FREE EXPRESSION AND EU PRIVACY REGULATION: CAN THE GDPR REACH U.S. PUBLISHERS?

Kurt Wimmer†

CONTENTS

† U.S. Co-Chair, Data Privacy and Cybersecurity Practice, Covington & Burling LLP, Washington, D.C. The author is grateful for the assistance of Kristof Van Quathem in the Brussels office of Covington & Burling LLP and for the inspired research and hard work of Chloe Goodwin and Danielle Kehl, both members of the Class of 2018 at Harvard Law School, without whom this article would not have been possible.

INTRODUCTION

Since the advent of publishing on the Internet, media companies have been rightly concerned about the reach of international jurisdiction over U.S. publishers. 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] Media companies publish locally, but must defend globally.

The question of whether distant law should apply to online publishers has taken on new immediacy because of a new European Union (EU) privacy law that is set to come into force in May 2018. This law, the General Data Protection Regulation (GDPR), is the largest and most significant overhaul of EU privacy law in more than twenty years.[2] The GDPR will be a sea-change in EU privacy law for many reasons, including fines that can amount of as much as four percent of a company's *global* revenues and the creation of a new and powerful pan-European privacy regulatory agency—and a new and more aggressive stance toward EU jurisdiction over non-EU companies.[3]

European media companies, to be sure, are gearing up to comply with the GDPR.[4] The open question for companies operating outside of the borders of Europe, however, is whether this stringent new regulation will apply to them. One reason that this question of jurisdiction is of significant concern to publishers is the GDPR's inclusion of the so-called

1. *See* Kurt Wimmer, Eve Pogoriler & Stephen Satterfield, *International Jurisdiction and the Internet in the Age of Cloud Computing*, BUREAU NAT'L AFF. 2 (2011); Kurt Wimmer, *Toward a World Rule of Law: Freedom of Expression*, 603 ANNALS AM. ACAD. POL. & SOC. SCI. 209–10 (2006). *See generally* Kurt Wimmer, *Enforcing Foreign Judgments in the United States and Europe: When Publishers Should Defend*, *in* INTERNATIONAL LIBEL AND PRIVACY HANDBOOK: A GLOBAL REFERENCE FOR JOURNALISTS, PUBLISHERS, WEBMASTERS AND LAWYERS 338–45 (C.J. Glasser, ed., Bloomberg Press, 2006) (summarizing several instances where U.S. based media companies were subject to litigation in foreign jurisdictions and explaining how U.S law and foreign law are reconciled and applied in those cases).

2. Council Regulation 2016/679, 2016 O.J. (L 119) 1; *Getting Ahead of the GDPR Deadline: Why Consistency is Key*, GDPR.REP. (May 22, 2017), https://gdpr.report/news/2017/05/22/getting-ahead-gdpr-deadline-consistency-key/.

3. ERNST & YOUNG, EU GENERAL DATA PROTECTION REGULATION: ARE YOU READY? 2–3 (2016).

4. Sara Fischer & Kim Hart, *Companies Brace for European Privacy Rules*, AXIOS (Aug. 1, 2017), https://www.axios.com/american-companies-brace-for-gdpr-firestorm-2467635383.html; Aliya Ram, *Tech Sector Struggles to Prepare for New EU Data Protection Laws*, FIN. TIMES (Aug. 30, 2017), https://www.ft.com/content/5365c1fa-8369-11e7-94e2-c5b903247afd; Chiara Rustici, *What Should a Company's 2017 EU General Data Protection Regulation Budget Look Like?* BLOOMBERG BNA (Jan. 11, 2017), https://www.bna.com/companys-2017-eu-n73014449643/.

"right to be forgotten"—the right of an EU national to insist that data about her or him be erased.[5] 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.[6] Two 2016 cases in Belgium[7] and Italy[8] required newspapers to anonymize articles under right to be forgotten petitions, with one saying that the public's right to information can expire "just like milk," in as short a time as two years.[9]

Under pre-GDPR law, publishers outside of the EU could structure their activities to avoid EU jurisdiction and avoid issues under the right to be forgotten.[10] The GDPR aspires to a broad jurisdictional reach, and it is intended to cover any company, anywhere in the world, with an online presence that "monitors the behavior" of EU data subjects.[11] 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[12]—and face substantial fines for refusing to comply with such an order.[13]

The GDPR's aspiration to global jurisdiction, however, does not answer the question of whether any EU law properly can have

5. Roy Greenslade, *Does 'the Right to be Forgotten' Ruling Threaten Our Right to Know?* GUARDIAN (Sept. 19, 2016), https://www.theguardian.com/media/greenslade/2016/sep/19/does-the-right-to-be-forgotten-ruling-threaten-our-right-to-know; Josh Halliday, *Google to Fight Spanish Privacy Battle*, GUARDIAN (Jan. 16, 2011), https://www.theguardian.com/technology/2011/jan/16/google-court-spain-privacy.

6. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 EUR-Lex CELEX 62012CJ0131 ¶ 98 (May 13, 2014).

7. *See* Hugh Tomlinson, *"Right to be Forgotten" Requires Anonymisation of Online Newspaper Archive*, U. LONDON (July 26, 2016), https://infolawcentre.blogs.sas.ac.uk/2016/07/26/right-to-be-forgotten-requires-anonymisation-of-online-newspaper-archive.

8. 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 (citing Cass., 24 giugno 2016, n. 13161/16 (It.)); 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 (citing Cass., 24 giugno 2016, n. 13161/16 (It.) (holding that, given widespread access to online news pieces, two and a half years is a sufficient time period for the public to be informed, and therefore the right to privacy prevails over the right to be enforced once that period of time has passed)).

9. Matthews, *supra* note 8.

10. *See* Council Regulation 2016/679, *supra* note 2, at 33.

11. INTERNET ADVERT. BUREAU UK, THE EU GENERAL DATA PROTECTION REGULATION: A BRIEFING FOR THE DIGITAL ADVERTISING INDUSTRY 12 (2016).

12. KENT D. STUCKEY & ROBERT L. ELLIS, INTERNET AND ONLINE LAW 11–48 (2017).

13. *See* Council Regulation 2016/679, *supra* note 2, at 82–83.

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.[14]

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 GENERAL DATA PROTECTION REGULATION: A SEA-CHANGE IN EU LAW

The GDPR was developed with the goal of providing consistent privacy protections for individuals across the EU.[15] 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").[16] The result was a patchwork of slightly 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.[17] The GDPR aims to "harmoni[ze]" privacy laws in the EU by providing the same strong data protections for the entire region.[18]

In addition to harmonizing and strengthening privacy protections across the board, the GDPR broadens the jurisdictional reach of the Directive.[19] The GDPR covers data controllers and processors outside the EU if they offer goods and services to, or monitor the behavior of, EU

14. Arthur Lenhoff, *International Law and Rules on International Jurisdiction*, 50 CORNELL L. REV. 5, 5 (1964).

15. *See* COUNCIL OF THE EUROPEAN UNION, No. 2012/0011, DRAFT STATEMENT OF THE COUNCIL'S REASONS 3 (Mar. 31, 2016) [hereinafter COUNCIL'S REASONS] (providing the Council's reasons for proposing the GDPR and repealing the Directive); JAN PHILIPP ALBRECHT, EUROPEAN FREE ALL., EU GENERAL DATA PROTECTION REGULATION: STATE OF PLAY AND 10 MAIN ISSUES 3 (2015) [hereinafter STATE OF PLAY], http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf.

