AN A.S. PRATT PUBLICATION
APRIL 2019
VOL. 5 • NO. 3

# PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

# Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 | NUMBER 3 | APRIL 2019



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*, [5] 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

(2019–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.

# Accessing Personal Data in European Criminal Investigations

***Steven G. Stransky****

*The Court of Justice of the European Union recently addressed law enforcement's ability to access personal data held by telecommunications service providers to assist in a criminal investigation. The author of this article discusses the case, which will undoubtedly influence EU Member States as they seek to modernize their own internal security and surveillance laws and regulations to address evolving technology and trends.*

Recently, European data privacy issues have centered on the development and implementation of the General Data Protection Regulation ("GDPR"), which became effective in May 2018.[1] In light of its global impact and the concerns over its future regulatory enforcement, the focus on the GDPR is justified. Yet, although the Court of Justice of the European Union ("CJEU") may not garner as much attention as the GDPR, its decisions will continue to have a significant role in defining individual data privacy rights. The CJEU's judgment in *Ministerio Fiscal* is a case in point.[2]

In *Ministerio Fiscal*, the CJEU addressed law enforcement's ability to access personal data held by telecommunications service providers to assist in a criminal investigation. This case will undoubtedly influence EU Member States as they seek to modernize their own internal security and surveillance laws and regulations to address evolving technology and trends.

## FACTS AND PRELIMINARY HISTORY

The facts[3] underlying the *Ministerio Fiscal* decision are relatively straightforward and center around an all-too-common experience: a stolen cell phone. On February 16, 2015, Hernández Sierra (a citizen of Spain) was the victim of a violent robbery during which his wallet and cell phone were stolen. In response, Sierra filed a complaint with his local police department. On February 27, 2015, police officials requested a judicial order compelling various telecommunications service providers to disclose the

* Steven G. Stransky is senior counsel in Thompson Hine's Business Litigation, Privacy & Cybersecurity, and Government Contracts groups, advising clients on national and international privacy and information security issues. He may be reached at steve.stransky@thompsonhine.com.

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

[2] C-207/16 (Oct. 2, 2018, ECLI:EU:C:2018:788).

[3] Unless otherwise noted, all the background and facts of this case are derived from *Ministerio Fiscal*, at para. 19-26.

following information: (1) all recently activated telephone numbers that were linked to the International Mobile Equipment Identity ("IMEI") code of Sierra's cellphone,[4] and (2) the identity and corresponding personal data (e.g., names, addresses) of the owners or users of the telephone numbers corresponding to any subscriber identity module ("SIM card")[5] activated with this IMEI code.

On May 5, 2015, a magistrate refused the request because it did not satisfy the criteria set forth in Spain's domestic law and criminal code. More specifically, the magistrate held that local Spanish law only authorized the disclosure of this type of data to law enforcement officials when the criminal matter subject to investigation involved a "serious offense," which was interpreted as an offense punishable by imprisonment for a term of five years or more.[6]

## LAW AND ANALYSIS

One of the primary issues presented in *Ministerio Fiscal* was whether law enforcement's access to personal data to investigate a minor crime infringes upon an individual's fundamental rights.[7] In resolving this issue, the CJEU focused on the scope and meaning of the ePrivacy Directive,[8] which governs the processing of personal data in the electronic communications sector. Article 5 of the ePrivacy Directive mandates the confidentiality of communications and of its related traffic data,[9] including while such data is stored by a telecommunications service provider. Article 6 places similar restrictions on the collection, use, and retention of traffic data.

---

[4] An IMEI code is a unique number assigned to a certain cell phone that identifies the phone model and serial number. *PC Magazine,* Encyclopedia, *available at* www.pcmag.com/encyclopedia.

[5] A cell phone's SIM card contains a unique identification number, authentication codes, network-specific data, and telephone contact and other information. *Id.*

[6] After the magistrate's ruling, the Spanish legislature amended its criminal code and established two alternative criteria for determining the degree of seriousness of a criminal offense.

[7] The CJEU analyzed a separate issue and found that it had the authority to address matters arising under certain EU laws that concern Member States' legislation in the area of criminal investigations and public security. *Ministerio Fiscal*, at para. 29-43.

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ 2002 L 201), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337) (ePrivacy Directive). The CJEU also analyzed Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, 2010 O.J. C 83/02, which dictate that everyone has the right "to respect for his or her private and family life, home and communications," and "to the protection of personal data concerning him or her," respectively. The CJEU found that law enforcement's access to the personal data in question would constitute an interference with both of these rights. *Ministerio Fiscal*, at para. 48.

[9] The term "traffic data" is defined as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof." ePrivacy Directive, at Article 2.

However, the ePrivacy Directive provides that EU Member States may adopt legislative measures to restrict the scope of the rights and obligations set forth in Articles 5 and 6, "when such restriction constitutes a *necessary*, *appropriate and proportionate measure* . . . to safeguard national security (i.e., State security), defense, public security, and *the prevention, investigation, detection and prosecution of criminal offenses*. . . ."[10] In analyzing this text, the CJEU held that "the objective of preventing, investigating, detecting and prosecuting criminal offenses," is not limited "to the fight against serious crime alone, but refers to 'criminal offenses' generally."[11] Thus, if law enforcement's access to personal data was "necessary, appropriate and proportionate," it could be authorized for the purpose of investigating a minor criminal offense.

In analyzing the "necessary, appropriate and proportional" principle, the CJEU reiterated its previous holding that EU Member States could permit legislation governing access to the content of communications and related data only if such access is proportionate to the seriousness in which an individual's fundamental rights are impacted.[12] More specifically, the "serious interference" with one's fundamental rights can only be justified if the crime being investigated is also considered "serious." According to the CJEU, "only the objective of fighting *serious crime* is capable of justifying public authorities' access to personal data retained by providers of electronic communications services which, taken as a whole, *allow precise conclusions* to be drawn concerning the private lives of the persons whose data is concerned."[13] On the other hand, "when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offenses' generally."[14]

Based on the foregoing, the CJEU found that accessing the personal data in question was not serious. It reiterated that the request by Spanish law enforcement to the local magistrate was part of an ongoing criminal investigation and sought "to identify the owners of SIM cards activated over a period of 12 days with the IMEI code of the stolen mobile telephone."[15] Moreover, "that request seeks access to only the telephone numbers corresponding to those SIM cards and to the data relating to the identity of the owners of those cards."[16] According to the CJEU, the data in question does not involve the communications content and its disclosure could not be used to identify the "date, time, duration and recipients of the communications . . . nor the locations

[10] *Id.* at Article 15 (emphasis added).
[11] *Ministerio Fiscal*, at para. 53.
[12] *Id.* at 54.
[13] *Id.* at 54 (emphasis added).
[14] *Id.* at 57.
[15] *Id.* at 59.
[16] *Id.*

where those communications took place or the frequency of those communications with specific people during a given period."[17]

The CJEU held that the disclosure of this information does not "allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned," and therefore the access to the data cannot be considered a "serious" interference with any party's fundamental rights.[18] Therefore, because the disclosure of this type of personal data does not seriously infringe upon one's fundamental rights, its access does not have to be limited in the area of enforcing minor criminal offenses.[19]

## CONCLUSION

The CJEU's decision in *Ministerio Fiscal* allows law enforcement to access innocuous personal data retained by a telecommunications service provider as part of its investigation into routine and minor criminal matters. However, EU Member States still retain the discretion on whether to permit access to this type of data by law enforcement in accordance with the derogation principles set forth in Article 15 of the ePrivacy Directive.[20] Because access to such personal data is authorized, but not mandated, by EU Member States, it will be subject to debates and actions within local EU legislatures and parliaments. As seen in other contexts, the sensitivity of the personal data in question will likely evolve with the development of new technology and, with it, the corresponding privacy debate.

---

[17] *Id.* at 60.

[18] *Id.* at 61. The previous decision by the Advocate General addressed other reasons why accessing the data in question would not violate EU law. "The potentially harmful effects," according to the Advocate General, "are both slight and circumscribed" because the data sought is "intended to be used in the sole context of a measure of investigation," and is "not intended to be disclosed to the public at large." *Ministerio Fiscal*, C-207/16, at para. 37 (May 3, 2018, ECLI:EU:C:2018:300). Moreover, the risk of harm to the individuals whose data is accessed is limited in light of the fact that the police's access to the data "is accompanied by procedural guarantees under Spanish law, since it is subject to review by a court." *Id.*

[19] *Ministerio Fiscal*, at para. 63.

[20] Although it is anticipated that the ePrivacy Directive will soon be replaced by the ePrivacy Regulation, the most recent draft of the latter has an exception similar to the one set forth in Article 15 of the current ePrivacy Directive.