AN A.S. PRATT PUBLICATION
APRIL 2021
VOL. 7 • NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 3** **April 2021**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [69] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Further Tension Between National Security and Protecting Privacy: Latest EU Judgments

By Natasha G. Kohne, Michelle A. Reed, Jenny Arlington, Rachel Claire Kurzweil, Jay Jamooji, and Sahar Abas*

The Court of Justice of the European Union has ruled on whether United Kingdom, French, and Belgian national security laws were compatible with European Union privacy, data protection, and fundamental rights principles. This article explains the decisions and their implications.

United Kingdom, French, and Belgian national security laws (and such laws of other European Union ("EU") Member States) fell under the scrutiny of the Court of Justice of the European Union ("CJEU"), which on October 6, 2020, ruled on whether such laws were compatible with EU privacy, data protection, and fundamental rights principles. The take-away point is that the CJEU confirmed that certain national security laws were incompatible with Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (the "ePrivacy Directive"),[1] which together with the General Data Protection Regulation ("GDPR") provides the main pillars of the framework of EU data protection and privacy laws. This raises complex questions as to what steps EU Member States would need to take to resolve the tension between national security and protection of privacy.

Further, the United Kingdom ("U.K.") officially left the EU at the end of the transition period in December 2020, and negotiations are ongoing in relation to granting the U.K. an "adequacy" status, which would ensure seamless flows of personal data between the U.K. and the EU. Against that background, the fall-out from the rulings would be of particular importance to international businesses.

* Natasha G. Kohne (nkohne@akingump.com) and Michelle A. Reed (mreed@akingump.com) are partners at Akin Gump Strauss Hauer & Feld LLP and co-head the firm's cybersecurity, privacy, and data protection practice. Jenny Arlington (jarlington@akingump.com) is a counsel at the firm. Rachel Claire Kurzweil (rkurzweil@akingump.com), Jay Jamooji (jay.jamooji@akingump.com), and Sahar Abas (sahar.abas@akingump.com) are associates at the firm.

[1] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.

CONCERNS SO FAR ABOUT THE USE OF BULK COMMUNICATIONS DATA

The CJEU handed down two connected judgments, in *Privacy International v. United Kingdom*[2] and in *La Quadrature du Net & Others v. France*,[3] *Ordre des barreaux francophones and germanophone & Others v. Belgium*.[4] The CJEU examined the lawfulness of Member State legislation which required providers of electronic communication services to forward users' traffic and location data to public authorities or to retain such data in a general or indiscriminate manner.

National surveillance laws in the U.K., France, and in other EU jurisdictions oblige electronic communications service providers ("ECSP") to retain, in certain circumstances, a large amount of personal data for later use or collection by security and intelligence agencies. In recent years, the CJEU examined various aspects of such retention,[5] and appeared to suggest that EU Member States were not allowed to require that ECSP retain traffic and location data in a general, indiscriminate manner. Some Member States became concerned that the CJEU rulings might be read to deprive national authorities of the ability to safeguard national security and combat crime.

Against that background, Privacy International, La Quadrature du Net and other organizations commenced various proceedings in a number of EU Member States, challenging the legality of member states legislation authorizing the acquisition and use of bulk communications data by the security and intelligence agencies.

Privacy International v. U.K.

In 2015, Privacy International, a non-governmental organization, brought proceedings in the U.K. against the Security Service ("MI5"), the Secret Intelligence Service ("MI6"), the Government Communications Headquarters ("GCHQ"), the Secretary of State for Foreign and Commonwealth Affairs, and the Secretary of State for the Home Department, on the basis mentioned above.

As it transpired, the security and intelligence agencies had been acquiring and using sets of bulk personal data, such as biographical data, travel data, financial or commercial information, and communications data liable to include sensitive data covered by professional secrecy. Such data had been obtained by various, possibly secret, means, and analyzed by cross-checking and automated processing; the data could also

---

[2] C-623/17, http://curia.europa.eu/juris/document/document.jsf;jsessionid=09E52135406894B23D43DC9A7258380B?text=&docid=232083&pageIndex=0&doclang=EN&mode=req&dir=&occ= first&part=1&cid=6419040.

[3] Joined Cases C-511/18 and C-512/18, http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=6419123.

[4] C-520/18, http://curia.europa.eu/juris/documents.jsf?num=C-520/18.

[5] *See, for example*, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15) and *Ministerio Fiscal* (C-207/16).

further be disclosed to other agencies and foreign partners. The acquisition of the data was in compliance with U.K. legislation, however, that legislation obliged ECSP to forward traffic and location data to security and intelligence agencies for the purposes of safeguarding national security.

Two questions were "referred for a preliminary ruling" to the CJEU (a special procedure as regards the interpretation of EU law) and they concerned whether the relevant U.K. legislation was in compliance with EU law.

First, the CJEU addressed the question of whether the U.K. legislation fell within the material scope of the ePrivacy Directive. The U.K., as well as a number of other governments supporting its position (including France, Ireland, Sweden, and Poland), argued that the ePrivacy Directive should not apply. The argument put forward by the U.K. government was that the purpose of the U.K. legislation was to safeguard national security.

It was submitted that the activities of the security and intelligence agencies were essential state functions relating to the maintenance of law and order and the safeguarding of national security; and, under the relevant EU law provisions, those functions were the sole responsibility of Member States (and not the EU). The CJEU found that the U.K. legislation (and, by extension, similar laws in other EU Member States) fell within the scope of the ePrivacy Directive. Therefore, the U.K. legislation had to comply with the various requirements set out in the ePrivacy Directive.

Second, as regards what those requirements under the ePrivacy Directive were, the CJEU essentially stated that the U.K. legislation was incompatible with EU law (which takes precedence). The CJEU explained that Article 15(1) of the ePrivacy Directive, when read in light of the EU Charter of Fundamental Rights (the "Charter") and other EU law provisions, precluded Member State legislation which would require that ECSP carry out general, indiscriminate transmission of traffic and location data to security and intelligence agencies (even if for the purposes of safeguarding national security). The CJEU stressed that restrictions on privacy rights must be proportionate and only apply so far as was "strictly necessary"; the U.K. legislation exceeded the limits of what was strictly necessary and could not be considered to be justified within a democratic society.

Of particular concern for the CJEU was the fact that the transmission of data was carried out in a general and indiscriminate way. This was considered disproportionate because it affected all persons using ECSP, including those for whom there was no evidence to suggest their conduct might have a link, even indirectly or remotely, with the objective of safeguarding national security. The CJEU emphasized that the ePrivacy Directive enshrined the principle of confidentiality of electronic communications/related traffic data, essentially preventing persons other than users from storing those communications and data without the users' consent. Users of electronic communications services were entitled to expect, according to the CJEU, that their communications/data would remain anonymous and not recorded, unless they had agreed otherwise.

La Quadrature du Net & Others v. France; Ordre des barreaux francophones and germanophone & Others v. Belgium

The cases against the governments of France and Belgium raised similar issues to the case against the U.K., namely the extent to which EU law applied and, if it was applicable, the nature of safeguards required to govern data retention and access regimes. In line with the CJEU's reasoning above, the CJEU found that the ePrivacy Directive prohibited legislative measures obliging ECSP to carry out the general and indiscriminate retention of traffic and location data as a purely preventative measure.

According to the CJEU, the requirement to forward and retain such data in a general, indiscriminate manner constituted serious interferences with the fundamental rights guaranteed by the Charter. This was especially so where there was no link between the conduct of the data subjects concerned and the objective pursued by the relevant legislation. The CJEU further found that the provisions of the GDPR (in particular Article 23(1)) also allowed only "necessary and proportionate" restrictions on privacy rights.

Nevertheless, the CJEU recognized that EU Member States might face serious threats to national security that proved to be genuine, present or foreseeable. Provided that certain conditions are met, the ePrivacy Directive allows an order requiring ECSP to retain traffic and location data (including IP addresses), generally and indiscriminately, or to conduct automated analysis of such data.

Any such order must, however, be (a) limited in time to ensure it is "strictly necessary," (b) on the basis of objective, non-discriminatory factors, such as a geographic criterion, and (c) subject to effective review by a court or an independent administrative body. For example, real-time collection of traffic and location data would be permitted where such collection was limited to persons in respect of whom there was a valid reason to suspect they were involved in terrorist activities and where the underlying legislative measures were subject to prior review by a court or independent administrative body.

IMPLICATIONS OF THE CJEU JUDGMENTS

Although, in general, EU Member States have sole responsibility to protect their national security, the CJEU ruled that certain national security laws concerning data access and retention have to be aligned with EU privacy and fundamental rights laws and principles. In addition, the CJEU ruled that legislation currently in force in (at least) the U.K., France, and Belgium are incompatible with the ePrivacy Directive.

The next step in the process is for EU Member State courts and tribunals to consider what action they would need to take, in light of the CJEU judgment, in the proceedings that Privacy International and La Quadrature du Net (and others) commenced at the national level.

The steps the U.K. takes in particular will be watched closely by stakeholders. Obtaining an "adequacy" decision from the EU Commission post-Brexit, i.e., a decision declaring that the U.K. has adequate data protection laws, would mean data flows between the EU and the U.K. can continue seamlessly. It is likely that the EU Commission would take into consideration the latest CJEU judgment when analyzing whether "adequacy" may ultimately be granted. Indeed, the EU Commission expressly referred to the latest CJEU judgment in the draft adequacy decision published on February 19, 2021.