The Long Arm of the European Privacy Regulator: Does the New EU GDPR Reach U.S. Media Companies?

KURT WIMMER

Since the advent of publishing on the Internet, media companies have been rightly concerned about the problem of international jurisdiction. Repeatedly, media companies with few contacts outside of the United States have been subjected to the jurisdiction of distant courts in countries from Australia to Zimbabwe applying their own domestic law to content that should be governed by the First Amendment and the standards set by U.S. law.[1]

One of the most significant concerns to media companies globally has been the rise of the so-called "right to be forgotten" in the European Union ("EU") and elsewhere, as well as the general ascendance of privacy concerns in the context of newsgathering and publishing news and information. The right to be forgotten, recently enforced against Google to require articles to be de-listed from search results, has a long history in the EU.[2] Two 2016 cases in Belgium[3] and Italy[4] required newspapers to anonymize articles under right to be forgotten petitions, with one saying that the public's right to information has an expiration date as short as two years. Although this trend has not been universal,[5] it is likely that publishers will continue to receive data anonymization orders from certain European courts.

This concept and a wide array of new privacy obligations are now part of the General Data Protection Regulation ("GDPR"), the largest and most significant overhaul of EU privacy law in more than 20 years. The GDPR will be a sea-change in EU privacy law for many reasons, including fines that can amount to as much as 4 percent of a company's *global* revenues and the creation of a new and powerful pan-European privacy regulatory agency.

The GDPR enters into force on May 25, 2018. European media companies, to be sure, are gearing up to comply with the GDPR. The open question for companies operating outside of the borders of Europe, however, is whether this stringent new regulation will apply to them, even though they have little or no actual presence within the EU.

The GDPR aspires to a broad jurisdictional reach, and is almost certainly intended to cover companies with websites that use cookies and other tracking devices to monitor people in the EU. Once subject to the GDPR's jurisdiction, a non-EU media company could be confronted with substantial enforcement burdens, such as court orders to fulfill right to be forgotten requests that would be untenable under American law — and face substantial fines for refusing to comply with such an order.

Even though the GDPR aspires to global jurisdiction, that aspiration does not answer the question of whether an EU law can have extraterritorial effect outside the boundaries of Europe. There are longstanding rules and norms of international jurisdiction that must be satisfied before regulatory agencies and courts can exercise jurisdiction over distant subjects.

This article analyzes those principles and concludes that pure U.S. media companies would have persuasive arguments against the jurisdiction of EU regulatory authorities and courts to enter orders against them, and a strong argument against the enforcement of such orders or subsequent fines. Aside from legal considerations, however, there may be significant reputational and practical issues that arise from resisting an order under the GDPR that companies will take into consideration.

I. The GDPR

The GDPR was developed with the goal of providing consistent privacy protections for individuals across the EU.[6] Prior to the adoption of the GDPR, each EU member country implemented its own data privacy laws under the guidance of the 1995 EU Data Protection Directive (the "Directive").[7] The result was a patchwork of somewhat divergent privacy protections among EU countries, which led to claims that companies could strategically select their EU country affiliations based on the strength of local privacy laws.[8] The GDPR aims to "harmoni[ze]" privacy laws in the EU by providing the same strong data protections for the entire region.[9]

In addition to harmonizing privacy protections across the board, the GDPR broadens the jurisdictional reach of the Directive.[10] The GDPR covers data controllers and processors outside the EU if they offer goods and services to, or monitor the behavior of, EU data subjects.[11] Behavior monitoring occurs when a natural person is "tracked on the internet," including the use of personal data to "profil[e] a natural person, particularly in order to take decisions concerning her or him or for analy[zing] or predicting her or his personal preferences, behavio[rs] and attitudes."[12] Personal data is defined as "any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as … [an] online identifier."[13] The intention behind this broad scope is to "ensure that individuals are not deprived of

Kurt Wimmer *U.S. Chair, Data Privacy and Cybersecurity Practice, Covington & Burling LLP, Washington, D.C.**The author is grateful for the inspired assistance of Chloe Goodwin and Danielle Kehl, both members of the Class of 2018 at Harvard Law School.*

protection of their data" when they are in the EU, and to "enhance[] legal certainty for controllers and data subjects."[14] The GDPR's intended jurisdiction almost certainly aspires to cover websites and services outside of the EU that use cookies to monitor the behavior of individuals in the EU.

II. The Jurisdictional Aspirations of the GDPR

The GDPR contains a broad jurisdictional test. There are, however, specific principles under international law to assess when the extraterritorial reach of a state is permissible under international law.

A. Bases for International Jurisdiction

Under international law, there are several traditionally recognized bases for asserting jurisdiction, including the territoriality principle, the nationality principle, the passive personality principle, and the protective principle.[15] Especially with regard to online conduct, states have also increasingly exercised jurisdiction under variations of these principles such as the objective territoriality test and the effects doctrine.

Territoriality and Nationality. The most commonly invoked principles are territoriality and nationality, which permit states to assert jurisdiction over what happens within their borders[16] as well as over acts committed by individuals and organizations of the state's nationality (even if those acts take place outside of the state's physical territory).[17] A variation of the traditional territoriality concept is the so-called "objective territoriality principle," under which a state can assert jurisdiction over acts that were initiated abroad but completed within a state's territory, as well as where a "constitutive element of the conduct" occurred in the state.[18] The jurisdictional test in the Directive appears to be a manifestation of the objective territoriality principle because it allows European regulators to assert jurisdiction over foreign websites or online service providers based solely on their use of equipment or the location of servers within the EU.[19]

Passive Personality and the Protective Principle. In addition to asserting jurisdiction over acts committed abroad *by* their own nationals, states can sometimes assert jurisdiction for acts committed *against* their own nationals by foreigners. The passive personality principle permits states to exercise authority based on their connection to the victim of illegal conduct. Although this basis for jurisdiction has ordinarily been limited to serious crimes (*e.g.*, terrorist attacks or assassinations) as opposed to ordinary torts or crimes,[20] it has occasionally been applied in the civil law context as well.[21] The United States has traditionally disfavored exercising jurisdiction under this principle, but more recently U.S. courts have recognized it in certain instances such as acts of terrorism.[22] The protective principle extends this idea to allow the state to protect itself (rather than its citizens) from harmful acts inflicted outside of its territory.[23]

The Effects Doctrine. Finally, under the so-called "effects doctrine," states can assert jurisdiction based on the fact that conduct taking place entirely outside of the state has substantial effects within the state.[24] The concept is closely related to the objective territoriality idea, but it does not require that *any* element of the conduct being regulated actually take place within the territory of the state.[25] The effects doctrine is generally regarded as the most controversial basis upon which to assert jurisdiction under international law, but despite criticism from legal scholars has become widely used with regard to conduct over the internet.[26]

B. Reasonableness Analysis in International Jurisdiction

The mere fact that conduct or activity falls under one of these bases for jurisdiction does not necessarily justify its exercise. The current presumption in international law is that the party seeking to assert jurisdiction has to further prove why it is reasonable to exercise extraterritorial jurisdiction under any one of the bases described above.[27] The Third Restatement of Foreign Relations Law provides various factors for the courts to balance in making this determination — a limitation on the exercise of jurisdiction reflected in U.S. domestic law that has also emerged as a principle of international law.[28] These factors include:

> (1) the link of the activity to the territory of the regulating state, including whether it has a "substantial, direct, and foreseeable effect,"
>
> (2) the connections between the regulating state and the person who is principally responsible for the activity or the person who is supposed to be protected,
>
> (3) the nature of the activity, its importance to the regulating state, and the extent to which other states regulate it,
>
> (4) the "existence of justified expectations that might be protected or hurt by the regulation,"
>
> (5) the importance of the regulation to the international system,
>
> (6) the extent to which the regulation is consistent with the traditions of the international system,
>
> (7) the extent to which another state may have an interest in regulating the activity, and
>
> (8) the likelihood of conflict with regulation of another state.[29]

If an evaluation of these factors suggests that the extraterritorial application of the law in question would be unreasonable, courts are likely to find that there is no jurisdiction.

The concept of reasonableness described in the Third Restatement is also closely aligned with the principle of comity, which is often characterized as the "golden rule" among nations — that is, that each state should respect the laws, policies, and interests of other states just as it would have others respect its own in similar circumstances.[30] Comity dictates that states should generally

avoid extraterritorial application of their laws against foreign citizens where those laws conflict.[31] Where two states have concurrent jurisdiction over an individual or a particular act, states should do a balancing test and defer to the state whose interests are clearly greater.[32]

In data protection and other internet-related cases, determining whether a jurisdictional basis should be exercised can be quite complex. The courts may consider the place where the data controller is established; the place where personal data is stored or processed; the place where the allegedly wrongful act occurs; the residence of the data subject; and the use of cookies or similar technologies in another state.[33] If jurisdiction is based on the location of the data controller or the location where a marketing email is received, the exercise of that jurisdiction tends to be accepted under the territoriality principle and effects doctrine.[34] On the other hand, a more tenuous connection, such as the use of a single tracking cookie, might be viewed with greater skepticism even if it could be construed as falling under the effects doctrine or the protective principle.

Ultimately, the strongest grounds for a regulator to assert jurisdiction over a non-EU media company would be to base it on a combination of the objective territoriality principle, the passive personality principle, and the effects test.[35] There is a colorable argument that such an assertion of jurisdiction would nonetheless be unreasonable under the Third Restatement test or otherwise violate the principles of comity. A successful argument against the application of the GDPR would likely require showing that it conflicted with a U.S. law or regulation, such as the First Amendment's free speech and free press protections, and that the publisher's free expression interests outweigh the European Union's interest in safeguarding its citizens' privacy rights.

III. Enforceability of EU Orders

Even if European DPAs can properly assert jurisdiction over websites and online service providers under the GDPR's jurisdictional test, it is highly unlikely that a U.S. court would enforce an EU order requiring a newspaper to alter its contents under a right to be forgotten request, or a subsequent fine for not complying with such an order. This is largely due to the fact that any right to be forgotten order would very likely infringe upon the publisher's First Amendment rights.

A. The First Amendment and the Right to be Forgotten

Any right to be forgotten order directed at a newspaper would almost certainly violate the First Amendment. In general, freedom of press can only be restricted to "prevent grave and immediate danger to interests which the state may lawfully protect."[36] Further, the First Amendment protects the publication of "lawfully obtain[ed] truthful information about a matter of public significance . . . absent a need . . . of the highest order."[37]

Although the Supreme Court has acknowledged the significance of an individual's right to privacy, "privacy concerns give way when balanced against the interest in publishing matters of public importance."[38] A full analysis of this issue would depend on the facts of a particular case and is beyond the scope of this article, but given the primacy of the First Amendment it is unlikely that an order requiring a newspaper to alter its content or archived material would be construed as consistent with freedom of the press.[39]

B. Lack of Enforceability Under International Law

International law also distinguishes between the ability to *apply* versus *enforce* laws extraterritoriality. As such, even if the GDPR is applicable to certain conduct of U.S. companies under international law, penalties for violating the law may not actually be enforceable.[40] Much like the jurisdiction to prescribe, a state's ability under international law to exercise jurisdiction over a foreign individual through its courts is also limited by whether it is "reasonable."[41]

The two tests for reasonableness, however, are not the same. The reasonableness standard that countries must meet in order to assert jurisdiction to adjudicate focuses on whether the relationship between the state and the person over which it wishes to exercise jurisdiction is reasonable. The distinction between jurisdiction to prescribe and jurisdiction to adjudicate can be analogized to the difference between subject matter jurisdiction and personal jurisdiction in U.S. law.

Section 421 of the Third Restatement of Foreign Relations Law lays out the criteria for reasonableness in this area. Once again, a foreign company's permanent physical presence in the state would likely qualify as reasonable grounds to assert jurisdiction.[42] However, exercising jurisdiction over a company located entirely outside the EU whose only activity was the use of browser cookies to track individuals in the EU would likely be viewed with greater skepticism.[43] Although a European regulator could attempt to assert jurisdiction based on the effects of that monitoring within the state,[44] the publisher has a plausible argument that the use of cookies does not have a "substantial, direct, and foreseeable" effect and that it would therefore be unreasonable to assert jurisdiction on the basis of cookies alone.

C. Lack of Enforceability Under U.S. Common Law

Under the doctrine of comity, U.S. courts will generally grant extraterritorial effect to the valid judgments of foreign courts.[45] First, a U.S. court must be satisfied that the foreign court properly had jurisdiction over the matter at hand.[46] For reasons stated above, it is likely that a right to be forgotten order under the GDPR would fail to fulfill this requirement.

Even if a U.S. court finds that the foreign court did have jurisdiction over the case, comity does not extend to orders that are found to be contrary to public policy.[47] A foreign judg-

ment is considered contrary to public policy "to the extent that it is repugnant to fundamental notions of what is decent and just in the State where enforcement is sought."[48] Another formulation of this concept defines a foreign order as contrary to public policy when it "direct[ly] violat[es] the policy of our laws, and does violence to what we deem the rights of our citizens."[49] This is a very high standard that requires more than the mere fact that there are differences between foreign and domestic law.[50] Among the policy issues that are considered grounds for refusal to enforce foreign orders are those that implicate constitutional rights.[51]

When a foreign judgment is one that would violate the First Amendment, courts have found that it violates public policy and is thus unenforceable.[52] For example, courts have consistently refused to enforce UK orders related to libel, because English libel law is considered to be antithetical to First Amendment doctrine.[53] Because an order or fine under the GDPR related to the right to be forgotten would almost certainly violate the First Amendment, a U.S. court would likely refuse to enforce such an order from an EU court.

D. Lack of Enforceability Under U.S. Statutory Law: The SPEECH Act

There is an additional a statutory basis to argue that any penalties would be unenforceable under U.S. law. The Securing the Protection of Our Enduring and Established Constitutional Heritage (SPEECH) Act was enacted in 2010 to codify the common law presumption against enforcing foreign libel judgments in U.S. courts. Under the SPEECH Act, foreign libel judgments are unenforceable unless the legislation applied offers "at least as much protection for freedom of speech and press," or the defendant would have been found liable if the case had been heard under U.S. law.[54]

Although the SPEECH Act has rarely been invoked in the seven years since its passage, it could apply here either directly or by analogy. Interpreted broadly, the SPEECH Act suggests that all foreign judgments that would violate the First Amendment or chill free speech should be unenforceable through the U.S. court system if those cases are deliberately brought in jurisdictions whose laws are less protective of free speech — as would likely be the case with right to be forgotten actions brought against U.S. companies abroad.[55] And even if read narrowly to apply only to libel cases, the SPEECH Act and its legislative history[56] offer persuasive evidence that Congress certainly did not intend to foreign laws that violate the First Amendment to be enforced by U.S. courts.[57]

IV. Practical Consequences and Policy Considerations

As any general counsel knows, strict applicability of the law is only one factor in determining a company's potential responses to an enforcement action. Even if a publisher has a strong legal argument against being subject to the GDPR — and particularly right to be forgotten requests — there may be significant practical and reputational costs associated with defying Europe and European law.

Privacy is considered to be a fundamental right in the EU; freedom of press, on the other hand, does not enjoy the same reverence it receives in the United States.[58] In a public opinion poll on personal data processing, 89 percent of Europeans said it was important that their personal data should always receive the same level of protection, regardless of whether the company holding that data is established in the EU.[59] Publically resisting a new and significant EU privacy law may attach a negative stigma to a publisher in the minds of privacy-focused Europeans. Accordingly, public perception and policy considerations will surely play a significant role in media companies' calculus of how to approach compliance with EU privacy law generally, and the GDPR in particular.

In making this calculus, U.S. companies are likely to focus on their current and future approach to Europe. Elements of this calculus might include the importance of Europe as a market for advertising and home for subscribers, whether the company operates offices or bureaus in Europe and employs Europeans, and whether the company expects to expands its operations in the EU in the future. GDPR compliance requires a great deal more preparation than merely determining whether a company will comply with specific orders under sections of the GDPR dealing with the right to be forgotten or privacy rights relating to newsgathering, of course; any assessment of whether a company will comply with the GDPR will focus not only on the editorial side of any internet publisher but the business and ownership sides as well.

In making these multifaceted going-forward decisions, however, it may be useful to consider that the jurisdictional reach of the GDPR should be tempered by the application of longstanding international principles that govern jurisdiction. For a purely non-EU entity, a realistic view of the likely exercise and enforcement of jurisdiction would be a useful complement to a clear-eyed look at the business realities of working within Europe.

Endnotes

1. *See* Pogoriler, Satterfield and Wimmer, *International Jurisdiction and the Internet in an Age of Cloud Computing*, Bureau of National Affairs/ Bloomberg (2011); Wimmer, *Toward a World Rule of Law: Free Expression*, 603 *Annals of the American Academy of Political and Social Science* 202 (2006); Wimmer, *Enforcing Foreign Judgments in the United States and Europe: When Publishers Should Defend,* International Libel and Privacy Handbook: A Global Reference for Journalists, Publishers, Webmasters and Lawyers (C.J. Glasser, ed., Bloomberg Press, 2006).

2. *See, e.g.*, Case C-131/12, Google Spain v. Agencia Espanola de Proteccion de Datos, 2014 EUR-Lex CELEX 62012CJ0131 (May 13, 2014).

3 *See* Hugh Tomlinson, *"Right to*

be Forgotten" Requires Anonymisation of Online Newspaper Archive, University of London: Information Law and Policy Centre (July 26, 2016), https://infolawcentre.blogs.sas.ac.uk/2016/07/26/ right-to-be-forgotten-requires-anonymisation-of-online-newspaper-archive/#more-1162 (summarizing Cour de Cassation [Cass.] [Court of Cassation], Apr. 29, 2016, C.15.0052.F (Belg.)).

4. *See* Guido Scorza, *A Ruling by the Italian Supreme Court: News do Expire*, L'Espresso (July 1, 2016), http://espresso.repubblica.it/attualita/2016/07/01/news/a-ruling-by-the-italian-supreme-court-news-do-expire-online-archives-would-need-to-be-deleted-1.275720?ref=HEF_RULLO&refresh_ce (summarizing Cass., 24 giugno 2016, n. 13161/16 (It.)); Athalie Matthews, *How Italian Courts Used the Right to be Forgotten to Put an Expiry Date on News*, Guardian (Sept. 20, 2016), https://www.theguardian.com/media/2016/sep/20/how-italian-courts-used-the-right-to-be-forgotten-to-put-an-expiry-date-on-news.

5. *See* Kristof Van Quathem, *Right to be Forgotten: High Courts Disagree*, Inside Privacy (June 2, 2016), https://www.insideprivacy.com/international/european-union/right-to-be-forgotten-high-courts-disagree/ (summarizing Cour de Cassation [Cass.] [Court of Cassation], May 12, 2016, [15-17729](Fr.)); Emiel Jurjens, Google Spain in the Netherlands III, Media Report (June 5, 2015), http://www.mediareport.nl/en/press-law/05062015/google-spain-in-the-netherlands-iii-does-convicted-murderer-have-right-to-be-forgotten/ (summarizing Rechtbank Noord-Nederland, Groningen, 1 mei 2015, ([redacted]/Vereniging Voor Veiligheid, Respect en Soldariteit) (Neth.)).

6. *See* Council of the European Union, Draft Statement of the Council's Reasons 3 (Mar. 31, 2016) (providing the Council's reasons for proposing the GDPR and repealing the Directive) [hereinafter Council's Reasons]; The Greens/European Free Alliance, EU General Data Protection Regulation: State of Play and 10 Main Issues 1 (2015), http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf [hereinafter State of Play].

7. *See* State of Play at 1; Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part I)*, 18 Int'l J.L. & Info. Tech. 176, 179 - 80 (2010).

8. See State of Play at 1

9. Council's Reasons at 3.

10. *See, e.g.*, Allen & Overy, the EU General Data Protection Regulation 3 (2017).

11. Regulation 2016/679, art. 3(2), 2016 O.J. (L 119) 1, 32 - 33 [hereinafter GDPR].

12. *Id.* at 5.

13. *Id.*

14. Council's Reasons at 7.

15. *See* Restatement (Third) of Foreign Relations Law § 402 (Am. Law Inst. 1987) [hereinafter Rest. (Third)]. Although the Third Restatement primarily reflects the development of the law as it has been interpreted and enforced by U.S. courts, these rules (especially relating to the reasonableness of exercising extraterritorial jurisdiction) tend to be followed by other states and have emerged as principles of customary international law. *Id.* § 403 cmt. a.

16. *Id.* § 402(1)(a)-(b).

17. *Id.* § 402(2).

18. Kuner at 188.

19. *Id.*

20. Rest. (Third) § 402 cmt. g (noting that the passive personality principle "has not been generally accepted for ordinary torts or crimes, but it is increasingly accepted as applied to terrorist and other organized attacks on a state's nationals by reason of their nationality, or to assassination of a state's diplomatic representatives or other officials.").

21. Kuner at 188-89.

22. *See, e.g.*, United States v. Bin Laden, 92 F. Supp. 2d 189, 221 (S.D.N.Y. 2000) (upholding exercise of jurisdiction because while the U.S. has traditionally not exercised jurisdiction under the passive personality principle, it is increasingly accepted for acts of international terrorism).

23. Rest. (Third) § 402(3).

24. Rest. (Third) § 402(1)(c); Kuner at 190. *See also* Hartford Fire Ins. Co. v. California, 509 U.S. 764, 796 (1993) (holding that a domestic law "applies to foreign conduct that was meant to produce and did in fact produce some substantial effect in the United States.").

25. Int'l L. Comm'n, *Rep. on the Work of Its Fifty-Eighth Session*, U.N. Doc. A/61/10, at 521-22 (2006).

26. *Id.*

27. Rest. (Third) § 403(1).

28. *Id.* § 403 cmt. a.

29. *Id.* § 403(2)(a)-(h).

30. *See, e.g.*, Joel R. Paul, *Comity in International Law*, 32 Harv. Int'l L.J. 1, 11 (1991). Comity is "the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience." Hilton v. Guyot, 159 U.S. 113, 163-64 (1895).

31. *See, e.g.*, Hartford Fire Ins. v. California, 509 U.S. 764 (1993).

32. Rest. (Third) § 403 cmt. e.

33. Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 2)*, 18 Int'l J.L. & Info. Tech. 227, 237-40 (2010).

34. *Id.* at 241.

35. Cedric Ryngaert, *Symposium on Extraterritoriality and EU Data Protection*, 5 Int'l Data Privacy L. 221, 222 (2015).

36. W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 639 (1943).

37. Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 102 (1979).

38. Bartnicki v. Vopper, 532 U.S. 514, 533 (2001). It appears that the Supreme Court has yet to define what qualifies as a matter of public importance.

39. Many commentators have noted as much. *See, e.g.*, Eric Posner, *We all Have the Right to be Forgotten*, Slate (May 14, 2014, 4:37 PM), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_ european_right_to_be_forgotten_is_just_what_the_internet_needs.html; Robert

G. Larson III, *Forgetting the First Amendment*, 18 Comm. L. & Pol'y 91 (2013) (asserting the right to be forgotten is "fundamentally at odds with the right of freedom of speech").

40. Rest. (Third), ch. 4 (Introduction).

41. *Id.* § 421 cmt. a.

42. *Id.* § 421(2)(c). Permanent presence does not require actual residence in an EU member state, but "transitory presence" (*i.e.*, brief presence in a state enabling "tag" jurisdiction) would not satisfy the requirement. *Id.* § 421 cmt. e.

43. Kuner at 235.

44. Rest. (Third) § 421(j) states that an exercise of jurisdiction to adjudicate is reasonable if "the person… had carried on outside the state an activity having a substantial, direct, and foreseeable effect within the state, but only in respect of such activity."

45. *See* Ritchie v. McMullen, 159 U.S. 235, 243 (1895); Velsicol Chem. Corp. v. Hooker Chem. Corp., 230 F. Supp. 998, 1018 (N.D. Ill. 1964); Gull v. Constam, 105 F. Supp. 107, 108 (D. Colo. 1952).

46. *See* Ackermann v. Levine, 788 F.2d 830, 837 (2d Cir. 1986).

47. Corporacion Mexicana De Mantenimiento Integral v. Pemex-Exploracion Y Produccion, 832 F.3d 92, 96 (2d Cir. 2016); *see* Hilton v. Guyot, 159 U.S. 113, 193 (1895); Rest. (Second) of Conflict of Laws § 117 cmt. c.

48. *See Ackermann*, 788 F.2d at 841.

49. *See Hilton*, 159 U.S. at 193.

50. *See id.* at 194; Somportex Ltd. v. Pa. Chewing Gum Corp., 318 F. Supp. 161, 168 (E.D. Pa. 1970).

51. *See, e.g.*, Mata v. Am. Life Ins. Co., 771 F. Supp. 1375, 1384 (D. Del. 1991) (due process).

52. See Matusevitch v. Telnikoff, 877 F.Supp. 1, 2 (D.D.C. 1995) ("Because recognition and enforcement of a foreign judgment, based on libel standards that are repugnant to the public policies of the State of Maryland and the United States, would deprive the plaintiff of his First and Fourteenth Amendment rights, the court grants summary judgment for the plaintiff as a matter of law.").

53. *See id.*; Abdullah v. Sheridan Square Press, Inc., 1994 WL 419847, at *1 (S.D.N.Y. May 4, 1994) ("Since establishment of a claim under the British law of defamation would be antithetical to the First Amendment-protections accorded the defendants, the second cause of action alleged in the complaint is dismissed." (citation omitted)); Bachchan v. India Abroad Publ'ns Inc., 585 N.Y.S.2d 661, 662 (Sup. Ct. 1992) (denying summary judgment on the grounds that "[t]he protection to free speech and the press embodied in [the First Amendment] would be seriously jeopardized by the entry of foreign libel judgments granted pursuant to standards deemed appropriate in England but considered antithetical to the protections afforded the press by the U.S. Constitution").

54. 28 U.S.C. §§ 4101-05.

55. In the findings section of the bill, Congress noted that "[t]he freedom of speech and the press is enshrined in the first amendment to the Constitution, and is necessary to promote the vigorous dialogue necessary to shape public policy in a representative democracy" and that "[s]ome persons are obstructing the free expression rights of United States authors and publishers, and in turn chilling the first Amendment to the Constitution of the United States interest of the citizenry in receiving information on matters of importance, by seeking out foreign jurisdictions that do not provide the full extent of free-speech protections. . . that are available in the United States."

56. *See, e.g.*, S. Rept. 111-224, at 8 (2010) (noting that "[t]he SPEECH Act will ensure that no domestic court can be used to diminish the First Amendment rights of American authors, reporters and publishers by enforcing a foreign libel judgment that is inconsistent with U.S. law. . . . This bill will prevent the chilling of American free speech that is the inevitable result of these foreign libel lawsuits.").

57. Dana Green, *The Speech Act Provides Protection Against Foreign Libel Judgments*, Am. Bar Ass'n (n.d.), http://apps.americanbar.org/litigation/litigationnews/mobile/firstamendment-SPEECH.html (noting that "[t]he act's symbolic significance, as an expression of the depth of Congressional commitment to free speech, should be heartening to free speech advocates").

58. *See generally* Adam Liptak, *When American and European Ideas of Privacy Collide*, N.Y. Times (Feb. 27, 2010), http://www.nytimes.com/2010/02/28/weekinreview/28liptak.html.

59. Vera Jourova, Data Protection: Factsheet 4 (2015), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf.