to in their data privacy practices: notice, choice, onward transfer, access, security, data integrity, and enforcement.[33] Under Safe Harbor, businesses voluntarily chose to enact certain data protection safeguards and they self-certified compliance with the core principles.[34]

B. The Schrems Decision's Pivotal Impact on Data Privacy

In October 2015, the European Court of Justice ("ECJ") found Safe Harbor invalid in *Schrems* because it did not ensure adequate protection for EU personal data.[35] The ECJ interpreted "adequate level of protection" under the EU Directive as a degree of security for basic rights and liberties that is substantially similar to the protection guaranteed within the European Union.[36] In finding Safe Harbor inadequate, the ECJ largely concentrated on the absence of legal remedies available to EU citizens to vindicate their basic rights to privacy under Safe Harbor.[37] The court further observed the deficiency of enforcement methods and liability under Safe Harbor, largely because U.S. entities self-certified their compliance.[38]

Following *Schrems*, the EU Data Protection Authorities ("DPAs") declared that organizations could no longer rely on Safe Harbor to conduct EU-U.S. data transfers.[39] Consequently, all U.S. organizations that engaged

---

[32] Commission Decision 2000/520/EC, 2000 O.J. (L 215) 8; U.S. Dep't of Commerce, *Safe Harbor Privacy Principles*, EXPORT.GOV (July 21, 2000), https://build.export.gov/main/safeharbor/eu/eg_main_018475 [https://perma.cc/DUC8-MK8E]; *see* Bennett, *supra* note 5, at 61 (stating that Safe Harbor was negotiated from 1998 to 2000).

[33] U.S. Dep't of Commerce, *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://2016.export.gov/safeharbor/eu/eg_main_018476.asp [https://perma.cc/LX65-SHQ4].

[34] Bennett, *supra* note 5, at 61; *see Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, at 2, COM (2013) 847 final (Nov. 27, 2013) (explaining that Safe Harbor is structured so that organizations voluntarily self-certify their compliance with its principles, but those who volunteer to do so are bound by the agreement).

[35] Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650, 25; Lisa Mays, *The Trickle Down Effect of Privacy Shield Uncertainty: Fluctuating Lines for Anti-Bribery Compliance*, 19 J. INT'L L. 1, 8 (2016).

[36] *Schrems*, 2015 E.C.R at 21. The European Court of Justice ("ECJ") noted that a third-party country cannot be required to ensure an "identical" level of protection to the European Union, but merely an "adequate" level of protection. *Id*.

[37] Bennett, *supra* note 5, at 61; *see Schrems*, 2015 E.C.R. at 24 (noting that the European Commission acknowledged that under Safe Harbor, people did not have access to any redress methods that would allow them to obtain, change, or delete their personal information).

[38] *Schrems*, 2015 E.C.R. at 22–23; Bennett, *supra* note 5, at 61.

[39] Bennett, *supra* note 5, at 61; ARTICLE 29 WORKING PARTY, STATEMENT OF THE ARTICLE 29 WORKING PARTY (Oct. 16, 2015), https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2015/10/20151016_wp29_statement_on_schrems_judgement-2.pdf [https://perma.cc/3NXZ-YHWZ]. The Article 29 Working Party on the Protection of Individuals with regard to the Pro-

in data transfers with the European Union could no longer self-certify under Safe Harbor.[40] In order to continue transferring data across the Atlantic, these organizations had to take additional steps to separately validate that they protected personal information adequately under the EU Directive.[41]

C. The EU-U.S. Privacy Shield: The New and Improved Safe Harbor

The European Commission officially approved Privacy Shield as Safe Harbor's replacement on July 16, 2016.[42] Privacy Shield preserved many of Safe Harbor's principles.[43] However, Privacy Shield requires more transparency than Safe Harbor and institutes supervision methods to guarantee ongoing compliance.[44]

---

cessing of Personal Data is a separate advisory group made up of delegates from the Data Protection Authorities ("DPAs") of each EU country, as well as delegates from other EU government departments, formed pursuant to Article 29 of the EU Directive. ARTICLE 29 WORKING PARTY, *supra*.

[40] Bennett, *supra* note 5, at 61. Affected organizations included those with offices in both the European Union and the United States, EU organizations that contracted work out to the United States, and all organizations that sent data from the European Union to the United States. *Id*.

[41] *Id*. Alternate mechanisms for permissible transatlantic data flow included: (1) entering into contracts that incorporated the Model Contract Clauses provided by the European Commission; (2) establishing approved binding corporate rules for transfers within a multinational organization; or (3) obtaining the "free and informed" consent of the individual whose data was to be transferred. Mays, *supra* note 35, at 8.

[42] *See* Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 1, 35 (finding that Privacy Shield provided the requisite adequate protection for EU data); European Commission Press Release IP/16/433, Restoring Trust in Transatlantic Data Flows Through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield (Feb. 29, 2016) [hereinafter Privacy Shield Press Release] (unveiling Privacy Shield). The European Commission emphasized four critical elements of Privacy Shield that were meant to ensure its conformity with the ECJ's decision in *Schrems*: (1) powerful responsibilities for companies and vigorous enforcement; (2) explicit protections and unequivocal commitments regarding access by the U.S. government; (3) efficacious preservation of the rights of EU citizens with multiple avenues for redress; and (4) a yearly multilateral assessment process. Privacy Shield Press Release, *supra*; Corley, *supra* note 1, at 751.

[43] Daugirdas & Mortenson, *supra* note 29, at 365; *see* Corley, *supra* note 1, at 751 (explaining that the first of the European Commission's highly regarded elements, concerning duties and enforcement, encompass many of Privacy Shield's remaining links to Safe Harbor). Like Safe Harbor, Privacy Shield includes seven central principles that participating organizations must adhere to when collecting and using personal data from the European Union. Corley, *supra* note 1, at 751. Also like Safe Harbor, Privacy Shield makes participation voluntary, allows participating organizations to self-certify their adherence to Privacy Shield's principles, and subjects participating organizations to the Federal Trade Commission's ("FTC") enforcement power. Corley, *supra* note 1, at 752; Daugirdas & Mortenson, *supra* note 29, at 365.

[44] Corley, *supra* note 1, at 752; Daugirdas & Mortenson, *supra* note 29, at 365. Organizations may be subject to sanctions or exclusion for non-compliance. Daugirdas & Mortenson, *supra* note 29, at 365.

For instance, Privacy Shield requires organizations to notify individuals about the collection and use of their data.[45] It also establishes more stringent conditions and heightened liability for transferring data to third parties.[46] Privacy Shield requires that participating companies furnish the Department of Commerce, upon request, with information about or a copy of the relevant contract terms governing data transfers with a third party.[47] Moreover, organizations are liable if a third party to which it transferred data does not comply with Privacy Shield, unless the organization can show that it did not exercise control over the offending acts.[48] Additionally, Privacy Shield subjects organizations to the purview of U.S. governmental agencies, giving them powers of inquiry and enforcement in order to facilitate conformity with its requirements.[49]

A new oversight measure puts explicit limitations on U.S. government access to EU personal data.[50] Privacy Shield equips EU citizens with multiple options for recourse that were not previously available under Safe Harbor.[51] Overall, Privacy Shield represents a significant shift from Safe Harbor in favor of stronger data protection measures.[52]

---

[45] PRIVACY SHIELD, *supra* note 14, at II(1); Mays, *supra* note 35, at 8.

[46] PRIVACY SHIELD, *supra* note 14, at II(7)(d); Corley, *supra* note 1, at 752; Daugirdas & Mortenson, *supra* note 29, at 365.

[47] Corley, *supra* note 1, at 752 n.216.

[48] *Id. Compare* PRIVACY SHIELD, *supra* note 14, at II(7)(d) (extending liability for transfers to third parties), *with* U.S. Dep't of Commerce, *supra* note 32 (failing to impose liability on participating organizations when third parties act contrary to the Safe Harbor, unless the organization was aware or should have been aware of the act and did not take appropriate action to stop it).

[49] PRIVACY SHIELD, *supra* note 14, at I(2); Corley, *supra* note 1, at 752.

[50] *See* Privacy Shield Press Release, *supra* note 42 (explaining the second European Commission element regarding U.S. government access). Privacy Shield is the European Union's first written guarantee from the U.S. government and Office of the Director of National Intelligence of distinct restraints, protections, and supervision procedures on all national security related government use of personal information. *Id.*; Corley, *supra* note 1, at 753; Daugirdas & Mortenson, *supra* note 29, at 365.

[51] Privacy Shield Press Release, *supra* note 42; Corley, *supra* note 1, at 753. Under Privacy Shield, individual EU citizens may bring complaints directly to participating organizations that they believe are violating the agreement; participating organizations must resolve the complaints within forty-five days. Privacy Shield Press Release, *supra* note 42; Corley, *supra* note 1, at 753; Daugirdas & Mortenson, *supra* note 29, at 365. Organizations must also make an alternative dispute resolution process available at no cost. Privacy Shield Press Release, *supra* note 42. EU citizens may also inform their national DPAs, which will work with the FTC to guarantee the resolution of their complaints. *Id.*; Corley, *supra* note 1, at 753. If a complaint is not resolved by any of the aforementioned redress options, EU citizens may obtain an "enforceable remedy" through binding arbitration. Privacy Shield Press Release, *supra* note 42; Corley, *supra* note 1, at 753.

[52] *See* Daugirdas & Mortenson, *supra* note 29, at 365 (noting the changes from Safe Harbor to Privacy Shield, including "strong obligations," "robust enforcement," "clear safeguards and transparency obligations," and "effective protection").

D. GDPR: The Impending Shake-Up

On April 27, 2016, the European Union adopted the GDPR to replace the 1995 EU Directive.[53] The GDPR takes effect on May 25, 2018.[54] Although the GDPR encompasses some core aspects of the EU Directive, it contains many significant differences.[55]

The GDPR is broader in scope than the EU Directive, as it applies to all data pertaining to a EU citizen, regardless of whether the data is actually processed within the European Union.[56] This extraterritorial application of EU data privacy law will have a huge impact on international data flow and will make the GDPR a de facto global standard.[57] The regulation not only maintains a requirement of adequate protection for data transfers to third-party countries, like the EU Directive, but also provides rules for such transfers.[58]

The GDPR broadens the range of data types and categories of personal data governed in order to keep up with developments in digital technology and to strengthen individuals' control over their information.[59] This means that companies will have to obtain consent from data subjects for a broader

---

[53] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[54] *Id.* at 86.

[55] W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. L. 221, 222 (2016); *see* Marianna Meriani, *Digital Platforms and the Spectrum of Data Protection in Competition Law Analyses*, 38 EUR. COMPETITION L. REV. 89, 93 (2017) (asserting that the GDPR has significantly altered EU data regulation, with the goal of safeguarding data despite worldwide technological and societal changes).

[56] GDPR, *supra* note 53, at 32; EU Directive, *supra* note 28, at 39; Allison Callahan-Slaughter, *Lipstick on a Pig: The Future of Transnational Data Flow Between the EU and the United States*, 25 TUL. J. INT'L & COMP. L. 239, 252 (2016). The EU Directive subjects data controllers to regulation only if they process an EU citizen's personal data within the European Union; under the GDPR, the consideration is only whether EU personal data is processed. GDPR, *supra* note 53, at 32. Non-EU companies must comply with the same rules as EU companies when they make goods or services available to, or observe, people in the European Union. *Id.*

[57] *See* Callahan-Slaughter, *supra* note 56, at 252 (explaining that the European Union's global market power, in conjunction with the GDPR's application to all data controllers which process EU personal data, means that the GDPR will in effect apply across the globe).

[58] *See* GDPR, *supra* note 53, at 61 (requiring an adequate level of data protection for third-party country transfers); EU Directive, *supra* note 28, at 45 (allowing data transfers to third-party countries only if that country guarantees an adequate level of protection). Transfers of data to third-party countries can occur if the European Commission has verified that the country guarantees adequate protection, approved binding corporate rules are in place, the data controller ensures suitable protections, or the subject explicitly consents. GDPR, *supra* note 53, at 61–64; Callahan-Slaughter, *supra* note 56, at 252.

[59] Callahan-Slaughter, *supra* note 56, at 251; Meriani, *supra* note 55, at 94; *see, e.g.*, GDPR, *supra* note 53, at 6 (asserting that individuals might be identifiable by online identifiers made available by their devices, like IP addresses and cookie identifiers, information which may be compiled to profile someone and determine their identity).

array of collection mechanisms and information types.[60] Furthermore, "consent" under the GDPR requires data processors to acquire express consent from data subjects for their precise intentions, eliminating implied consent.[61] The GDPR provides individuals with a new distinct right called the "right to be forgotten," effected through a powerful right to erasure.[62] Data controllers must also immediately inform their DPA of a personal data breach unless they can show that the breach is not likely to adversely affect the data subjects' privacy rights.[63]

Unlike the EU Directive, the GDPR explicitly governs orders from foreign judiciaries to produce evidence regarding the personal information of EU citizens.[64] Importantly, the GDPR provides for extremely high sanctions—up to four percent of the company's revenue—for data protection violations.[65] The strengthening of data protection encompassed in the GDPR will have a significant and wide-reaching impact on data privacy practices worldwide.[66]

E. The European Union Means Business: EU Regulators Are Doling Out Serious Punishments for Data Privacy Violations

The heightened focus and tougher stance on data privacy in the European Union in recent years has hinted that EU regulators might start cracking down on prominent companies, especially ones that process large amounts of EU citizens' data.[67] Predictions of such sort have proven to be true.[68]

---

[60] *See* Meriani, *supra* note 55, at 94 (including information collected by online identifiers, device identifiers, cookie IDs, and IP addresses). Online data processors are resistant to the idea of systematically gaining consent for every instance of data collection. *Id.* It is therefore believed that this expansion of the legal requirements for consent may not be very consequential in practice; companies typically meet the consent requirement by notifying their users of their data practices in "Terms and Conditions" agreements that few users look at or comprehend. *Id*.

[61] GDPR, *supra* note 53, at 34; Callahan-Slaughter, *supra* note 56, at 251.

[62] GDPR, *supra* note 53, at 43; Callahan-Slaughter, *supra* note 56, at 251.

[63] GDPR, *supra* note 53, at 16–17. According to the GDPR, a data breach necessitates immediate notification because it can cause harm to the data subjects. *Id*. Pseudonymisation is a mechanism for data protection introduced in the GDPR, included as one of the "appropriate safeguards" for processing data, whereby identifiable information is replaced by a random code so that the individual can no longer be identified by that information. *Id.* at 29, 33; Meriani, *supra* note 55, at 94.

[64] *See infra* notes 137–140 and accompanying text (explaining that Article 48 stipulates that such orders may only be complied with according to international agreements such as judicial assistance treaties).

[65] Voss, *supra* note 55, at 229; *see* GPDR, *supra* note 53, at 83 (stipulating that specified infringements will result in administrative fines up to €20,000,000, or for companies, up to 4% of their total worldwide annual revenue for the previous financial year, whichever is higher).

[66] *See* Callahan-Slaughter, *supra* note 56, at 251–52 (discussing the GDPR's substantial bolstering of data protection as well as its global effects).

[67] *See supra* notes 28–66 and accompanying text (explaining recent changes in EU data privacy law); *see also* Bennett, *supra* note 5, at 63 (quoting Neil Stelzer, the general counsel for Identity Finder, who predicted in early 2016 that EU regulators would "go after big names that will

For example, the Spanish Agency for Data Protection fined Google €900,000 in December 2013.[69] Not long after, privacy regulators across Europe combined efforts to probe Facebook's data practices.[70] The coordinated effort by the Netherlands, Germany, Belgium, France, Italy, and Spain is noteworthy; Facebook had always been subject to the regulatory authority of a single country, Ireland, where its European headquarters are located.[71] In anticipation of the forthcoming and pivotal GDPR, however, the DPAs of the EU member states have gained the courage to challenge high-powered U.S. companies.[72] This hyperactive focus on Facebook's data practices is just one example of the increasing EU vitriol towards U.S. technology companies.[73]

The French DPA, the National Commission on Informatics and Liberty ("CNIL"), fined Google, and has publically and formally threatened sanctions against Facebook and Microsoft for data privacy law violations.[74] On March 10, 2016, the CNIL announced a €100,000 fine against Google for disobeying the CNIL's order regarding the right to delisting.[75] On February 8, 2016, the CNIL published an order demanding that Facebook change the

---

make the papers and try to get big fines issued against them"); Sam Schechner, *Facebook Privacy Controls Face Scrutiny in Europe: Tension Between EU Authorities and U.S. Tech Giants Is Likely to Escalate*, WALL ST. J. (Apr. 2, 2015), https://www.wsj.com/articles/facebook-confronts-european-probes-1427975994 [https://perma.cc/KZ66-YBXW] [hereinafter Schechner, *Facebook Privacy*] (quoting Christian Wiese Svanberg, a privacy attorney in Copenhagen, who stated that inquiries by EU DPAs are indicative of what the future holds for Facebook, and that in the near future, similar inquiries will come with the threat of massive sanctions).

[68] *See infra* notes 69–84 and accompanying text (explaining enforcement actions by EU DPAs against well-known multinational companies like Google, Facebook, and Microsoft).

[69] David Roman, *Google Fined in European Privacy Probe: Five Other Countries May Follow Spanish Example*, WALL ST. J. (Dec. 19, 2013), https://www.wsj.com/news/articles/SB10001424052702304367204579268143320003938 [https://perma.cc/2SBY-V2LK]. Spain was the first of the six countries that started investigating Google's privacy compliance in 2012 to actually fine the company. *Id.*

[70] Schechner, *Facebook Privacy*, *supra* note 67.

[71] *Id.*

[72] *Id.* Mathias Moulin, the leader of the National Commission on Informatics and Liberty's ("CNIL") effort to look into Facebook, is quoted as saying, "We are showing a united front before a global actor. It's time for us to focus on Facebook." *Id.*

[73] *Id.* Google faces an EU antitrust inquiry; both Amazon and Apple's corporate tax practices are being investigated by the European Union; France and Germany want heightened regulation over large U.S. technology companies, "escalat[ing] its war against U.S. technology superpowers"; the European Parliament voted strongly in favor of a resolution to possibly break up Google. *Id.*; Sam Schechner, *Europe Targets U.S. Web Firms: French, German Officials Call for Greater Power to Regulate Internet Companies*, WALL ST. J. (Nov. 27, 2014), https://www.wsj.com/articles/french-german-officials-call-for-fresh-look-at-internet-giants-1417110508 [https://perma.cc/4NN4-J7JM].

[74] *See infra* notes 75–78 and accompanying text (describing the actions).

[75] Julia Floretti, *France Fines Google Over 'Right to Be Forgotten,'* REUTERS (Mar. 24, 2016), http://www.reuters.com/article/us-google-france-privacy-idUSKCN0WQ1WX [https://perma.cc/BR8N-VS4D].

ways it collects and uses information about Internet users within three months or face sanctions and fines of up to €150,000.[76] On July 20, 2016, the CNIL threatened Microsoft with sanctions and fines of up to €150,000 if they did not stop tracking browsing patterns of its users and gathering unnecessary user information.[77] The CNIL further ordered Microsoft to improve its data security practices within three months and to cease illegally transferring personal information to the United States based on the invalidated Safe Harbor.[78]

In September 2016, the Hamburg Commissioner for Data Protection and Freedom of Information ("HmbBfDI") ordered WhatsApp, a messaging application and Facebook subsidiary, to stop transferring the data of its German users to Facebook due to privacy issues.[79] In January 2017, the Federation of German Consumer Organizations sued the messaging service, alleging that the company "partly illegally" gathered data and then transferred it to Facebook, which could result in a multi-million euro penalty for Facebook.[80] In addition, the HmbBfDI announced in November 2016 that ten German Data Protection Supervision authorities would complete a coordinated audit of companies transferring the personal data of EU citizens to non-EU countries, with the objective of raising awareness about such data privacy transfers.[81]

In the wake of the WhatsApp German lawsuit, Ireland's Data Protection Commissioner, Helen Dixon, also stepped up to the plate.[82] She created

---

[76] Sam Schechner, *France's Privacy Regulator Threatens to Fine Facebook*, WALL ST. J.: MARKETWATCH (Feb. 8, 2016), http://www.marketwatch.com/story/frances-privacy-regulator-threatens-to-fine-facebook-2016-02-08 [https://perma.cc/F9S6-T83B].

[77] CNIL, *Windows 10: CNIL Publicly Serves Formal Notice to Microsoft Corporation to Comply with the French Data Protection Act Within Three Months* (July 20, 2016), https://www.cnil.fr/en/windows-10-cnil-publicly-serves-formal-notice-microsoft-corporation-comply-french-data-protection [https://perma.cc/3KFZ-94Q7]; *France Threatens Microsoft with Sanctions for Tracking & Collecting 'Excessive' User Info*, RT (July 21, 2016), https://www.rt.com/news/352417-france-microsoft-user-data/ [https://perma.cc/SDT5-G5BF].

[78] CNIL, *supra* note 77. The CNIL investigated Microsoft in April and June of 2016 and found several deficiencies in the company's privacy practices, including unnecessary information gathering, insecure login methods, insufficient consent obtained from users to track their behavior, no notice given of advertising cookies, and the continued conveyance of data to the United States based on the invalidated Safe Harbor. *Id.*

[79] *Germany Bans WhatsApp Data Transfer to Facebook*, DW (Sept. 27, 2016), http://www.dw.com/en/germany-bans-whatsapp-data-transfer-to-facebook/a-35903021 [https://perma.cc/74UQ-RKVR].

[80] *German Consumer Group Sues WhatsApp*, DW (Jan. 30, 2017), http://www.dw.com/en/german-consumer-group-sues-whatsapp/a-37335926 [https://perma.cc/5UUJ-7L84].

[81] Hamburg Comm'r for Data Prot. & Freedom of Info. ("HmbBfDI"), *Data Protection Authorities of the Länder Are Checking Cross-Border Data Transfers*, HMBBFDI, https://www.datenschutz-hamburg.de/news/detail/article/datenschutzaufsichtsbehoerden-der-laender-pruefen-grenzueberschreitende-datenuebermittlungen.html?tx_ttnews[backPid]=170&cHash=756c8c2e6bddd3d467899f35fc3c110a [https://perma.cc/XRV5-RAL5].

[82] Schechner, *Ireland's Privacy Cop*, *supra* note 2.

a ten-person task force to investigate multinational technology companies and put Facebook and WhatsApp through the wringer at the agency's offices.[83] With Ireland as the home of several technology titans' European headquarters, including Facebook, Apple, Google, and Airbnb, Dixon is positioned to shape data privacy's global landscape over the coming years.[84]

II. THE DISCOVERY DILEMMA: WHEN U.S. DISCOVERY REQUESTS CONTRAVENE EU DATA PRIVACY PROTECTION

Discovery is the official process dictated by the Federal Rules of Civil Procedure through which litigants request and provide information for the purpose of deciphering the facts of a case and what may come to light at trial.[85] The discovery process in the United States can be extremely time-consuming and in-depth, especially when compared to the rest of the world.[86] Notably, even when requested discovery materials are located outside of the United States or revealing them is limited or illegal under foreign law, U.S. courts have the power to compel parties to provide them.[87] If a litigant does not comply with a discovery order, the court can impose sanctions.[88]

This Part explores the conflict between EU data privacy law and the discovery process in U.S. litigation.[89] Section A explains the intersection of U.S. discovery procedures and foreign law, including how U.S. courts approach the issue.[90] Section B explores the specific problem posed when a party in possession of personal information of EU citizens, protected by EU data privacy law,

---

[83] *Id*.

[84] *Id*. Dixon said, "The standards that we set in Europe will influence how data privacy is done around the world." *Id*. According to Ireland's Data Protection Commissioner, Ireland will be steadfast and resolute in administering the forthcoming GDPR. *Id*.

[85] SEDONA CONFERENCE, *supra* note 4, at 1; *see Discovery*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining discovery as the mandatory divulgence of information associated with a legal action); *see also* FED. R. CIV. P. 26 (outlining the federal discovery rules).

[86] Sedona Conference, *The Sedona Conference Practical In-House Approaches for Cross-Border Discovery & Data Protection*, 17 SEDONA CONF. J. 397, 405–06 (2016) [hereinafter *Sedona Conference Discovery and Data Protection*]; Steven C. Bennett, *EU Privacy vs. U.S. Discovery: Practical Responses to the Conflict*, 58 PRAC. L. 31, 32 (2012); *see* FED. R. CIV. P. 34(a) (describing the types of discoverable information). The common law approach is that justice will be best achieved when adversarial litigants conduct discovery themselves; the civil law approach presumes that the judicial branch is the most prudent conductor of discovery procedures and will best protect individuals' fundamental right to privacy. *Sedona Conference Discovery and Data Protection*, *supra*, at 405. Pre-trial discovery is very limited in most civil law countries, which do not compel the production of any more information than is essential to argue a case. *Id.* at 406.

[87] SEDONA CONFERENCE, *supra* note 4, at 2.

[88] *See* FED. R. CIV. P. 37(b)(2) (providing that the court can impose sanctions for noncompliance with a discovery order, including "payment of expenses").

[89] *See infra* notes 93–142 and accompanying text.

[90] *See infra* notes 93–126 and accompanying text.

is asked to produce that information during litigation in a U.S court.[91] Section C discusses the potential effects of the GDPR on discovery deliberations in the United States.[92]

A. U.S. Discovery Rules vs. Foreign Law: How U.S. Courts Determine the Victor

When a discovery order conflicts with foreign law, U.S. courts must carefully consider how best to proceed.[93] A primary source of guidance in these instances is the Hague Evidence Convention ("Hague Convention"), an international assistance agreement that governs the collection of evidence abroad.[94] The principle of international comity also informs courts' decisions in these instances.[95]

1. The Hague Convention: An International Effort to Alleviate Cross-Border Discovery Woes

The Hague Convention is an international judicial assistance agreement between fifty-nine countries, including the United States and most EU member states.[96] The Hague Convention aims to increase harmonization in international litigation by reconciling differing or conflicting practices.[97] Accordingly, it provides specific mechanisms for courts in one nation to request evidence located in another.[98]

---

[91] *See infra* notes 67–136 and accompanying text.

[92] *See infra* notes 137–142 and accompanying text.

[93] SEDONA CONFERENCE, *supra* note 4, at 2–3.

[94] Société Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522, 522 (1987).

[95] *Id.* at 543–44.

[96] David P. Stewart, *Private International Law: A Dynamic and Developing Field*, 30 U. PA. J. INT'L L. 1121, 1122 (2009).

[97] *Id.*

[98] *Aerospatiale*, 482 U.S. at 522; Stewart, *supra* note 96. *See generally* Hague Conference on Private International Law, Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, 847 U.N.T.S. 231 [hereinafter Hague Convention] (providing transnational discovery procedures). Twenty-five of the twenty-eight EU member states are parties to the Hague Convention. Hague Conference on Private Int'l Law, *Status Table: 20: Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters*, HCCH, https://www.hcch.net/en/instruments/conventions/status-table/?cid=82 [https://perma.cc/7QND-B72S]. The Convention is applicable only between states that are parties to it and contains two methods for taking evidence: (1) Letters of Request, and (2) diplomatic or consular agents and commissioners. HAGUE CONFERENCE ON PRIVATE INT'L LAW, OUTLINE: EVIDENCE CONVENTION 1 (2010), https://assets.hcch.net/docs/ec1fc148-c2b1-49dc-ba2f-65f45cb2b2d3.pdf [https://perma.cc/9765-9LNL] [hereinafter HAGUE CONVENTION OUTLINE]. Judiciaries may also seek evidence located abroad by means of letters rogatory, a comparable mechanism to Letters of Request used when there is no treaty in place, but one that involves diplomatic channels. *See* Lou-

Litigants commonly seek to have information obtained through the Hague Convention's Letter of Request function when a discovery request involves information located abroad and if disclosure would violate foreign data privacy law.[99] That mechanism is preferable to the litigants producing it themselves and possibly violating privacy laws and facing sanctions.[100] Although the Hague Convention provides that Letters of Request must be promptly executed by contracting states, there are several exceptions by which a state may refuse to comply.[101] The U.S. Supreme Court has held that, while the Hague Convention provides options for acquiring evidence located abroad, its procedures are neither mandatory nor the exclusive means of doing so.[102]

2. International Comity: Recognition of Foreign Sovereignty

Even though U.S. courts are not required to comply with foreign discovery law or the Hague Convention procedures, their use can help to account for foreign interests.[103] The judicial principle of respect for the sovereign power of other countries is called international comity.[104] This concept, which seeks a middle ground between mere courtesy and complete deference, has been acknowledged in U.S. jurisprudence since the 1800s.[105] Comity involves the balancing of international and domestic interests to gauge if, and to what extent, one nation will allow the law of another nation

---

is B. Kimmelman & Steven L. Smith, *The Hague Evidence Convention*, *in* BUSINESS AND COMMERCIAL LITIGATION IN FEDERAL COURTS § 21:89 (4th ed. 2016) (defining letters rogatory).

[99] *See Aerospatiale*, 482 U.S. at 522. The Letter of Request method consists of the judicial authority of one state requesting that an appropriate authority of another state acquire evidence for use in litigation in the requesting state. HAGUE CONVENTION OUTLINE, *supra* note 98, at 1. The Hague Convention requires all contracting states to establish a "Central Authority" to process Letters of Request from judicial authorities of other states and disseminate them to the proper national authorities. Hague Convention, *supra* note 98, at art. 2.

[100] *See Aerospatiale*, 482 U.S. at 522.

[101] Hague Convention, *supra* note 98, at arts. 5, 9; Kimmelman & Smith, *supra* note 98. Article 9 instructs that a Letter of Request must be performed promptly. Hague Convention, *supra* note 98, at art. 9. Article 5 provides that a Central Authority can oppose a Letter of Request that it regards as outside the Hague Convention's scope or noncompliant with its requirements, but must immediately inform the requesting state's Central Authority. *Id.* at art. 5. Article 12 limits refusal of Letters of Request to situations where execution outside the scope of that court's authority and where execution would bias the "sovereignty or security" of the nation. *Id.* at art. 12; Kimmelman & Smith, *supra* note 98.

[102] *See infra* notes 114–122 and accompanying text.

[103] Diego Zambrano, *A Comity of Errors: The Rise, Fall, and Return of International Comity in Transnational Discovery*, 34 BERKLEY J. INT'L L. 157, 173–75 (2016).

[104] *Id.* at 161; *see Comity*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining comity as a custom between governmental bodies, such as sovereign nations or judiciaries, in which they acknowledge each other's laws and authority).

[105] Zambrano, *supra* note 103.

to apply within its jurisdiction.[106] In other words, even if a court has jurisdiction over a case and its parties, the doctrine of international comity obligates judges to contemplate how the outcome will affect the concerned foreign nations.[107]

Three decades ago, the Supreme Court provided a multi-factor balancing test for determining when U.S. courts should exercise their authority to compel production of evidence constrained by foreign law.[108] The balancing test considers five factors: (1) the significance of the requested discovery in regard to the litigation; (2) the precision of the request; (3) whether the requested information was generated in the United States; (4) the availability of an alternate method for acquiring the discovery materials; and (5) the damage to the United States' or foreign nation's concerns if the discovery is not executed.[109]

The controlling U.S. Supreme Court case on the international comity analysis is *Société Nationale Industrielle Aerospatiale v. United States District Court for the Southern District of Iowa*.[110] There, the plaintiffs, survivors of a plane crash involving the defendants' plane, sought discovery information physically located in France.[111] The defendants, French aircraft companies, filed a motion for a protective order, claiming that the Hague Convention was the appropriate means for obtaining it.[112] The defendants further asserted that a French penal statute prevented them from complying with the discovery request and that complying could subject them to criminal liability.[113]

---

[106] Hilton v. Guyot, 159 U.S. 113, 164 (1895); Zambrano, *supra* note 103.

[107] Zambrano, *supra* note 103, at 161–62.

[108] *See Aerospatiale*, 482 U.S. at 544 n.28 (providing the balancing test); SEDONA CONFERENCE, *supra* note 4, at 2–3 (noting that the *Aerospatiale* balancing test is used to decide whether to order discovery from parties in violation of foreign law).

[109] *See Aerospatiale*, 482 U.S. at 544 n.28 (citing RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 442 (AM. LAW INST. 1987)).

[110] *Id.* at 533. In *Aerospatiale*, two French defendants were sued in U.S. federal court for personal injuries caused by an aircraft accident. *Id*. at 522. The defendants were French government-owned aircraft corporations. *Id*. at 524–25. When the plaintiffs sued in the U.S. District Court for the Southern District of Iowa, the defendants did not dispute the district court's jurisdiction and answered the complaints. *Id*. at 525.

[111] *Id*.at 525.

[112] *Id*. at 524–25. The defendants had willingly participated in initial discovery, which involved evidence located in the United States, but the second round of discovery requested evidence located in France. *Id*. at 525 n.4.

[113] *Id*. at 526 n.6. French Penal Code Law No. 80-538, the French blocking statute, stipulates in Article 1A that:

> Subject to treaties or international agreements and applicable laws and regulations, it is prohibited for any party to request, seek or disclose, in writing, orally or otherwise, economic, commercial, industrial, financial or technical documents or information leading to the constitution of evidence with a view to foreign judicial or administrative proceedings or in connection therewith.

The defendants argued that Hague Convention procedures were the sole means for procuring evidence located within a signatory country.[114] They argued, in the alternative, that the Court should establish a rule of first resort to Hague Convention mechanisms, prior to the Federal Rules of Civil Procedure.[115] The Court rejected both arguments.[116]

The Court insisted that the international comity analysis demands a detailed evaluation of the interests of both the nation requesting discovery and the foreign nation.[117] To weigh those competing interests, the Court adopted the approach in the *Restatement of Foreign Relations Law of the United States*.[118] Section 442 indicates the five factors that are pertinent to international comity analysis.[119] In addition to these factors, the Court prescribed two other considerations.[120] First, the Court specified the need for the "exercise [of] special vigilance" by U.S courts during pretrial proceedings, so as to shield foreign parties from unwarranted, useless, or excessively onerous discovery.[121] Second, U.S. courts must be mindful of unique difficulties facing foreign parties, as well as the sovereign state's demonstrated interests.[122]

Id. Article 3 provides for a punishment of two to six months in jail, a fine of 10,000 to 120,000 francs, or both, for violating Article 1A. *In re* Societe Nationale Industrielle Aerospatiale, 782 F.2d 120, 126 (8th Cir. 1986).

[114] *Aerospatiale*, 482 U.S. at 529. The French government agreed with the defendants in an amicus brief submitted to the Court. *Id.* at 529 n.11; Brief for Republic of France as Amicus Curiae at 4, *Aerospatiale*,482 U.S. 522 (No. 85-1695).

[115] *Aerospatiale*, 482 U.S. at 541–42.

[116] *Id*. at 541–43. The Court rejected the defendants' first argument, deciding instead that Hague Convention procedures are optional and at the court's disposal when it will make conducting foreign discovery easier. *Id.* at 541. The Court also rejected the defendants' second argument, reasoning that it would be incompatible with U.S. courts' paramount interest in "just, speedy, and inexpensive determination" of legal proceedings. *Id*. at 542–43. The Court noted that Letters of Request are more time consuming and expensive and less effective than the evidentiary rules set forth in the Federal Rules of Civil Procedure. *Id*. at 542. The Court dismissed the French blocking statute, noting well-established precedent that such laws did not prevent U.S. courts from compelling discovery that might defy them. *Id.* at 544 n.29. The Court also pointed to the American Law Institute's determination that blocking statutes should not be deferred to at the same level as substantive foreign laws. *Id*. The Court concluded that the French statute merely demonstrated foreign interests. *Id.* The Court also noted that by the nature of international comity, neither the Court's discovery order nor the French blocking statute could have absolute authority. *Id*.

[117] *Id*. at 543–44. The Court refused to adopt an outright rule that international comity automatically leads to use of the Hague Convention without a comprehensive inquiry into the specific circumstances of each individual case, the concerns of the foreign nations involved, and the probability of success of the Hague Convention's methods. *Id.* at 544.

[118] *Id*. at 544 n.28.

[119] *Id.*; *supra* note 109 and accompanying text (describing the five factors). The court asserted that any examination of international comity involved those factors, but noted that this approach was not necessarily fitting with the global consensus. *Aerospatiale*, 482 U.S. at 544 n.28.

[120] *Aerospatiale*, 482 U.S. at 546.

[121] *Id*. The Court noted that courts must monitor pretrial proceedings for abusive discovery especially carefully when evidence is sought abroad and must take claims by foreign parties of abusive discovery very seriously. *Id*.; *see Discovery Abuse*, BLACK'S LAW DICTIONARY (10th ed.

U.S. courts apply the factors laid out in *Aerospatiale* to determine how to conduct discovery regarding evidence located abroad, with particular emphasis on balancing foreign and U.S. interests.[123] The balancing test, however, permits courts to easily prioritize U.S. interests over foreign interests, because the U.S. Supreme Court did not provide an explicit procedure for weighing them.[124] The legacy of *Aerospatiale*, therefore, was a rise in expansive U.S. discovery, with international comity falling by the wayside.[125] In fact, in an overwhelming majority of cases where the balancing test was applied, the court decided that U.S. interests outweighed foreign interests and ordered discovery to be conducted under U.S. rules.[126]

2014) (defining discovery abuse as the inappropriate use of the discovery phase of litigation, especially by means of excessive information requests that are unimportant or impermissible, or engaging in discovery with an ulterior motive).

[122] *Aerospatiale*, 482 U.S. at 546. The Court acknowledged that it was not providing explicit rules for this deliberation of foreign problems and interests. *Id*. The Court cited the well-established consideration of international comity in adjudicating cases connected with foreign nations as either parties to the litigation or as sovereigns with an interest in the outcome. *Id*.

[123] David J. Kessler et al., *The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery from the United States*, 17 SEDONA CONF. J. 575, 600 (2016); *see* Laydon v. Mizuho Bank, Ltd., 183 F. Supp. 3d 409, 422 (S.D.N.Y. 2016) ("The fifth factor—the balancing of national interests—is the most important, as it directly addresses the relations between sovereign nations."); *see also supra* notes 110–122 and accompanying text (describing the *Aerospatiale* case).

[124] Zambrano, *supra* note 103, at 176; *see* Scarminach v. Goldwell GmbH, 531 N.Y.S.2d 188, 189 (Sup. Ct. 1988) (lamenting that the *Aerospatiale* Court "declined to set forth specific rules to guide such exercise of judicial discretion"). The *Aerospatiale* test seemed to consider foreign interests only superficially and was criticized on several fronts: (1) U.S. judges were not sufficiently knowledgeable about foreign law to properly evaluate foreign interests; (2) the test gave district courts expansive authority on discovery without adequate supervision by appellate courts; and (3) the test enabled courts to dismiss the concept of international comity and prioritize U.S. interests. Zambrano, *supra* note 103, at 176–77.

[125] Zambrano, *supra* note 103, at 176–77. Most courts deliberating over discovery acknowledged the Hague Convention *pro forma*, but ultimately declined to resort to it. *Id*.; *see infra* note 126 and accompanying text (providing examples).

[126] Kessler et al., *supra* note 123, at 600; *see, e.g.*, Wultz v. Bank of China Ltd., 910 F. Supp. 2d 548, 558–59 (S.D.N.Y. 2012) (determining that U.S. interests in "fully and fairly adjudicating matters before its courts" and its counterterrorism efforts outweighed China's interests in banking secrecy laws and sovereignty concerns); Strauss v. Credit Lyonnais, S.A., 242 F.R.D. 199, 222–23 (E.D.N.Y. 2007) (finding that U.S. and French interests in subverting the funding of terrorism exceeded France's interests in stopping the defendant from complying with the discovery requests, protecting the privacy of bank customers, and administering its national banking, money laundering, anti-terrorism, and criminal investigation laws). U.S. courts have ruled that insubstantial or questionable U.S. interests exceed foreign interests even when the foreign interests were significant. Zambrano, *supra* note 103, at 176. Uncommonly, courts have found that discovery should be conducted pursuant to the Hague Convention or not conducted at all. Kessler et al., *supra* note 123, at 602–03; Zambrano, *supra* note 103, at 177; *see, e.g.*, *In re* Payment Card Interchange Fee & Merch. Disc. Antitrust Litig., No. 05-MD-1720(JG)(JO), 2010 U.S. Dist. LEXIS 89275, at *29 (E.D.N.Y. Aug. 27, 2010); *In re* Perrier Bottled Water Litig., 138 F.R.D. 348, 356 (D. Conn. 1991); Volkswagen, A.G. v. Valdez, 909 S.W.2d 900, 903 (Tex. 2015).

B. The Intersection Between EU Data Privacy Obligations and U.S. Civil Procedure Discovery Rules

Foreign data privacy law oftentimes protects information requested during the discovery phase of litigation.[127] U.S. courts, however, have the power to compel the production of requested information, despite the fact that disclosing it may be constrained or forbidden by foreign law.[128] While courts do take the party's subjugation to foreign data privacy law into consideration, the possibility of foreign civil or criminal sanctions against the party is not determinative of a court's decision to require production.[129] Therefore, companies engaged in litigation in the United States may be forced to respond to discovery requests that place them directly in breach of EU data privacy law.[130]

International comity for discovery purposes often comes up in the context of the Hague Convention and blocking statutes.[131] Blocking statutes are data privacy laws enacted with the distinct purpose of shielding a country's nationals from broad discovery orders in foreign court proceedings.[132] Thus,

---

[127] SEDONA CONFERENCE, *supra* note 4, at *2.

[128] *Id*.

[129] *See Aerospatiale*, 482 U.S. at 544 n.29 (explaining that the French blocking statute's applicability to the defendants was relevant to the Court's evaluation of international comity merely insofar as it demonstrated the foreign interests in the security of certain information, a factor to be weighed).

[130] SEDONA CONFERENCE, *supra* note 4, at 3; *see, e.g.*, *In re* Air Cargo Shipping Serv. Antitrust Litig., 278 F.R.D. 51, 54–55 (E.D.N.Y. 2010) (noting that neither party disputed the fact that compliance by the French litigant with an order to produce the relevant documents would amount to violating the French blocking statute and give rise to the possibility of criminal sanctions). Although U.S. sanctions are normally not imposed when the litigant has made an "active, good-faith effort" to obey a discovery order, a litigant merely pointing to data privacy laws, such as blocking statutes, or to the existence of the Hague Convention, is not enough to forestall sanctions; litigants would have to demonstrate a sincere attempt to comply, such as seeking an exception from their home government authority or producing as much information as possible. Graco, Inc. v. Kremlin, Inc., 101 F.R.D. 503, 526 (N.D. Ill. 1984); Robert F. Koets, Annotation, *Sanctions for Failure to Make Discovery Under Federal Civil Procedure Rule 37 as Affected by Defaulting Party's Good Faith Efforts to Comply*, 134 A.L.R. Fed. 257 at § 2[a], 4 (1996).

[131] *See, e.g.*, *Air Cargo*, 278 F.R.D. at 52 (deciding whether to compel discovery through the Hague Convention when the discovery order would contravene France's blocking statute); *Strauss*, 242 F.R.D. at 206 (deciding whether to compel discovery through the Hague Convention when the discovery order would contravene France's blocking statute); *see also supra* notes 98–102 and accompanying text (explaining the Hague Convention).

[132] Bennett, *supra* note 86, at 31–32. Some countries have instituted blocking statutes to restrain the expansive or "intrusive" scope of U.S. discovery. *Sedona Conference Discovery and Data Protection*, *supra* note 86, at 407; John T. Yip, *Addressing the Costs and Comity Concerns of International E-Discovery,* 87 WASH. L. REV. 595, 615 (2012). Countries such as France, China, Malaysia, the Netherlands, and Switzerland have enacted blocking statutes. Yip, *supra*. Blocking statutes are commonly met with skepticism in American courts. *Sedona Conference Discovery and Data Protection*, *supra* note 86, at 407.

blocking statutes create a clash between foreign data privacy law and U.S. discovery rules.[133]

When faced with a conflict between discovery needs and EU data privacy law, U.S. courts have sometimes decided to not require foreign litigants to produce evidence that would violate privacy laws.[134] Overwhelmingly, however, U.S. courts have disregarded EU data privacy laws and ordered the relevant discovery.[135] Even after a French citizen was criminally prosecuted and fined €10,000 for complying with a U.S. court order to produce documents in violation of a French blocking statute in 2007, subsequent cases dismissed such sanctions as unrealistic.[136]

C. Stepping into the Unknown: The GDPR's Potential Effect on Discovery

In Article 48, the GDPR imposes specific conditions for transfers to third-party countries.[137] Article 48 stipulates that any non-EU court, tribunal, or administrative decision which orders a data controller to provide or divulge personal information can be acknowledged or enforced only if the order is based on an international agreement, such as a judicial assistance treaty.[138] The U.S. Supreme Court in *Aerospatiale* noted that for international comity purposes, substantive foreign laws should be given more def-

---

[133] *Sedona Conference Discovery and Data Protection*, *supra* note 86, at 407.

[134] *See* SEDONA CONFERENCE, *supra* note 4, at 3 (explaining that in some instances courts have decided against ordering discovery because of significant privacy interests); *see, e.g.*, *Volkswagen*, 909 S.W.2d at 903 (holding that a German company was not required to produce a phone book that contained personal information in violation of German data privacy law because Germany's interests in privacy rights would be subverted, alternative means of obtaining the requested information existed, and the phone book was not significant to the case).

[135] *See* Kessler et al., *supra* note 123, at 600 (stating that the majority of courts have decided to compel discovery under U.S. rules rather than the Hague Convention); *see, e.g.*, *Laydon*, 183 F. Supp. 3d at 420–26 (requiring that defendants comply with plaintiffs' discovery request in violation of the United Kingdom's Data Protection Act); Fenerjian v. Nong Shim Co., Ltd., No. 13-cv-04115-WHO (DMR), 2016 WL 245263, at *5–6 (N.D. Cal. Jan. 21, 2016) (granting plaintiff's motion to compel production of contact information for former employees in violation of Korea's Personal Information Protection Act).

[136] *See* Cour de cassation [Cass.] [supreme court for judicial matters] Paris, crim., Dec. 12, 2007, Bull. crim., No. 7168 [JurisData No. 2007-83228] (Fr.) [hereinafter *Christopher X*] (upholding the criminal conviction of the French party under the blocking statute for not complying with the Hague Convention, as well as the €10,000 fine against him); *see also Strauss*, 242 F.R.D. at 228 (ordering the French defendant to produce documents pursuant to U.S. discovery rules); *Air Cargo*, 278 F.R.D. at 54 (dismissing the possibility of criminal prosecution pursuant to the blocking statute as unlikely despite *Christopher X* and differentiating the case at bar because in *Christopher X* the defendant attempted to bypass the blocking statute by "deceptive means").

[137] GDPR, *supra* note 53, at 64. No comparable provision existed in the EU Directive, so Article 48 may have unpredictable effects on cross-border discovery. Kessler et al., *supra* note 123, at 577.

[138] GDPR, *supra* note 53, at 64.

erence than blocking statutes, which exist merely to impede discovery.[139] Whether courts view Article 48 of the GDPR as substantive data privacy law or as more similar to a blocking statute will heavily affect their decision to compel discovery.[140] Furthermore, the mere anticipation of the GDPR seems to have encouraged the EU DPAs to sanction large multinational companies for data privacy violations.[141] The atmosphere of EU data privacy is therefore clearly trending towards a toughening of data privacy protection.[142]

III. Increased Enforcement and Expansion of EU Data Privacy Law Justify More Deference in U.S. Discovery Deliberations

The purpose of the international comity analysis is to determine whether, and to what extent, foreign interests outweigh those of the United States.[143] While it is not appropriate in every case to rule that discovery should be conducted pursuant to the Hague Convention, foreign interests in the right to privacy should not be dismissed merely because it seems unlikely that a foreign litigant will be prosecuted for violations of data privacy law.[144] In order to duly respect EU data privacy law, U.S. courts must be willing to consider how important the right to privacy is in the European Union and the fact that litigants face an increasing risk of sanctions for data privacy violations.[145] Dismissing foreign interests as inherently less important than U.S. interests runs counter to the concept of international comity and the purpose of the

---

[139] *Aerospatiale*, 482 U.S. at 544 n.29.

[140] Kessler et al., *supra* note 123, at 610.

[141] *See* Schechner, *Facebook Privacy*, *supra* note 67 (noting that EU regulators are increasing enforcement actions in anticipation of a pivotal shift in the law); *see also supra* notes 53–66 and accompanying text (explaining the GDPR and its momentous impact on the future of data privacy, including that EU member states will have the formidable ability to fine companies up to four percent of their global revenue).

[142] *See supra* notes 28–66 and accompanying text (explaining the evolution of EU data privacy laws, with each new law imposing stronger obligations on data controllers than the previous one); *see also supra* notes 67–84 and accompanying text (explaining the increased enforcement of data privacy laws by EU regulators).

[143] Hilton v. Guyot, 159 U.S. 113, 163–64 (1895); Zambrano, *supra* note 103, at 161.

[144] *See* Société Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522, 544 n.28 (1987) (laying out a five-factor balancing test for determining if and when foreign interests are significant enough to outweigh U.S. interests); *In re* Xarelto (Rivaroxaban) Prod. Liab. Litig., MDL No. 2592, 2016 WL 3923873, at *17–18 (E.D. La. July 21, 2016) (determining in part that German interests in privacy outweighed U.S. interests despite the fact that the German defendant did not prove a cognizable chance of prosecution under German data privacy law because German law prioritizes privacy and the German government demonstrated its dedication to that right).

[145] *See Xarelto*, 2016 WL 3923873, at *17 (considering the fact that Germany had a notable stake in safeguarding the personal information of its citizenry); *see also supra* notes 28–66 and accompanying text (explaining the toughening of EU data privacy laws and potential for large sanctions in the future); *supra* notes 67–84 and accompanying text (explaining how EU regulators are cracking down on multinational companies for data privacy violations).

Hague Convention.[146] Section A of this Part discusses how U.S. courts should adjust their international comity analysis to properly respect EU data privacy law, and contends that courts should heavily weigh both EU interests in the right to privacy and the increased risk to litigants for violating EU data privacy law in favor of ordering discovery through the Hague Convention.[147] Section A also explains alternative methods for protecting information governed by EU data privacy law.[148] Section B provides policy arguments in favor of deferring to EU data privacy law when appropriate.[149]

A. U.S. Courts Should Increase Weight on the Fifth Aerospatiale Factor and Compel Discovery Through the Hague Convention if Appropriate

U.S. courts should respect EU data privacy law when considering discovery orders by adjusting their approach under the international comity analysis and, specifically, in regards to the fifth factor.[150] U.S. courts have historically found that U.S. interests in compelling discovery outweigh a foreign nation's interests in data privacy.[151] While it will not always be appropriate to rule that discovery should be conducted pursuant to the Hague Convention, U.S. courts should strongly consider foreign interests in privacy, and not merely as a matter of form.[152]

The Hague Convention provides a viable method for conducting foreign discovery that respects the sovereign interests of the nations involved.[153] Its procedures allow litigants to comply with their data privacy

---

[146] *See* Zambrano, *supra* note 103, at 177 (asserting that the overwhelming trend of cases finding that even insubstantial U.S. interests outweighed significant foreign interests was a "wholesale and total rejection of both international comity and the Hague Convention"); *supra* notes 98–102 and accompanying text (explaining the Hague Convention).

[147] *See infra* notes 150–164 and accompanying text.

[148] *See infra* notes 165–169 and accompanying text.

[149] *See infra* notes 173–192 and accompanying text.

[150] *See* SEDONA CONFERENCE, *supra* note 4, at 7 (advocating for courts to respect foreign data privacy laws and the concerns of people governed by them in the context of discovery); *supra* notes 117–122 and accompanying text (describing the *Aerospatiale* balancing test); *supra* note 123 and accompanying text (explaining that the fifth *Aerospatiale* factor has historically been the most significant).

[151] *See supra* note 135 and accompanying text (explaining how U.S. courts overwhelmingly rule that a foreign nation's interest in information privacy is secondary to U.S. interests); *see also supra* note 126 and accompanying text (explaining the same phenomenon in international comity cases generally).

[152] *See supra* notes 124–125 and accompanying text (explaining how U.S. courts superficially consider foreign interests and use of the Hague Convention before ultimately favoring U.S. interests and discovery rules); *infra* notes 173–192 and accompanying text (explaining policy arguments in favor of privacy rights and respecting foreign law).

[153] *Aerospatiale*, 482 U.S. at 561 (Blackmun, J., dissenting in part and concurring in part) (asserting that the Hague Convention established viable methods for litigants to conduct foreign discovery). The four-judge opinion concurring in part and dissenting in part actually advocated for

obligations while still achieving the goal of obtaining the relevant information.[154] Indeed, the United States was instrumental in creating the Hague Convention, and it seems odd that its courts have so frequently refused to use it.[155] U.S. courts should not hesitate to compel discovery through the Hague Convention when justified.[156]

The evolution of EU data privacy law over the last two decades shows an increasing trend towards stronger protections for data privacy and greater obligations and liability for data controllers.[157] The forthcoming GDPR should be considered substantive law and deferred to at a higher degree than blocking statutes because it explicitly declares the European Union's desire to preserve the privacy of its citizens' information and heightens sanctions for violations.[158] While, in the past, courts may have been correct in stating that there was a minimal chance of data privacy laws being enforced, they can no longer conclusively say so.[159] The fact that enforcement is expected

---

a rule of first resort to the Hague Convention. *Id*. at 548–49 (Blackmun, J., Brennan, J., Marshall, J., O'Connor, J., dissenting in part and concurring in part).

[154] *See id.* at 561, 565 (Blackmun, J., dissenting in part and concurring in part) (asserting that the Hague Convention established viable methods for litigants to conduct foreign discovery and that the Hague Convention is completely compatible with laws like the French blocking statute that allow for discovery pursuant to international agreements); Laydon v. Mizuho Bank, Ltd., 183 F. Supp. 3d 409, 420 (S.D.N.Y. 2016) (explaining the defendants' assertion that they wished to have the requested information produced in a matter compatible with their duties under UK data privacy law and that the Hague Convention is a sufficient alternate method for the Federal Rule of Civil Procedure because the United Kingdom regularly executes Hague Convention discovery requests).

[155] Zambrano, *supra* note 103, at 177; *see Aerospatiale*, 482 U.S. at 549 (Blackmun, J., dissenting in part and concurring in part) (noting that the United States advocated for and eagerly engaged in the creation of the Hague Convention).

[156] *See Aerospatiale*, 482 U.S. at 550 (Blackmun, J., dissenting in part and concurring in part) (maintaining that the Hague Convention advances U.S. interests because it supplies alternative foreign discovery methods that resolve the differences between civil and common law approaches to discovery, as well as promotes the U.S. long-term goal of fostering a peaceful international environment); *infra* notes 153–155 and accompanying text (explaining the viability of the Hague Convention).

[157] *See In re* Xarelto (Rivaroxaban) Prod. Liab. Litig., No. 4:17-CV-578, 2016 WL 3923873, at *17 (E.D. La. July 21, 2016) (considering the fact that Germany recently changed its Data Protection Act to more strongly safeguard personal information when balancing the U.S. and German national interests).

[158] Kessler et al., *supra* note 123, at 609–10; *see Aerospatiale*, 482 U.S. at 544 n.29 (noting that substantive laws deserve more deference than blocking statutes); *see also supra* notes 137–140 and accompanying text (explaining Article 48 of the GDPR).

[159] *See* Bennett, *supra* note 5, at 63 (positing that recent developments in EU law mean that companies in U.S. litigation might be able to more successfully argue that there is a true threat of sanctions for violating them) (citing Bodner v. Paribas, 202 F.R.D. 370, 375 (E.D.N.Y. 2000); Adidas (Canada) Ltd. v. SS Seatrain Bennington, Nos. 80 Civ. 1911 (PNL), 82 Civ. 0375 (PNL), 1984 WL 423, at *3 (S.D.N.Y. 1984)); *see also* Strauss v. Credit Lyonnais, S.A., 242 F.R.D. 199, 221 (E.D.N.Y. 2007) (refusing to accept the French blocking statute as a reason that litigants could not comply with discovery demands in part because "there is no significant risk of prosecution for violations of the French blocking statute"); *supra* notes 67–84 and accompanying text

to escalate, as well as the significant sanctions provided for under the forthcoming GDPR, should be considered.[160] EU regulators have been cracking down on data privacy violations and imposing substantial fines on prominent companies that process EU citizens' data.[161] Accordingly, U.S. courts should start taking the threat of EU sanctions seriously and consider the adverse effects of ordering foreign litigants to violate EU data privacy laws.[162] The Second and Ninth circuits consider the "hardship" or harm that would be caused to litigants if they were ordered to violate foreign law.[163] Given these developments, as well as policy considerations for international comity and privacy, U.S. courts should no longer dismiss EU privacy interests when weighing the fifth factor identified in *Aerospatiale* and compel discovery through the Hague Convention when appropriate.[164]

Alternatively, should U.S. courts be unwilling to find that the Hague Convention is the proper means for obtaining information located in the European Union, there are other options for safeguarding the personal information of EU citizens from disclosure in U.S. discovery.[165] First, courts

(summarizing the increase in EU enforcement actions against large multinational companies for data privacy violations).

[160] *See supra* notes 65–66 (explaining that the GDPR imposes high sanctions for data privacy violations of up to 4% of a company's annual revenue); *see also* Kessler et al., *supra* note 123, at 609 (stating that it is believed that EU DPAs will intensify enforcement when the GDPR comes into force).

[161] *See supra* notes 67–84 and accompanying text (describing enforcement actions by EU DPAs against companies like Google, Facebook, and Microsoft that included fines of hundreds of thousands of Euros). There is also a generally hostile attitude towards U.S. technology companies in the European Union. *See supra* note 73 and accompanying text (pointing out the EU hostility towards U.S. companies like Google, Amazon, and Apple).

[162] *See supra* notes 67–84 and accompanying text (summarizing the increase in EU enforcement actions against large multinational companies for data privacy violations).

[163] *See* Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1475 (9th Cir. 1992) (stating that beyond the five *Aerospatiale* factors, the court has also examined how incompatible legal obligations would adversely affect a foreign litigant); United States v. First Nat. City Bank, 396 F.2d 897, 902 (2d Cir. 1968) (stating that when a litigant is subject to the laws of two countries, the court must contemplate how incompatible legal obligations would adversely affect that litigant).

[164] *See* SEDONA CONFERENCE, *supra* note 4, at 3 (explaining that in some instances courts have decided against ordering discovery because of significant privacy interests); *supra* notes 117–122 and accompanying text (describing the *Aerospatiale* balancing test for international comity analysis); *infra* notes 176–183 and accompanying text (explaining the benefits of international comity); *infra* notes 184–192 and accompanying text (explaining why privacy rights are worthy of protection); *see, e.g.*, *Xarelto*, 2016 WL 3923873, at *17–18 (determining in part that German privacy interests outweighed U.S. interests because Germany's law and government prioritize privacy); Volkswagen, A.G. v. Valdez, 909 S.W.2d 900, 901–03 (Tex. 2015) (holding that a German company was not required to produce personal information in violation of German data privacy law in part because Germany's interests in privacy rights would be subverted).

[165] *See infra* notes 166–169 and accompanying text (describing alternatives).

can limit the scope of discovery conducted in the European Union.[166] Second, courts can encourage use of measures like protective orders and redaction when EU personal data is produced in discovery.[167] A protective order demonstrates to DPAs that data privacy laws are being acknowledged and that the private information will be dealt with appropriately.[168] Privacy is not only worthy of protection, but it is also a fundamental right in the European Union, and so it should be preserved as much as possible.[169]

B. Policy Reasons for Respecting EU Data Privacy Law

There are rationales for deferring to foreign law in some instances beyond mere legal arguments.[170] For instance, courts looking to the principle of international comity for guidance would be beneficial in many ways.[171] Additionally, privacy is an important right and courts should aspire to protect it whenever possible.[172]

This section discusses policy rationales for respecting the EU's data privacy laws and its interest in privacy rights.[173] Subsubsection One explains the benefits of international comity and the harm that could result from dismissing it.[174] Subsubsection Two explains why the right to privacy is important and should be protected.[175]

---

[166] *See* SEDONA CONFERENCE, *supra* note 4, at 12 (prescribing that the range of information requested in discovery should be restricted to information that is pertinent and required for the litigation to reduce hardship caused by incompatible legal obligations, as well as harm to the subject of the information).

[167] *See id.* at 16, 17 (advocating for courts to preserve information protected by foreign data privacy law and curtail the harm to foreign litigants from incompatible discovery and data privacy duties through protective orders); *see, e.g.*, *Xarelto*, 2016 WL 3923873, at *17 (noting that unnecessary information could be redacted before being produced); Fenerjian v. Nong Shim Co., Ltd., No. 13-cv-04115-WHO (DMR), 2016 WL 245263, at *5 (N.D. Cal. Jan. 21, 2016) (noting that there was a protective order in place in the case stipulating that the data protected by Korea's data privacy law received confidential treatment); *Bodner*, 202 F.R.D. at 376 (asserting that utilizing a protective order mitigates privacy worries).

[168] SEDONA CONFERENCE, *supra* note 4, at 17.

[169] Francesca Bignami, *A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 641 (2007); *see infra* notes 184–192 and accompanying text (explaining policy rationales for protecting data privacy).

[170] *See infra* notes 176–192 and accompany text.

[171] *See infra* notes 176–183 and accompany text.

[172] *See infra* notes 184–192 and accompany text.

[173] *See infra* notes 176–192 and accompany text.

[174] *See infra* notes 176–183 and accompany text.

[175] *See infra* notes 184–192 and accompany text.

1. International Comity in Discovery: An Argument for Respecting Foreign Law and Limiting Court-Ordered Law Breaking

The central purpose of international comity in the discovery context is to facilitate harmony in the global legal system.[176] A lack of international comity can, therefore, cause undesirable results.[177] U.S. court orders to violate the laws of foreign nations have surged astronomically in the last fifteen years.[178] These cases usually involve discovery requests and thus apply the five-factor *Aerospatiale* test.[179] The *Aerospatiale* comity analysis is highly criticized, in part because it strongly depends on subjective evaluations by the court, and its application has resulted in an undeniable "pro-forum bias" in favor of U.S. interests.[180] Not only is it disconcerting that U.S. courts are in effect making decisions based on litigants' nationalities, but this pro-forum bias has directly corresponded to a dramatic rise in discovery requests involving court-ordered foreign law violation and, possibly, abusive discovery.[181] Furthermore, U.S. foreign relations suffer from the "legal imperialism" of expansive cross-border discovery orders denounced

---

[176] Zambrano, *supra* note 103, at 160. In the context of discovery, the Hague Convention is the best way to achieve international comity. *See* Stewart, *supra* note 96 (explaining that the Hague Convention is one of the leading judicial assistance treaties in international law today).

[177] *See* Geoffrey Sant, *Court-Ordered Law Breaking*, 81 BROOK. L. REV. 181, 182–83 (2015) (explaining the phenomenon of "pro-forum bias" in comity analysis by U.S. courts and the harm it causes).

[178] *Id.* Before 1987, when *Aerospatiale* was decided, it was highly uncommon for U.S. courts to order litigants to violate foreign law. *Id*. In 1987, one district court even stated its uncertainty of its ability to order the breaking of foreign law. *In re* Sealed Case, 825 F.2d 494, 498 (D.C. Cir. 1987); *id.* In the decade after *Aerospatiale*, a mere two cases applied comity analysis, but there have been over fifty cases in the last decade. Sant, *supra* note 177, at 225–26.

[179] Sant, *supra* note 177, at 181–82.

[180] *Id.* at 182. Four of the five *Aerospatiale* factors are subjective, asking judges to assess, for example, the importunate of the requested discovery and the risk of subversion of U.S. or foreign interests should the discovery not be executed. *See supra* notes 117–122 and accompanying text (describing the five *Aerospatiale* factors). U.S. judges have not hesitated to make their bias clear, citing "the United States' interests in vindicating the rights of American plaintiffs" as their grounds for directing the contravention of foreign law. Sant, *supra* note 177, at 182. Pro-forum bias was a major concern of the four dissenters in *Aerospatiale*., 482 U.S. at 552 (Blackmun, J., Brennan, J., Marshall, J., O'Connor, J., dissenting in part and concurring in part); Sant, *supra* note 177, at 182. Justice Blackmun expressed that pro-forum bias was "likely to creep into the supposedly neutral balancing process" because courts are likely to resort to the rules and procedures of their own jurisdiction to which they are accustomed, rather than defer to foreign law. *Aerospatiale*, 482 U.S. at 552 (Blackmun, J., dissenting in part and concurring in part). Critics of the *Aerospatiale* test have asserted that it is a "confusing and unworkable standard" and that the balancing test offers a mere pretense of reasonableness. Sant, *supra* note 177, at 189.

[181] Sant, *supra* note 177, at 182. Parties in U.S. litigation have adopted the strategy of extracting settlements from the opposing party by purposely requesting unnecessary documents whose production would violate foreign law, thereby ensnaring the foreign litigant in a "Catch-22." *Id.* The fact that U.S. courts have been consistently inclined to order such discovery appears to have considerably motivated litigants to request it. *Id*.

by countries like China, France, Germany, and Switzerland.[182] It is in the best interests of the United States to respect EU data privacy law in the context of discovery orders.[183]

2. Data Privacy Is Worthy of Protection by the United States

In the modern digital age, technological advancements mean that almost everything a person does is trackable and recordable, and that information can now be used in more ways than ever.[184] High-profile data breaches and revelations of government surveillance have brought privacy issues to the forefront of public discourse.[185] The majority of U.S. citizens are concerned about privacy and control over their personal information, and they desire stronger protection for personal privacy.[186] The U.S. legal approach to data privacy, however, is decidedly weaker than that of other countries, and is often criticized as deficient.[187] The U.S. Constitution does not provide for the right to

---

[182] Zambrano, *supra* note 103, at 157. The Supreme Court noted that some extra-jurisdictional exercises of U.S. law can amount to "legal imperialism" incompatible with the concept of international comity. F. Hoffmann-La Roche Ltd. v. Empagran S.A., 542 U.S. 155, 169 (2004); Zambrano, *supra* note 103, at 180.

[183] *See* Zambrano, *supra* note 103, at 197 (asserting that legal disputes involving discovery necessarily touch on significant foreign interests like the economy, diplomacy, and international legal coordination, thus requiring a strong consideration of international comity). The *Aerospatiale* balancing test requires consideration of U.S. interests; stable foreign relations have been considered an important interest of the United States. *See* Daimler AG v. Bauman, 134 S. Ct. 746, 762–63 (2014) (finding that comity concerns weighed against applying a U.S. law to a German party partly because of potential repercussions for international relations).

[184] Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 355 (2015).

[185] *See* Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ [https://perma.cc/B6B4-YGZK] (observing that the Snowden disclosures of government surveillance facilitated public dialogue about privacy in the United States). The Pew Research Center found that 64% percent of U.S. adults have been a victim of a major data breach. Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, PEW RES. CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/ [https://perma.cc/MPU5-GD8R].

[186] *See* Rainie, *supra* note 185 (citing Pew Research polls that found that 91% percent of U.S. adults feel that the public no longer has control over how businesses process their personal information; 74% said that being in control of who has access to their information is "very important"; 65% said that what kind of information was gathered about them was significant); *see also* Brookman, *supra* note 184, at 355 (observing that a multitude of polls show that U.S. consumers want legal authority over their personal data).

[187] *See* Brookman, *supra* note 184, at 357–58 (asserting that the U.S. privacy law regime is "lag[ging] behind the rest of the world" because it does not provide comprehensive personal data protection like most developed countries); Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 J. CORP. L. 461, 462 (2016) (observing that numerous critics of the U.S.' self-regulating data privacy regime claim it is ineffectual and improper because businesses are expected to regulate data privacy, but the less regulation results in greater profits). Internet privacy laws in the United States are enforced by the FTC, which can only go after businesses that violate their own privacy policies. *Id*. at 467. Data privacy

privacy, unlike the constitutions of most nations which establish a fundamental right to privacy.[188]

Privacy has always been viewed as an important human right, and Americans are highly concerned with privacy issues.[189] The United States, however, seems to be trending away from stronger protection for personal information.[190] It is in the best interests of the United States to reverse that trend and respect individuals' right to privacy.[191] Even in absence of domestic legal reform, U.S. courts should at least respect that privacy is a fundamental right in many foreign countries, including the European Union, and

---

in the United States is largely reliant on self-regulation within certain industries, but most foreign nations rely on comprehensive state regulation. Gaff et al., *supra* note 12, at 9 (describing the differing approaches to data privacy).

[188] Ryan Moshell, . . . *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH. L. REV. 357, 364 n.53 (2005); *see What Is Privacy?*, PRIVACY INT'L, https://privacyinternational.org/explainer/56/what-privacy [https://perma.cc/SE28-5BUV] (noting that more than 130 countries' constitutions include privacy protection); *see also* Charter of Fundamental Rights of the European Union 2016 O.J. C 202/389, 395 [hereinafter EU Charter of Fundamental Rights] (guaranteeing every EU citizen a right of "respect for his or her private and family life, home and communications"); EU Charter of Fundamental Rights, *supra*, at art. 8 (guaranteeing the "right to the protection of personal data"). The right to privacy in America is not specifically provided for in the U.S. Constitution, but has been found to be an implied right in other ways. Fairclough, *supra* note 187, at 465; *see* Roe v. Wade, 410 U.S. 113, 152 (1973) (acknowledging that the Supreme Court has inferred a right to privacy from the First, Fourth, and Ninth Amendments, the Bill of Rights, and the idea of liberty provided for by the Fourteenth Amendment).

[189] *See* Moshell, *supra* note 188, at 364 (noting that the concept of privacy is one that can be traced throughout history to ancient civilizations); *supra* notes 185–186 and accompanying text (explaining Americans' feelings toward privacy).

[190] Brookman, *supra* note 184, at 356; *see* Natasha Singer, *Why a Push for Online Privacy Is Bogged Down in Washington*, N.Y. TIMES (Feb. 28, 2016), https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html?_r=0 [https://perma.cc/2H6L-EMHT] (discussing the Obama administration's failed proposal for a comprehensive privacy law that would have established consumer privacy as a fundamental right of U.S. citizens); Tom Wheeler, *How the Republicans Sold Your Privacy to Internet Providers*, N.Y. TIMES (Mar. 29, 2017), https://www.nytimes.com/2017/03/29/opinion/how-the-republicans-sold-your-privacy-to-internet-providers.html?emc=edit_th_20170329&nl=todaysheadlines&nlid=62836501&_r=1 [https://perma.cc/6HKK-328N] (explaining how in 2017 the House of Representatives revoked restrictions on internet service providers, allowing them to sell their customers' personal data). The bill, approved by Congress in March 2017, is viewed as a huge setback for internet privacy, as it gives Internet Service Provider's "free rein" over customer data regarding browsing history, shopping patterns, physical location, and other internet activity, while also precluding the Federal Communications Commission from prescribing similar safeguards for consumer privacy in the future. Wheeler, *supra*.

[191] *See* Fairclough, *supra* note 187, at 478 (advocating that the United States enact a new data privacy legal framework that comprehensively protects the personal information of its citizens); *see also* Matthew Crain, *How Congress Can Fix Internet Privacy Rule*, CNN (Mar. 29, 2017), http://www.cnn.com/2017/03/29/opinions/internet-privacy-crain/ [https://perma.cc/W2V3-465Z] (asserting that the public must increase political pressure for stronger privacy protections such as a universal opt-in law so that the status quo on the internet would be privacy rather than automatic surveillance).

take that right seriously when balancing the factors of international comity analysis for the purposes of discovery.[192]

CONCLUSION

Courts should not order foreign litigants to violate data privacy laws by which they are governed. Data privacy law protects an important individual right, and the Hague Convention provides a viable alternative that achieves the goal of obtaining discovery while simultaneously respecting foreign law and harmonizing the international legal sphere. The recurring justification of courts that EU data privacy law is unlikely to be enforced can no longer be argued with certainty. Recent changes in EU data privacy law in favor of more stringent rules, the potential for massive sanctions, and the increased data privacy law enforcement actions taken by EU member states makes EU enforcement a more serious possibility. The principle of international comity, furthermore, calls on courts to consider any laws or interests of foreign nations that are implicated. Additionally, privacy in and of itself is a valuable right that should be protected when practicable to do so. U.S. courts should more strongly consider data privacy law, EU interests, and the hardship placed on foreign parties when making discovery deliberations.

SAMANTHA CUTLER

[192] *See supra* note 144 and accompanying text (explaining the *Aerospatiale* balancing test and citing a case that respected EU data privacy interests).