AN A.S. PRATT PUBLICATION
MAY 2017
VOL. 3 • NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 4 | MAY 2017

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) 487-3000
Fax Number .... (518) 487-3584
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 ..... (518) 487-3000

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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [129] (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

(2017–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, 718.224.2258. 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.

Evolution in International Cybersecurity and Data Privacy Governance

By Gabriela Kennedy, Kendall C. Burman, Xiaoyan Zhang, and Lei Shen*

The authors of this article discuss international cybersecurity and data privacy developments including major changes in the European Union (the forthcoming General Data Protection Regulation and Brexit); evolving restrictions on international data transfers; and new data localization laws in China and Russia.

Cybersecurity and data privacy have been topics of focus around the world, and several significant recent developments in this realm will affect multinational businesses in 2017. Among these developments are: major changes in the European Union, including the forthcoming General Data Protection Regulation and Brexit; evolving restrictions on international data transfers; and new data localization laws in China and Russia.

GENERAL DATA PROTECTION REGULATION

In 2016, the European Parliament approved the new General Data Protection Regulation ("GDPR"), which will come into force on May 25, 2018. The GDPR is intended to update and make data protection law more consistent across the European Union member states. The GDPR will apply to data controllers and processors across all sectors, and even organizations established outside the European Union will have to comply if they are offering goods or services or monitoring individuals inside the European Union. Non-EU companies will need to consider whether their activities are covered by the GDPR and whether they must appoint an EU representative to monitor compliance with numerous new requirements, including breach notification, impact assessments and "the right to be forgotten."

BREXIT

Many companies are concerned about the impact of Brexit on data protection and cybersecurity in the United Kingdom. The procedural details and timing of the UK's departure from the EU are still under consideration, and there are several possible outcomes, creating substantial uncertainty. In particular, while the UK government has confirmed that the UK will apply the GDPR coming into force in May 2018,

* Gabriela Kennedy (gabriela.kennedy@mayerbrownjsm.com) is a partner of Mayer Brown JSM, head of the Asia IP and TMT group, and co-leader of the firm's global Intellectual Property practice. Kendall C. Burman (kburman@mayerbrown.com) is a Cybersecurity & Data Privacy counsel at Mayer Brown. Xiaoyan Zhang (xiaoyan.zhang@mayerbrownjsm.com) is a counsel of Mayer Brown JSM's IP & TMT group. Lei Shen (lshen@mayerbrown.com) is a senior associate in Mayer Brown's Cybersecurity & Data Privacy and Technology Transactions practices.

many questions have been raised about what impact Brexit will have on UK businesses' ability to transfer data to and from businesses and other entities within the EU.

DATA TRANSFERS

The topic of international data transfers attracted significant attention in 2016, starting with the European Commission and the U.S. Department of Commerce signing the EU-U.S. Privacy Shield agreement, a much-anticipated framework for protecting personal data transferred from the EU to the United States. After the invalidation of the Safe Harbor framework in 2015, companies in the United States are now able to self-certify with the Commerce Department, attesting to their compliance with the Privacy Shield's principles, to enable data transfers from the EU. Privacy Shield-certified companies will need to ensure that their existing contracts with any third parties to which they further transfer EU data comply with the Privacy Shield's onward transfer requirements.

It is important to note, however, that the future of the Privacy Shield agreement is uncertain. The agreement has already been challenged in the European Court of Justice under the same legal claim that led to the Safe Harbor framework's invalidation. More recently, questions have been raised about the U.S. commitment to the Privacy Shield agreement in a Trump administration.

For example, although intended to be "consistent with applicable law," the recent Executive Order on Enhancing Public Safety in the Interior of the United States has raised questions about privacy rights guaranteed by the Privacy Shield and the Judicial Redress Act. Companies that have certified or are considering the process should carefully track developments in this dynamic space.

Data transfer developments were not limited to Europe. For example, new rules on data transfers issued by Argentina's Data Protection Authority addressed two forms of model clauses to be used for cross-border data transfers—one for transfers to a data controller and another for transfers to a data processor. Argentina's new rules also provide a list of countries that, in the authority's view, offer an adequate level of data protection.

DATA LOCALIZATION RULES

Rules requiring data to remain within their country's jurisdiction will merit close scrutiny by companies doing business in China and Russia in 2017.

- China's comprehensive Cybersecurity Law ("CSL") was passed in 2016 and will come into force in June 2017. The nation's first comprehensive cybersecurity regulation, it applies to network operators and operators of critical information infrastructures ("CIIs"), with heightened requirements, such as data localization

and restrictions on cross-border data transfers, being imposed on the latter. Operators of CIIs are required to store within China "citizens' personal information and important data" gathered and produced while carrying out their operations, with exceptions subject to performance of a "security assessment." As of the date of writing, neither the exact scope of the CIIs nor the security assessment is known. Penalties for non-compliance include fines and the revocation of the business's license.

- Russia has been conducting inspections to verify compliance with its data localization law, which requires that Russian personal data be stored in data centers located within Russia, subject to exceptions. A court blocked online access in Russia to LinkedIn in November 2016, for example, for violation of the law.

CONCLUSION

Regulators, policymakers, litigants and contracting parties continue to pay close attention to businesses' cybersecurity and data privacy practices. The constant stream of significant developments in these fields requires companies to respond nimbly and strategically. 2017 is poised to deliver yet more cybersecurity and data privacy challenges for businesses, including as the Trump administration pursues its priorities at the federal level.

Developing effective, multidisciplinary responses based on a clear understanding of assessed risks and expertise across the enterprise will be crucial to managing those risks in the year ahead.