16. *See* STATE OF PLAY, *supra* note 15, 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).

17. *See* STATE OF PLAY, *supra* note 15, at 1.

18. COUNCIL'S REASONS, *supra* note 15, at 3.

19. ALLEN & OVERY LLP, THE EU GENERAL DATA PROTECTION REGULATION 3 (2017).

data subjects.[20] 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."[21] 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."[22] The intention behind this broad scope is to "ensure that individuals are not deprived of protection of their data" when they are in the EU, and to "enhance[] legal certainty for controllers and data subjects."[23] The GDPR's intended jurisdiction almost certainly aspires to cover websites and services outside of the EU that monitor the behavior of individuals in the EU.

II. THE JURISDICTIONAL ASPIRATIONS OF THE GDPR

The European Union always has been concerned about the potential avoidance of EU data protection laws by parties not established in the EU. The Directive, for example, provides that where parties not established in the EU use "equipment" in the EU to collect personal information, they are subject to the law.[24] In the early 1990s, when the Directive was drafted, lawmakers presumably were considering current technology, such as main-frame computers and servers, as the means to remotely collect personal information. This approach had the benefit (from the perspective of the potentially regulated entity) of permitting a company to decide whether it will be subject to European law by determining how to physically structure its business. As technology evolved, however, it quickly became apparent to regulators that reliance on "equipment" as a jurisdictional hook risks creating gaps, unless it is interpreted in an unjustifiably broad manner.[25]

20. Council Regulation 2016/679, *supra* note 2, at 32–33. A "data controller" is a party that controls data and makes the essential decisions about how the data will be treated. *Id.* at 33. A "data processor" is a party that processes data under the direction of a data controller. *Id.*

21. *Id.* at 5.

22. *Id.* at 33.

23. COUNCIL'S REASONS, *supra* note 15, at 7.

24. 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) 4(1)(c).

25. *See generally* Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation (unpublished manuscript 2013), http://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.

The GDPR uses an entirely different hook to attempt to capture additional behavior in the scope of the regulation. Article 3(2) of the GDPR applies specifically to entities not established in the EU and provides as follows:

> This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.[26]

The GDPR thus contains two criteria to establish its applicability to parties outside the EU. It applies to (1) parties offering services in the EU or (2) that monitor the behavior of EU users.

A. "Offering Good or Services"

In respect of the first prong concerning parties offering services in the EU, recital 23 of the GDPR contains a useful clarification:

> In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.[27]

Accordingly, the mere accessibility from the EU of a U.S. publisher's website or the use of English on a U.S. website are not sufficient to trigger the applicability of the GDPR. The targeting of EU users must be more obvious and "envisioned," for example, by allowing them to order goods and having them shipped to the EU, by using the Euro as

pdf. Some regulators now argue, for example, that the posting of cookies on a PC or laptop could be considered as use of equipment (i.e., the user's computer).

26. Council Regulation 2016/679, 2016 O.J. (L 119) art. 3, ¶ 2.

27. *Id.* at Recital 23.

currency option, or by offering content in languages adapted to EU users.

This first criterion of targeting a service is clearly inspired by existing case law in international private law. The key authority in this area is the *Pammer* case.[28] In this case, the Court of Justice of the EU (CJEU) was asked to clarify when an Internet service can be considered to target a Member State.[29] The CJEU held that mere accessibility of a website does not suffice. Similarly, the indication of the trader's address, e-mail address or phone number (without international code) cannot be construed as targeting.[30] To the contrary, the CJEU highlighted the following examples of activities that can demonstrate an intention to target:

1. The express mentioning that the service is provided to users in a Member State;
2. Paying search engines to have its website favorably indexed in order to facilitate access by consumers in particular Member States;
3. The international nature of the services;
4. The provision of international telephone numbers;
5. The use of internet domain levels other than those of where the service provider is established (or general ones, such as .eu, or .com19); and
6. The mentioning of international clientele, and accounts written by such customers.[31]

In the *Pammer* case, the service at issue, a travel package, was advertised on a third-party website.[32] The CJEU did not consider whether the third party website was a service targeting another Member State. The court only considered if the advertised service was targeting the Member State.[33] In relation to the intermediary website the court held:

> The fact that the website is the intermediary company's and not the trader's site does not preclude the trader from being regarded as directing its activity to other Member States, including that of the consumer's domicile, since that company [the website] was acting for and on behalf of the trader. It is for the relevant national court to ascertain whether the trader was or should have been aware of the international dimension of the intermediary company's activity and how the intermediary company

28. Case C-585/08, Pammer v. Reederei Karl Schlüter GmbH & Co., 2010 E.C.R. I-12527.

29. *Id.* ¶ 47.

30. *Id.* ¶ 95(2). The provision of this information is actually required under applicable e-commerce rules.

31. *Id.* ¶¶ 81, 83.

32. *Id.* ¶¶ 15, 16.

33. *Palmer*, 2010 E.C.R. I-12527 ¶ 47.

and the trader were linked.[34]

So a trader advertising its services on a third-party website may be targeting a Member State if the website targets that Member State, provided the trader can be reasonably aware of this and depending on the (contractual) relationship between the website and advertiser. The open question is whether this also applies in the other direction. In other words, can the intermediary, such as a news publisher, be considered to be targeting a Member State because it displays advertising directed to that Member State?

Websites often rely on third party advertising networks to deliver advertising. These networks target advertising to users based on the users' IP address and information obtained by means of cookies deployed by these networks via the publishers' and many other websites.[35] On this basis, it is quite possible that an all-U.S. website displays German advertising, if the advertising network that serves the advertising happens to know that the user is in Germany. This could happen unbeknownst to the publisher itself, which basically outsourced the advertising delivery on its website property to the advertising network. Is the serving of such "targeted" advertising evidence that the website is aimed at an EU audience? There is no clear guidance on this point. However, it stands to reason that this could be the case. If, as in the *Pammer* case, an advertiser can be expected to be aware of the geographic scope of the website on which it advertises, it could be argued that this website can also be aware of the international scope of the advertising network with which it contracts.

B. "Monitoring the Behaviour"

The second trigger for the applicability of the GDPR is whether the party outside the EU "monitors the behavior" of users in the EU. On this prong, recital 24 of the GDPR provides as follows:

> In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal

34. *Id.* ¶ 89.

35. FEDERAL TRADE COMM'N, FTC STAFF REPORT ON SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 2–3 (2009) [hereinafter FTC REPORT, ONLINE BEHAVIORAL ADVERTISING], https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

preferences, behaviours and attitudes.[36]

The recital assumes tracking of behavior that is quite extensive. The tracking should occur with the intention of influencing the user based on an analysis and prediction of personal preferences.[37] In the context of publisher websites, a relevant question is whether the publisher or the advertising network delivering the advertising actually tracking the user. In many cases, the tracking by the advertising network is likely to be much more extensive than by the website itself.[38] However, this does not mean that the publisher is not affected. In an opinion of June 2010, the Article 29 Working Party, which is composed of representatives of the data protection authorities for each EU Member State, argued that advertising networks can only operate in the way they do because publishers allow for it.[39] The publishers' websites redirect users to the advertising networks so that they can display advertising on the allocated publishers' website property. In doing so, publishers allow advertising networks to collect information about those users. According to the Working Party, the publishers could be co-responsible for this activity. In other words, publishers could be considered implicated in the monitoring of behavior of individuals in the EU because they rely on advertising networks that do so.[40]

In principle, the intention (or not) of websites and their adverting networks to specifically monitor EU visitors should not be relevant. From an EU perspective, the relevant factor is that personal information about EU residents is being collected to monitor and influence their behavior. The fact that it can reasonably be assumed that EU users will be implicated may suffice to trigger the application of the GDPR.

Whether this description of "monitoring" would apply to generally

36. Council Regulation 2016/679, *supra* note 2, at 5.

37. *Id.*

38. Joanna Geary, *Tracking the Trackers: What are Cookies? An Introduction to Web Tracking*, GUARDIAN (Apr. 23, 2012), https://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro.

39. ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 2/2010 ON ONLINE BEHAVIOURAL ADVERTISING 11, No. 00909/10/EN, (2010), https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/ notas_prensa/common/junio/ WP171en.pdf.

40. *Id.* at 11–12. A similar reasoning can be found in the recent (non-binding, but influential) opinion of Advocate General Bot in a pending case related to Facebook services. The Advocate General considered that a party creating a fan page on the Facebook platform is co-responsible for the collection of user data by Facebook. Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, 2017 CELEX 62016CC0210 (Oct. 24, 2017). Note that both documents address the allocation of responsibility once it is established that EU law applies. However, it would not be a big leap to apply the same argument in the context of the trigger for the applicability of the GDPR.

accepted Internet advertising techniques is an open question. Current Internet advertising strategies rely on data that does not contain contact or identifying information of "natural persons," but might rely on device identifiers, IP addresses, cookies, and other proxies for identifying a particular advertising subject on the Internet.[41] One could argue that "monitoring" that focuses on serving targeted advertising to a user based solely on device identifier, IP address, or other identifier that cannot be used to identify a "natural person" should not fall under the definition.

Recent EU cases suggest, however, that even general Internet advertising techniques that do not rely on the name or actual contact information of a particular Internet user might still be considered "monitoring" because of the broad definition of "personal information" favored by some European courts.[42] In *Google v. Vidal-Hall*, a British court held that browser-generated information collected using cookies (such as Internet surfing habits and news reading habits) constitutes private and/or personal information.[43] Although the use of cookies that do not collect personal data or track users—such as cookies that regulate a website's functionality—are unlikely to fall under the scope of the GDPR, cookies used to track individuals for advertising or other marketing purposes would likely be caught by the regulation.[44]

Maintaining logs of user IP addresses could also constitute monitoring, according to a recent ECJ case. In *Breyer v. Federal Republic of Germany*, the ECJ held that dynamic IP addresses registered by online media services providers could constitute personal data.[45] Notably, however, the court limited the ruling to cases where those service providers have some "reasonable means" to combine the IP address with other data that allows them to identify the individual.[46]

To the extent that courts and DPAs follow the approach set out by the court in *Google v. Vidal-Hall*, the publisher's use of cookies to collect information for advertising and other marketing-related purposes would likely qualify as "monitoring" under the definition of the GDPR. As long as the publisher continues to use cookies to track or target readers in

41. *See generally* FEDERAL TRADE COMM'N, CROSS-DEVICE TRACKING: AN FTC STAFF REPORT 2017, https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf (discussing current internet advertising strategies); FTC REPORT, ONLINE BEHAVIORAL ADVERTISING, *supra* note 35 (discussing behavioral advertising in order to deliver advertising to individual consumers).

42. *See, e.g.*, Google, Inc. v. Vidal-Hall [2015] EWCA (Civ) 311 [18] (Eng.).

43. *Id.* at [7.5].

44. *See id.* at [7.3]–[7.6].

45. Case C-582/14, 2016 E.C.R. 779 ¶ 49.

46. *Id.* ¶ 48.

Europe, therefore, European courts could plausibly interpret the GDPR as covering the company's activities, arguably exposing them to the requirements of GDPR as well as the jeopardy of potentially massive fines for violating it, even if the behavior of the publisher complied entirely with the laws of its own country.

To be sure, non-EU publishers would have a strong argument that the use of general Internet advertising techniques, without more, cannot constitute "monitoring" of EU data subjects. It is often impossible to know with any degree of certainty the country from which an online user is accessing an Internet service. Particularly if a publisher has not targeted EU data subjects specifically—for example, by advertising in a European language, using EU domains, specifically targeting advertising toward EU data subjects, or marketing subscriptions to European customers—a publisher would have a strong argument on the facts that it is not "monitoring" EU data subjects. Whether EU courts will accept such arguments, given that the GDPR's text appears focused on capturing Internet advertising techniques, remains to be seen.

III. INTERNATIONAL PRINCIPLES OF JURISDICTION AND THE GDPR

The GDPR contains a broad jurisdictional test.[47] There are, however, specific principles under international law to assess when the extraterritorial reach of a state is permissible under international law.[48]

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.[49] 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.[50]

1. Territoriality and Nationality

The most commonly invoked principles are territoriality and

47. *See* Council Regulation 2016/679, *supra* note 2, at 33 (establishing the test used to determine the expanse of jurisdiction over non-EU States).

48. *See* Kuner, *supra* note 16, at 188.

49. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 (AM. LAW INST. 1987). 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.

50. Kuner, *supra* note 16, at 188, 190.

nationality, which permit states to assert jurisdiction over what happens within their borders[51] 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).[52] 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.[53] 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.[54]

2. 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.[55] The passive personality principle permits states to exercise authority based on their connection to the victim of illegal conduct.[56] 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,[57] it has occasionally been applied in the civil law context as well.[58] 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.[59] 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.[60]

51. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402(1)(a)–(b).

52. *Id.* § 402(2).

53. Kuner, *supra* note 16, at 188.

54. Council Directive 95/46/EC, art. 4, 1995 O.J. (L 281).

55. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 cmt. g.

56. *Id.*

57. *Id.* ("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.").

58. Kuner, *supra* note 16, at 188.

59. *See, e.g.*, United States v. Bin Laden, 92 F. Supp. 2d 189, 221 (S.D.N.Y. 2000) (citing RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 cmt. g) (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).

60. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402(3).

3. 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.[61] 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.[62] The effects doctrine is generally regarded as the most controversial basis upon which to assert jurisdiction under international law,[63] but despite criticism from legal scholars has become widely used with regard to conduct over the Internet.[64]

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.[65] 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.[66] These factors include:

1. [T]he link of the activity to the territory of the regulating state, *i.e.*, the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory;
2. [T]he connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between that sate and those whom the regulation is designed to protect;
3. [T]he character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of

61. *Id.* § 402(1)(c); Kuner, *supra* note 16, at 190; *see* Hartford Fire Ins. Co. v. California, 509 U.S. 764, 796 (1993) (citing Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 582 (1986)) ("[A domestic law] applies to foreign conduct that was meant to produce and did in fact produce some substantial effect in the United States.").

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

63. Kuner, *supra* note 16, at 190.

64. *Id.*

65. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 403(1).

66. *Id.* § 403 cmt. a.

such regulation is generally accepted;

4. [T]he existence of justified expectations that might be protected or hurt by the regulation;
5. [T]he importance of the regulation to the international political, legal, or economic system;
6. [T]he extent to which the regulation is consistent with the traditions of the international system;
7. [T]he extent to which another state may have an interest in regulating the activity; and
8. [T]he likelihood of conflict with regulation by another state.[67]

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.[68]

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.[69] Comity dictates that states should generally avoid extraterritorial application of their laws against foreign citizens where those laws conflict.[70] 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.[71]

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.[72] 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.[73] On the

67. *Id.* § 403(2)(a)–(h).

68. *Id.* § 403 cmt. a.

69. *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, 164 (1895).

70. *See, e.g.*, Hartford Fire Ins. Co. v. California, 509 U.S. 764, 798–99 (1993).

71. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 403 cmt. e.

72. Kuner, *supra* note 16, at 237–40.

73. *Id.* at 241.

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.[74]

Ultimately, the strongest grounds for a regulator to assert jurisdiction over a non-EU publisher would be to base it on a combination of the objective territoriality principle, the passive personality principle, and the effects test.[75] 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. Such an argument could also point out the global nature of the Internet, and the fact that it is often difficult or impossible for a publisher to know, with certainty, the geographic location of a user of its services. When faced with broad laws such as the GDPR, publishers often are forced to apply EU legal requirements to all of their users[76]—a principle that will be familiar to any U.S. reader who has been forced by a U.S. website to grant consent to receive cookies, a requirement of the EU's e-Privacy Directive.[77] Such a practice can be only mildly annoying when applied to a needless cookie consent, but more serious when an EU regulatory demand directly contradicts U.S. standards for newsgathering and publication.

IV. WHAT TO EXPECT FROM EUROPEAN COURTS

Under the bases for international jurisdiction described above, European courts are likely to find that the GDPR's jurisdiction does extend to U.S. publishers with websites that employ standard Internet advertising

74. *Id.* at 242.

75. Cedric Ryngaert, *Symposium Issue on Extraterritoriality and EU Data Protection*, 5 INT'L DATA PRIVACY L. 221, 222 (2015).

76. Adrian Bridgwater, *Veritas: EU Data Protection Laws to Affect All Global Firms*, FORBES (May 25, 2016, 10:01 AM), https://www.forbes.com/sites/adrianbridgwater/2016/05/25/veritas-eu-data-protection-laws-to-affect-all-global-firms/#32eb109b2171 (reporting on Europe's imposition of stricter data storage requirements and corresponding costs to global firms with users in Europe, regardless of the company's country of origin); *see* Jeff Roberts, *Why Google, Facebook, and Amazon Should Worry About Europe*, FORTUNE (July 20, 2017), http://fortune.com/2017/07/20/google-facebook-apple-europe-regulations/ (reporting that the GDPR could significantly affect global tech firms' revenues in cutting off access to significant sources of advertising revenue).

77. 2002 O.J. (L 201) 41.

practices. Although it is not entirely clear how courts would balance the right to privacy, which is considered a fundamental human right in Europe,[78] against freedom of speech, a foundational right enshrined in the U.S. Constitution,[79] there is a possibility that a European court would order a U.S.-based publisher to comply with a right to be forgotten request. This section addresses a number of substantive issues that European courts would likely consider in deciding whether to assert jurisdiction if a European Data Protection Authority (DPA) were to bring an action against an American publisher under the GDPR. It considers Europe's historic approach to these issues, whether the use of cookies meets the GDPR definition of "monitoring," whether and how a right to be forgotten claim could be asserted against U.S. publishers, and analogous extraterritorial applications under U.S. law.

A. General Approach to Privacy Protection in Europe

The EU recognizes the right to privacy and the right to data protection as human rights in the Charter of Fundamental Rights of the European Union[80] (the "Charter") and the Treaty on the Functioning of the European Union.[81] The right to privacy is also recognized in the European Convention on Human Rights[82] and the International Covenant on Civil and Political Rights.[83] EU institutions generally consider Europe's privacy protections to be stricter than those in the United States.[84] The 2015 European Court of Justice (ECJ) case *Schrems v. Data Protection Commissioner* exemplifies this belief.[85] The ECJ struck down the Safe Harbor agreement that governed data transfers between the EU and the United

78. *See* Charter of Fundamental Rights of the European Union, arts. 7, 8, July 7, 2016, 2016 O.J. (C 202) 395 [hereinafter EU Charter]; *see also* Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community art. 16B, Dec. 13, 2007, 2007 O.J. (C 306) 51 ("Everyone has the right to the protection of personal data concerning them.").

79. *See* U.S. CONST. amend. I.

80. EU Charter arts. 7, 8, 2016 O.J. (C 202) 395.

81. Consolidated Versions of the Treaty on the Functioning of the European Union, art. 16(1), May 9, 2008, 2008 O.J. (C 115) 55.

82. Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14, Council of Europe, art. 8, Nov. 4, 1950, E.T.S 005.

83. United Nations Int'l Covenant on Civil and Political Rights art. 17, *adopted* Dec. 16, 1966, 999 U.N.T.S 14668.

84. *See* European Commission Press Release IP/16/2461, The Commission, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection For Transatlantic Data Flows (July 12, 2016).

85. *See generally* Case C-362/14, 2015 EUR-Lex CELEX C2014CJ0362 (Oct. 6, 2015) (enabling judicial review of the Austrian plaintiff's claim that Ireland did not ensure the adequate protection of his personal, private data, as required by EU Charter articles seven and eight when it transferred the storage of his personal data to the United States).

States, holding that the United States failed to ensure "a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order."[86]

That said, the right to data protection is not an absolute right in the EU. Under the Charter, fundamental rights may be limited so long as such a limitation is "provided for by law," "respect[s] the essence" of the right, and, "[s]ubject to the principle of proportionality," is necessary to "genuinely meet objectives of general interests recogi[zed] by the Union or the need to protect the rights and freedoms of others."[87] The ECJ turns to the principle of proportionality to determine whether the right to privacy and data protection has been unlawfully violated, asking whether the limitation in question is "appropriate for attaining the objective pursued and do[es] not go beyond what is necessary to achieve it."[88] Limitations to the protection of personal data "must apply only in so far as is strictly necessary."[89]

B. Limited Extraterritorial Applicability of the Directive

Although the jurisdictional reach of the Directive is less expansive than the GDPR, it has also been criticized by U.S. officials and businesses for overreaching when applied extraterritorially.[90] Article 4(1)(c) of the Directive authorized European DPAs to assert jurisdiction over non-European companies if they satisfied the "use of equipment" test, which has been understood to apply to websites or online service providers with servers or employees that process data in a particular EU member state.[91] The assertion of jurisdiction appears to be based largely on the objective territoriality theory, but the additional focus on the effect produced in the EU by data processing outside the EU suggests that it can also be understood as an application of the more controversial effects test as well.[92]

The European courts have placed some limits on the jurisdictional reach of the Directive, however. In *Bodil Lindqvist*, one of the first major decisions on the Directive's scope, the ECJ cautioned against the risk of the Directive's "special regime" becoming "a regime of general

86. *Id.* ¶ 96.

87. EU Charter art. 52(1), 2016 O.J. (C 202) 395.

88. Joined Cases C-92/09 & C-93/09, Volker & Markus Schecke GbR v. Land Hessen, 2010 E.C.R. I-11063 ¶ 74 (Nov. 9, 2010).

89. *Id.* ¶ 77.

90. *See, e.g.*, Kuner, *supra* note 16, at 177.

91. *See id.* at 190.

92. *Id.* at 188, 190.

application" that applied broadly to all personal data online.[93] The EJC held that the rules on international data transfers should not be applied "indiscriminately to the entire Internet."[94] Consequently, under the previous data protection regime, a U.S.-based publisher would have had a strong argument that the rules did not apply given the company's lack of physical presence in Europe.

C. Enforcing Right-to-be-Forgotten Requests Against Publishers

Assuming that a European court would conclude that a U.S.-based publisher's use of cookies brings it under the jurisdiction of the GDPR, it is unclear whether a court would go on to require the publisher to alter or delete its content under right to be forgotten requests. Until recently, right to be forgotten requests were generally directed at search engines such as Google.[95] However, two 2016 cases in Belgium[96] and Italy[97] 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.[98]

In *Google Spain v. Agencia Española de Protección de Datos,* the ECJ's landmark 2014 right to be forgotten case, the court held that the right to privacy outweighs the economic interests of a commercial entity, and, in some circumstances, may outweigh the public's interest in freely accessible information.[99] The case was brought by a Spanish lawyer whose personal information appeared in a 1998 newspaper auction notice indicating that he had defaulted on his social security debts.[100] In 2010, he requested that the newspaper remove his personal information from this article and that Google delist the article from its search results.[101] The Spanish DPA dismissed his complaint against the newspaper because the

93. *See* Case C-101/01, 2003 E.C.R. I-12971 ¶ 43 (citing Case C-376/98, Federal Republic of Germany v. European Parliament, 2000 E.C.R. I-2247).

94. Kuner, *supra* note 16, at 240.

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

96. Tomlinson, *supra* note 7.

97. *See* Matthews, *supra* note 8; Scorza, *supra* note 8.

98. Not all courts confronting the issue have agreed with the concept of applying the right to be forgotten to news publishers. *See* Emiel Jurjens, *Google Spain in the Netherlands III: Does Convicted Murderer Have 'Right To Be Forgotten,'* MEDIA REP. (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/; Kristof Van Quathem & Nicolas Rase, *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/.

99. *Google Spain SL*, 2014 EUR-Lex CELEX 62012CJ0131 ¶ 98.

100. *Id.* ¶¶ 14–15.

101. *Id.*

newspaper was legally required to publish the auction notice, but allowed his complaint against Google.[102] Google appealed this decision and the case was referred to the ECJ.[103] The ECJ held that the data subject's privacy interest must be weighed against the public's interest in the information; a balancing test that is highly dependent on the facts of a particular case.[104] The court considered factors such as the amount of time that had elapsed between the article's publication and present day, the petitioner's status as a nonpublic figure, and the significance of the article's content to the general public.[105] In this case, the court held that the petitioner's privacy interest outweighed the public's interest in the article and Google's economic interests.[106] As such, the court held that Google must remove links to the article in question.[107]

In recent years, European courts have gone beyond search engines, at times requiring newspapers to alter their content in right to be forgotten cases.[108] In April 2016, Belgium's High Court held that an individual's right to privacy may—and in this case, did—outweigh a newspaper's right to free expression.[109] In *Olivier G.*, the petitioner was a Belgian doctor who caused an accident while driving drunk in 1994, resulting in the death of two people.[110] The newspaper *Le Soir* included the petitioner's name in an article about the accident.[111] After *Le Soir* made its archives publicly available in 2008, this article appeared in Google searches of the petitioner's name.[112] He subsequently requested that the article be anonymized to remove any data that would have identified him.[113] In 2016, the Belgian Court of Cassation ruled that the petitioner's privacy interest was disproportionately damaged compared to the benefit received by the newspaper in respecting its right to free expression.[114] Like the ECJ in the *Google Spain* case, the court considered the length of time that elapsed between the event and the petitioner's request, and the fact that the

102. *Id.* ¶¶ 16–17.
103. *Id.* ¶¶ 18, 20.
104. *Google Spain SL*, 2014 EUR-Lex CELEX 62012CJ0131 ¶ 81.
105. *Id.* ¶¶ 93–97.
106. *Id.* ¶ 100(4).
107. *Id.*
108. *See* Tomlinson, *supra* note 7.
109. *Id.* (citing Cour de Cassation [Cass.] [Court of Cassation] Apr. 29, 2016, C.15.0052.F (Belg.)).
110. *Id.*
111. Tomlinson, *supra* note 7.
112. *Id.*
113. *Id.*
114. *Id.*

petitioner was not a public figure.[115] In an extraordinary order that would be constitutionally invalid under U.S. law, the court ordered the newspaper to replace the petitioner's name in the article with an "X."[116]

Shortly after the *Olivier G* decision, in June 2016, an Italian court held that the public's right to information expires "just like milk."[117] The facts of this case were quite similar to that of *Google Spain* and *Olivier G*: the petitioner wanted an article about a past transgression to be removed from a news outlet's website, largely because it would come up in a Google search of the petitioner or his business.[118] A key difference is that the petition was filed in 2010 for an article published in 2008.[119] Further, the news outlet, *Primadanoi*, had already complied with the petitioner's request six months after filing.[120] The court weighed the petitioner's right to privacy with the public's interest in accessing information and the newspaper's right to expression, and held that the latter expired after two years.[121] As such, the court fined *Primadanoi* € 10,000 for the six-month delay in taking down the article.[122]

Although the Belgian and Italian cases demonstrate that some European courts will find that an individual's right to privacy outweighs a publisher's right to free expression, this is not a universal trend. For example, in 2015 a Dutch court held that the right of expression could only be restricted in "exceptional cases," refusing a right to be forgotten petition against a victims' rights website.[123] In May 2016, the French Court of Cassation held that requiring a newspaper to remove content would impermissibly infringe upon freedom of press, even with regard to personal information under a right to be forgotten request.[124] However, as long as there are courts that are willing to require newspapers to alter their content in response to right to be forgotten petitions, and as long as the ECJ does not weigh in on this debate, the publisher could face such an order under the GDPR.

115. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 EUR-Lex CELEX 62012CJ0131, ¶ 81 (May 13, 2014); Tomlinson, *supra* note 7.

116. Tomlinson, *supra* note 7.

117. *See* Matthews, *supra* note 8 (citing Cass., 24 giugno 2016, n. 13161/16 (It.)).

118. Matthews, *supra* note 8.

119. *Id.*

120. *Id.*

121. *Id.*

122. Primadanoi was ordered to pay both €5,000 to both the petitioner and petitioner's business. *Id.*

123. Jurjens, *supra* note 98 (citing Rechtbank Noord-Nederland, Groningen, 1 mei 2015, ([redacted]/Vereniging Voor Veiligheid, Respect en Soldariteit) (Neth.)).

124. Quathem & Rase, *supra* note 98 (citing Cour de Cassation [Cass.] [Court of Cassation], May 12, 2016 [15-17729] (Fr.)).

There are several arguments based on EU privacy law that a U.S.-based publisher could make in response to a right to be forgotten case before a European court. First, it could argue that an order to alter the contents of a newspaper is not a proportional response to the petitioner's privacy concern. Proportionality is a cornerstone in EU law,[125] and has been invoked in every right to be forgotten case discussed above.[126] Given that the petitioner has the right to request that Google de-list the offending article under the *Google Spain* case, the publisher can argue that the individual's right to privacy is not significantly better off if the newspaper alters its content, whereas such an alteration would significantly impair the newspaper's right to expression. Indeed, the ECJ indicated that it might endorse this line of reasoning in its *Google Spain* opinion, saying: "[T]he consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same" when "carried out by the operator of a search engine" versus "the publisher of the web page."[127]

The publisher could also argue that the GDPR can only apply to the personal data of EU citizens that gave rise to the GDPR's jurisdiction in the first place. Article 3 of the GDPR says that the regulation "applies to the processing of personal data . . . where the processing activities are related to: . . . the monitoring of [EU data subject] behavior as far as their behavior takes place within the Union."[128] Construed narrowly, this would indicate that the GDPR applies *only* to the processing of personal data used to monitor EU data subjects—in other words, it only applies to the data gathered through the use of monitoring stratgies. If this is the case, then any enforcement actions under the GDPR could not extend to the *content* of the publisher's articles.

Another factor to consider is the practical likelihood that the publisher would face a court order to comply with a right to be forgotten request in the first place. The cases in which right to be forgotten orders have been enforced are similar in the sense that the allegedly offending article was published by a local newspaper reporting on a local crime.[129] Given that a U.S.-based publisher is unlikely to report on incidents such as drunk driving arrests in Europe, the likelihood that the publisher would

125. *See* Aurelien Portuese, *Principle of Proportionality as Principle of Economic Efficiency*, 19 EUROPEAN L.J. 612, 612–13 (2013).

126. *See, e.g.*, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 EUR-Lex CELEX 62012CJ0131 ¶ 63 (May 13, 2014).

127. *Id.* ¶ 86.

128. Council Regulation 2016/679, *supra* note 2, at 32–33.

129. *See Google Spain SL*, 2014 EUR-Lex CELEX 62012CJ0131 ¶ 14; Scorza, *supra* note 8; Tomlinson, *supra* note 7.

face a request that falls into this pattern is relatively slim.

That said, a publisher in these circumstances can look to Google's model for an example of how other companies are handling right to be forgotten requests. Google states that it is "required to weigh, on a case-by-case basis, an individual's right to be forgotten with the public's right to information," and that it wants to "strike this balance right."[130] Users can submit right to be forgotten requests on a dedicated web form, and must include information such as their name, country, and the search result they would like to delist.[131] They must also include a reason for removal, explaining how the page relates to the data subject, and why its content is "unlawful, inaccurate, or outdated."[132] After the *Google Spain* case, Google convened an Advisory Council on how it should accept, process, and execute right to be forgotten requests.[133] The council issued a report with its recommendations, suggesting that Google consider the "data subject's role in public life," the "nature of the information" on the offending page, the source of the content, and how much time has elapsed since the page was published.[134] The council also suggested that Google need only remove links from EU-specific Google pages—such as Google.de or Google.fr—and not elsewhere.[135] According to Google's transparency report, it has removed about forty-three percent of the URLs it reviewed under right to be forgotten requests.[136]

D. Distinguishing Extraterritorial Applications of U.S. Laws

It could be argued that arguments that the GDPR should not apply to U.S. publishers are inconsistent with the United States' own exercise of extraterritorial jurisdiction. In the privacy area, in particular, one might point out that the Federal Trade Commission (FTC) organic statute and the Children's Online Privacy Protection Act (COPPA) have been

130. Advisory Council, *How Should One Person's Right to Be Forgotten be Balanced With the Public's Right to Information*, GOOGLE, https://www.google.com/advisorycouncil/ (last visited Feb. 24, 2018) [hereinafter Google, Balancing Right to Be Forgotten].

131. *EU Privacy Removal*, GOOGLE, https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=0-636326164870136681-2178461795&rd=1 (last visited Feb. 24, 2018).

132. *Id.*

133. Google, Balancing Right to Be Forgotten, *supra* note 130.

134. GOOGLE ADVISORY COUNCIL, THE ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN 7–14 (2015), https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf.

135. *See id.* at 18–20.

136. *Transparency Report: Search Removals under European Privacy Law*, GOOGLE, https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en-US (last visited Feb. 24, 2018).

applied to behavior outside the United States.[137] Fortunately, the impact of these laws can likely be mitigated by distinguishing their limited extraterritorial applications from the broad authority asserted by the GDPR.

Section 5 of the FTC Act grants the agency the authority to prohibit "unfair or deceptive acts or practices in or affecting commerce," which includes privacy and data security violations.[138] In *Branch v. FTC*, the seminal case considering the extraterritorial application of the statute, the Seventh Circuit held that the FTC had the authority to issue an order against a U.S. company even though the affected consumers were located outside of the United States because the scheme was "conceived, initiated, concocted, and launched on its way in the United States."[139] Since *Branch*, courts have generally held that the FTC Act can be invoked to punish American companies for conduct affecting non-U.S. customers, including acts committed outside the United States.[140] While this line of cases could weaken the general argument that data protection laws should never be applied extraterritorially, the interpretation of the FTC Act by U.S. courts can be distinguished from the GDPR in several ways. The FTC Act applies to *domestic* companies for conduct affecting *foreign* customers, whereas the GDPR applies to the inverse situation: it covers *foreign* websites and service providers whose conduct affects *domestic* users.[141] This is an analytically distinct concept, and the publisher could make a persuasive argument that a regulator like the FTC should have greater discretion to police the conduct of its own companies when those acts affect customers abroad than when attempting to bring foreign companies under its purview.

Although Congress passed the U.S. SAFE Web Act in 2006, amending the FTC Act to explicitly "improve the [FTC's] . . . ability to provide more timely and effective international consumer protection," the changes do *not* appear to expand the territorial scope of Section 5 of the FTC Act.[142] Rather, the amendments focus squarely on clarifying the

137. *See* 15 U.S.C. § 6501(2)(A)(ii)(II) (2012).

138. 15 U.S.C. § 45(a)(1) (2012).

139. 141 F.2d 31, 34 (7th Cir. 1944).

140. *See, e.g.*, FTC v. SkyBiz.com, Inc., 57 F. App'x 374, 377 (10th Cir. 2003). Notably, however, the Eleventh Circuit has held that the FTC Act was not intended to apply extraterritorially. *See* Nieman v. Dryclean U.S.A. Franchise Co., 178 F.3d 1126, 1131 (11th Cir. 1999).

141. *Compare SkyBiz.com, Inc.*, 57 F. App'x at 377–78 (holding that the FTC Act could punish practices of defendants committed outside the United States), *with* Council Regulation 2016/679, *supra* note 2, at 5 (stating that the processing of data of subjects within the Union by a processor outside of the Union should be subject to the Regulation).

142. S. REP. NO. 109-219, at 2 (2006), *as reprinted in* 2006 U.S.C.C.A.N. 1806, 1806 (discussing the effect of the passage of the U.S. SAFE Web Act on Section 5 of the FTC Act).

FTC's authority to take action against American companies that engage in unfair or deceptive practices affecting foreign consumers.[143] Thus, while the new language did add an explicit reference to extraterritorial application in the text of the FTC Act,[144] it does not actually expand the agency's mandate and can still be distinguished on the grounds described in the previous paragraph.

On the other hand, COPPA applies to any website in the world that collects personal information from children in the United States, and especially to websites that are "directed to" children in the United States or "knowingly" collect information from them.[145] The FTC has the authority to levy penalties against websites and online service providers that violate COPPA, including foreign companies whose websites or services meet the definition described in the Act.[146] In this regard, COPPA's jurisdictional reach is more analogous to the GDPR than the FTC's general authority to enforce the FTC Act, since COPPA can be applied extraterritorially to companies owned and operated outside the United States if they are directed to or collect information from American children.[147] Nonetheless, COPPA is distinguishable on at least two grounds. First, it is a specialized law aimed at protecting children that applies only to a distinct subset of websites and online services,[148] and thus does not sweep up the wide range of foreign websites potentially covered by the GDPR's expansive jurisdictional test.[149] Second, the requirement that a website must

143. *See* U.S. SAFE Web Act of 2006, Pub. L. No. 109-455, sec. 3, 120 Stat. 3372, 3372 (codified at 15 U.S.C. § 45(a)(4) (2012)).

144. *See* 15 U.S.C. § 45(a)(4)(A) ("[U]nfair or deceptive acts or practices includes such acts or practices involving foreign commerce that—(i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States.").

145. 15 U.S.C. § 6502(a) (2012); *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (Mar. 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

146. 15 U.S.C. § 6505(a); *Complying with COPPA*, *supra* note 145.

147. *Compare* FTC v. SkyBiz.com, Inc., 57 F. App'x 374, 377–78 (10th Cir. 2003) (holding that the FTC Act could punish practices of defendants committed outside the United States), *and* Council Regulation 2016/679, *supra* note 2, at 5 (stating that the processing of data of subjects within the Union by a processor outside of the Union should be subject to the Regulation), *with Complying with COPPA*, *supra* note 145 ("Foreign-based websites and online services must comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the U.S.").

148. 15 U.S.C. § 6502(a); *see Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FED. TRADE COMM'N (July 2013), https://www.ftc.gov/tips advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compli ance. The FTC offers clear guidelines for companies to help determine whether they need to comply with COPPA, and most social networking and media companies do not have to worry about its requirements. *See id.*

149. Council Regulation 2016/679, 2016 O.J. (L 119) 26–27.

be directed to children or knowingly collect information from them appears to more closely resemble the narrower "purposeful targeting" test that some commentators advocated for during the GDPR consultations but was ultimately not adopted.[150]

V. 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. Any right to be forgotten order would very likely infringe upon the publisher's First Amendment rights, permitting the publisher to argue that it would be unconstitutional for a U.S. court to enforce it.

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 the press can only be restricted to "prevent grave and immediate danger to interests which the state may lawfully protect."[151] 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."[152]

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."[153] The remedy of requiring that an article be deleted or edited to ensure that it is "anonymized" would be extraordinary under the clear standard of *Miami Herald Publishing Co. v. Tornillo*, which struck down a state "right of reply" statute under the First Amendment because it constituted an "intrusion into the function of editors" and imposed "a penalty on the basis of the content."[154] Given the primacy of the First Amendment in American law, it is difficult to conceive that any order requiring a news publisher to alter its content or archived material on the basis of a judicial

150. *See, e.g.*, OMER TENE & CHRISTOPHER WOLF, FUTURE OF PRIVACY FORUM, OVEREXTENDED: JURISDICTION AND APPLICABLE LAW UNDER THE EU GENERAL DATA PROTECTION REGULATION 6 (2013), https://fpf.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf.

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

152. Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979).

153. Bartnicki v. Vopper, 532 U.S. 514, 534 (2001).

154. 418 U.S. 241, 244, 257–58 (1974).

or regulatory finding that it is no longer newsworthy would be construed as consistent with freedom of the press.[155]

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.[156] 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."[157]

The two tests for reasonableness, however, are not the same.[158] 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.[159] 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.[160]

Section 421 of the *Third Restatement of Foreign Relations Law* lays out the criteria for reasonableness in this area.[161] Once again, a foreign company's permanent physical presence in the state would likely qualify as reasonable grounds to assert jurisdiction.[162] 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.[163] Although a European regulator could attempt to assert jurisdiction based on the effects of that

155. Many commentators have noted as much. *See, e.g.*, Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech*, 18 COMM. L. & POL'Y 91, 98 (2013) (asserting that the right to be forgotten is "fundamentally at odds with theories of free speech"); 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.

156. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW, pt. IV, ch. 3, intro. note (AM. LAW INST. 1987).

157. *Id.* § 421 cmt. a.

158. *Id.*

159. *Id.*

160. *Id.*

161. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 421.

162. *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.

163. Kuner, *supra* note 16, at 235.

monitoring within the state,[164] 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[165]

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

Under the doctrine of comity, U.S. courts will generally grant extra-territorial effect to the valid judgments of foreign courts.[166] First, a U.S. court must be satisfied that the foreign court properly had jurisdiction over the matter at hand.[167] For reasons stated above in Section B, 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.[168] A foreign judgment 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.'"[169] 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."[170] This is a high standard that requires more than the mere fact that there are differences between foreign and domestic law.[171] Among the policy issues that are considered grounds for refusal to enforce foreign orders are those that implicate constitutional rights.[172]

164. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 421(2)(j) ("[A] state's exercise of jurisdiction . . . is reasonable if, at the time jurisdiction is asserted . . . 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[.]").

165. *Id.*

166. *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) (citing Gull v. Constam, 105 F. Supp. 107, 108 (D. Colo. 1952)).

167. *See* Ackermann v. Levine, 788 F.2d 830, 837 (2d Cir. 1986) (citing Fairchild, Arabatzis & Smith, Inc. v. Prometco Co., 470 F. Supp. 610, 615 (S.D.N.Y. 1979)).

168. Corporación Mexicana De Mantenimiento Integral v. Pemex-Exploración y Producción, 832 F.3d 92, 107 (2d Cir. 2016); *see* Hilton v. Guyot, 159 U.S. 113, 193 (1895) (quoting De Brimont v. Penniman, 7 F. Cas. 309, 311 (C.C.S.D.N.Y. 1873) (No. 3,715)); RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 117 cmt. c (AM. LAW INST. 1969).

169. *See Ackermann*, 788 F.2d at 841 (quoting Tahan v. Hodgson, 662 F.2d 862, 864 (D.C. Cir. 1981)).

170. *See Hilton*, 159 U.S. at 193 (quoting *De Brimont*, 7 F. Cas. at 311).

171. *See id.* at 194 (first quoting Elmendorf v. Taylor, 23 U.S. 152, 159–60 (1825)).

172. *See, e.g.*, de la Mata v. Am. Life Ins. Co., 771 F. Supp. 1375, 1384 (D. Del. 1991) (citing Koster v. Automark Indus., 640 F.2d 77, 79 (7th Cir. 1981)) (discussing the consideration of due process).

When a foreign judgment is one that would violate the First Amendment, courts have found that it violates public policy and is thus unenforceable.[173] 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.[174] 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 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.[175] 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.[176]

Although the SPEECH Act has rarely been invoked in the seven years since its passage,[177] it could apply here either directly or by analogy.

173. *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.").

174. *See id.* at 3–4 (citing Abdullah v. Sheridan Square Press, Inc., No. 93-CV-2515, 1994 WL 419847, at *1 (S.D.N.Y. May 4, 1994)) (mem.) ("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."); Bachchan v. India Abroad Publ'ns, Inc., 585 N.Y.S.2d 661, 664 (N.Y. Sup. Ct. 1992) ("[Denying summary judgment because] [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 US Constitution.").

175. *See* Securing the Protection of Our Enduring and Established Constitutional Heritage Act, Pub. L. No. 111-223, 124 Stat. 2381 (2010) (codified at 28 U.S.C. §§ 4101–05 (2012)); Ohno v. Yasuma, 723 F.3d 984, 1004 n.22 (9th Cir. 2013) (quoting S. REP. NO. 111-224, at 2 (2010)).

176. Securing the Protection of Our Enduring and Established Constitutional Heritage Act § 4012(a)(1)(A) (codified at 28 U.S.C. § 4102(a)(1)(A)).

177. *See generally* Securing the Protection of our Enduring and Established Constitutional Heritage Act; Citing references for 28 U.S.C. §§ 4101–05 (2012), LEXISNEXIS, https://advance.lexis.com/shepards/shepardspreview/ (search for 28 U.S.C. §§ 4101–05; for each statute, follow "Shepardize this document" hyperlink; follow "Citing Decisions" hyperlink) (cited 61 times since its enactment in 2010).

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.[178] And even if read narrowly to apply only to libel cases, the SPEECH Act and its legislative history[179] offer persuasive evidence that Congress intended to prevent U.S. courts from enforcing foreign laws that violate the First Amendment.[180]

CONCLUSION: PRACTICAL CONSEQUENCES AND POLICY CONSIDERATIONS

Based on the triggers for the applicability of the GDPR discussed above, U.S. publishers could consider specific measures to mitigate the risk that they may be found to be targeting EU audiences with digital advertising that might be claimed to be "monitoring the behaviour" of EU data subjects. In particular, publishers could consider the following strategies:

1. Avoid the use of languages other than English (and perhaps Spanish, which may be explained as being pointed toward Spanish-language-speaking U.S. users) in the content displayed by the website;
2. Not providing international dialing codes when providing U.S. telephone numbers for contact information;
3. Not delivering products to the EU or permitting registration by users known to reside in the EU (for example, eliminating any EU-country selection option on a drop-down menu for registration

178. Securing the Protection of Our Enduring and Established Constitutional Heritage Act sec. 2 ("The 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. Some 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.").

179. *See, e.g.*, S. REP. NO. 111-224, at 8 (2010) ("The 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.").

180. Dana Green, *The SPEECH Act Provides Protection Against Foreign Libel Judgments*, AM. BAR ASS'N, http://apps.americanbar.org/litigation/litigationnews/mobile/firstamendment-SPEECH.html (last visited Feb. 24, 2018) ("The act's symbolic significance, as an expression of the depth of Congressional commitment to free speech, should be heartening to free speech advocates.").

information); and

4. Not using the Euro or other EU currencies, such as Sterling, as currency for subscriptions and products sold.

Publishers could take additional steps to further distance themselves from the EU market. For example, they could insert a sentence clearly indicating that the website is not intended for EU users, as many U.S. publishers do today in their privacy policies. This language could read as follows: "Unless otherwise specified, the materials on this website are directed solely at those who access this website from the United States." Statements such as this provide some assistance in specifying the intended geographical scope of a website. Of course, such statements can only be useful if there is nothing on the website that undermines the statement.

Similarly, in terms of advertising displayed on the website, publishers could consider structuring their arrangements with advertising networks to limit their exposure. EU regulators have also focused on this point:

> The breadth of their [publishers'] responsibility, including the extent to which they become data controllers should be analysed on a case by case basis depending on the particular conditions of collaboration with ad network providers, as reflected in the service agreements. Accordingly, the service agreements between publishers and ad network providers should set up the roles and responsibilities of both parties in the light of their collaboration, as described in the agreement.[181]

Advertising networks often offer publisher choices in terms of the types of advertising that will be displayed, including the possibility to target markets geographically. Where possible, publishers could elect to geographically target their advertising to the U.S. market and only display advertising in English and for goods and services provided in the U.S. One step further, although less realistic in practice, might be for a U.S. publisher to consider contractually prohibiting advertising networks from using the personal information of potential EU users for segmentation purposes. For example, advertising networks could be required by contract to divert data obtained from EU IP addresses and to delete this information immediately. In practice, this is likely to be difficult to achieve both from a technical and business perspective, but strategies such as this one might be worth considering.

If these mitigation strategies are not successful, a U.S. publisher may still have a strong argument under international law that its operations

181. ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 39, at 11–12.

should not be subject to the terms of the GDPR. But 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[182]; freedom of the press, on the other hand, does not enjoy the same reverence it receives in the United States.[183] In a public opinion poll on personal data processing, eighty-nine 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.[184] Publicly 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

182. EU Charter art. 7, 2016 O.J. (C 202) 395.

183. *See* Adam Liptak, *When Free Worlds Collide*, N.Y. TIMES, Feb. 28, 2010, at 1, 4.

184. VERA JOUROVA, EUROPEAN COMM'N, DATA PROTECTION: FACTSHEET 4 (June 2015), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf (reciting data collected by the Commissioner for Justice, Consumers and Gender Equality).

working within Europe.