GDPR extraterritorial reach: Conflict with international law?

Do the principles of territoriality and nationality override the GDPR's territorial reach? **Kurt Wimmer** of Covington & Burling LLP analyses the issues at stake.

It has become commonplace for commentators and others to refer to the General Data Protection Regulation (GDPR) as a "global" law, or a "global" standard.[1] To be sure, the GDPR is having a significant impact on the privacy landscape around the world. And users around the world have had to deal with a hailstorm of new requests for consent and cookie banners based on widespread assumption of GDPR requirements even far outside the EU.

But no law passed by one country, or even a political and economic union as powerful as the EU, can be "global," regardless of ambition or breadth of terms. Even international treaties require countries to assent to their applicability.

The question of whether and to what extent a law can have extraterritorial effect is one that did not start with the GDPR and will not end with it. Over decades of global interpretation and scholarship, settled principles of public international law have been established to govern when it is appropriate for a law passed by one country to apply in the territory of another country that may have very different laws. These principles should be taken into account in determining whether it is, in fact, legal for European data protection authorities (DPAs) to enforce principles of the GDPR against companies with no presence in the EU.

This article analyzes those principles and concludes that companies with no EU presence may have colorable arguments against the jurisdiction of EU regulatory authorities and courts to enter orders against them.

The jurisdictional aspirations of the GDPR

The GDPR was developed with the goal of providing consistent privacy protections for individuals across the EU.[2] 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). The Directive provided that where parties not established in the EU use "equipment" in the EU to collect personal information, they are subject to the law.

The GDPR employs an entirely different approach to jurisdiction. 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 behavior as far as their behavior takes place within the Union."

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.

Offering goods or services: It is important to note that the recitals of the GDPR and long-standing European common law are extremely important in interpreting the terms of the GDPR. In terms of "goods or services" jurisdiction, 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."[3]

Accordingly, the mere accessibility from the EU of a non-EU company's website or the use of English on a US 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 a currency option, or by offering content in languages adapted to EU users.

This first criterion of targeting a service is clearly inspired by existing European case law. The key authority in this area is the *Pammer* case.[4] In this case, the Court of Justice of the EU (CJEU) was asked to clarify when an Internet service can be considered to target data subjects in a Member State. The CJEU held that mere accessibility of a website does not suffice. Similarly, the indication of the trader's address, email address or phone number (without international code) cannot be construed as targeting. To the contrary, the CJEU highlighted the following examples of activities that can demonstrate an intention to target:

- the express mentioning that the service is provided to users in a Member State;
- paying search engines to have its website favorably indexed in order to facilitate access by consumers in particular Member States;
- the international nature of the services;
- the provision of international telephone numbers;
- the use of Internet domain levels other than those of where the service provider is established (or general ones, such as .eu, or .com); and
- the mentioning of international clientele, and accounts written by such customers.

In the *Pammer* case, the service at issue, a travel package, was advertised on a third-party website. 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.

Monitoring behavior: 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 an important interpretative principle:

"In order to determine whether a processing activity can be considered to monitor the behavior 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 preferences, behaviors and attitudes."

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. The profiling required to trigger jurisdiction on this point is quite extensive. Longstanding online advertising strategies rely on data that does not contain contact or identifying information of "natural persons," but might rely on device identifiers, Internet Protocol (IP) addresses, cookies and other proxies for identifying a particular advertising subject on the Internet. One could reasonably 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.

International principles of jurisdiction and 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. These recognized bases for asserting jurisdiction include the territoriality principle, the nationality principle, the passive personality principle, and the protective principle.[5] 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[6] 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).[7]

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.

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.[8]

Reasonableness analysis in international jurisdiction

Under any of the preceding three theories, the party seeking to assert jurisdiction must prove why it is reasonable to exercise extraterritorial jurisdiction under any one of the bases described above.[9] The factors to be considered 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 responsible for the activity; (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 extent to which another state may have an interest in regulating the activity, and (6) the likelihood of conflict with regulation of another state.[10]

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 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. Comity dictates that states should generally avoid extraterritorial application of their laws against foreign citizens where those laws conflict.[11] 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.[12]

Practical consequences and policy considerations

Based on the triggers for the applicability of the GDPR discussed above, non-EU companies 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 behavior" of EU data subjects. In particular, companies may consider the following strategies:

- Avoiding the use of EU languages other than English in the content displayed by the website;
- Not providing international dialing codes when providing telephone numbers for contact information;
- 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 information); and
- Not using the Euro or other EU currencies as currency for products or services sold.

Companies may 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 non-EU companies do today in their privacy policies. Of course, such statements can only be useful if the website itself does not undermine the statement.

In making these multifaceted 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 public international law would be a useful complement to a clear-eyed look at the business realities of working within Europe.

REFERENCES

1 See, e.g. S. Greengard, Weighing the Impact of GDPR, *Communications of the ACM,* Vol. 61, p. 16 (November 2018), available at https://cacm.acm.org/magazines/2018/11/232192-weighing-the-impact-of-gdpr/fulltext.
2 See Council of the European Union, Draft Statement of the Council's Reasons 3 (Mar. 31, 2016).
3 GDPR, Recital 24.
4 *Peter Pammer v. Reederei Karl Schlüter GmbH & Co.*, KG (C-585/08) and *Hotel Alpenhof GesmbH v. Oliver Heller*, (C-144/09) (December 7, 2010), available at curia.europa.eu/juris/liste.jsf?language=en&num=C-585/08.
5 See Restatement (Third) of Foreign Relations Law § 402 (Am. Law Inst. 1987) [hereinafter Rest. (Third)].
6 *Id.* § 402(1)(a)-(b).
7 *Id.* § 402(2).
8 Rest. (Third) § 402(1)(c). See also *Hartford Fire Ins. Co. v. California*, 509 U.S. 764, 796 (1993).
9 Rest. (Third) § 403(1).
10 *Id.* § 403(2)(a)-(h).
11 See, e.g. *Hartford Fire Ins. v. California*, 509 U.S. 764 (1993).
12 Rest. (Third) § 403 cmt. e.

AUTHOR

Kurt Wimmer is Partner and U.S. Chair, Data Privacy and Cybersecurity Practice, Covington & Burling LLP, Washington D.C.

INFORMATION

A more extensive treatment is available at K. Wimmer, Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers?, 68 Syr. L. Rev. 547 (2018).

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Belgium: GDPR implementing Act enters into force

Laura Brodahl, **Laura De Boel** and **Cédric Burton** of Wilson Sonsini Goodrich & Rosati analyse the specifics of the law.

Following the adoption of the General Data Protection Regulation (GDPR) the Belgian legislator has adopted a new data protection law.

The Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (the 2018 Data Protection Act) repeals the Privacy Act of 8 December 1992 (the 1992 Privacy Act) and its implementing legislation. It entered into force on 5 September 2018.

The 2018 Data Protection Act is a massive piece of legislation. It

Continued on p.3

IAB revises its transparency and consent framework

As a result of feedback from DPAs and other stakeholders, a new version of this industry standard will be issued soon.

Laura Linkomies talked to IAB Europe in Brussels.

IAB (Interactive Advertising Bureau) Europe, the industry association for the digital advertising ecosystem in Europe, is working hard to make improvements to the "Transparency and Consent Framework" which was launched in April 2018 just in time for the GDPR. The voluntary framework is based on publishers and tech vendors using an open source standard to

Continued on p.4

Issue 157 **February 2019**

Separate Supplement
Tables of 132 laws and 28 bills

INTERNATIONAL report

ISSUE NO 157 **FEBRUARY 2019**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Laura Brodahl, Laura De Boel and Cédric Burton
Wilson Sonsini Goodrich & Rosati, Belgium

Kurt Wimmer
Covington & Burling LLP, US

Mark Sherwood-Edwards
This is DPO, UK

Hiroshi Miyashita
Chuo University, Japan

Katrine Evans
Hayman Lawyers, New Zealand

Emma Anderson
PL&B Correspondent

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

GDPR: The global benchmark

According to the EU Commission, during the peak month of May 2018, GDPR was searched more often on Google than American superstars Beyoncé and Kim Kardashian. On a more serious note, GDPR is undoubtedly having a global effect, as shown in Professor Graham Greenleaf's articles and global tables of privacy laws issued here as a supplement.

Numerous countries have updated their data protection laws since 2017, invariably strengthening them in ways which reflect some aspects of the GDPR, and there are currently 28 bills for new privacy laws (p.14 and p.19). However, our US correspondents observe that "no law passed by one country, or even a political and economic union as powerful as the EU, can be global, regardless of ambition or breadth of terms" (p.6).

The key word for 2019 is adequacy – the countries which have it, such as Argentina, are being reviewed. Japan's newly acquired adequacy status is being supplemented in the form of some amendments to existing legislation (p.12) and the EU-US Privacy Shield has been given another lease of life (p.18). As key voices from US industry now support a federal privacy law, the US Senate is to hold a hearing on a federal privacy law on 27 February.

Within the EU, the GDPR's effect is felt in a most concrete way. According to the EU there have been 41,500 breach notifications, 255 cross border cases, and 95,000 complaints*. The complaints mostly address telemarketing and promotional emails. For this issue, I interviewed FEDMA, the European umbrella organisation for direct marketers, about its concerns over the proposed EU e-Privacy Regulation (p.9) and IAB, the Interactive Advertising Bureau, about its Transparency & Consent Framework for GDPR compliance (p.1).

This issue introduces the new Belgian DP law (p.1). We aim to publish a report on each EU country's new GDPR adaptation law – if you would like to analyse your country's law please get in touch. An overview of GDPR implementation and the remaining issues will be provided at our 32nd Annual International Conference in Cambridge, 1-3 July 2019. See the 45 confirmed speakers and their sessions from 16 jurisdictions at www.privacylaws.com/ac

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

*EU statistics issued 28 January ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 125+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 125+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**"

Subscription Fees

Single User Access

International Reports **£560 + VAT***
UK Reports **£450 + VAT***
UK & International Reports **£900 + VAT***
* VAT only applies to UK based subscribers

Multi User Access

Discounts for Multiple User licence (up to 10) and Enterprise licence (unlimited users).

Subscription Discounts

Introductory discount (first year): 30% off for DPAs, public sector, charities, academic institutions, use code SUB30; 20% off for other organisations, use code SUB20.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £25, Outside Europe = £35

Combined International and UK Editions
Rest of Europe = £50, Outside Europe = £70

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK