AN A.S. PRATT PUBLICATION
MAY 2016
VOL. 2 • NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

EDITOR'S NOTE: CAN YOU KEEP A (TRADE) SECRET?
Victoria Prussen Spears

CRITICAL ISSUES FOR FOREIGN DEFENDANTS IN INTERNATIONAL TRADE SECRETS LITIGATION – PART I
Jeffrey A. Pade

DEPARTMENT OF DEFENSE REVISES LANDMARK CYBERSECURITY RULE, EXTENDS DEADLINE FOR SOME COMPLIANCE REQUIREMENTS
Benjamin A. Powell, Barry J. Hurewitz, Jonathan G. Cedarbaum, Jason C. Chipman, and Leah Schloss

CREDIT CARD DATA BREACHES: PROTECTING YOUR COMPANY FROM THE HIDDEN SURPRISES – PART I
David A. Zetoony and Courtney K. Stout

FDIC EMPHASIZES CORPORATE LEADERSHIP TO ADDRESS THE KEY RISK MANAGEMENT ISSUES RAISED BY CYBERSECURITY AND MARKETPLACE LENDING
Scott R. Fryzel and Lindsay S. Henry

EUROPEAN COMMISSION PRESENTS EU-U.S. PRIVACY SHIELD
Aaron P. Simpson

Pratt's Privacy & Cybersecurity Law Report

VOLUME 2 | NUMBER 4 | MAY 2016

Editor's Note: Can You Keep a (Trade) Secret?
Victoria Prussen Spears 119

Critical Issues for Foreign Defendants in International Trade Secrets Litigation – Part I
Jeffrey A. Pade 121

Department of Defense Revises Landmark Cybersecurity Rule, Extends Deadline for Some Compliance Requirements
Benjamin A. Powell, Barry J. Hurewitz, Jonathan G. Cedarbaum, Jason C. Chipman, and Leah Schloss 131

Credit Card Data Breaches: Protecting Your Company from the Hidden Surprises – Part I
David A. Zetoony and Courtney K. Stout 138

FDIC Emphasizes Corporate Leadership to Address the Key Risk Management Issues Raised by Cybersecurity and Marketplace Lending
Scott R. Fryzel and Lindsay S. Henry 144

European Commission Presents EU-U.S. Privacy Shield
Aaron P. Simpson 147

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 [121] (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

(2016–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.

European Commission Presents EU-U.S. Privacy Shield

By Aaron P. Simpson*

In this article, the author explains the EU-U.S. Privacy Shield framework and discusses next steps.

The European Commission recently issued the legal texts that will implement the EU-U.S. Privacy Shield. These texts include a draft adequacy decision[1] from the European Commission, Frequently Asked Questions[2] and a Communication[3] summarizing the steps that have been taken in the last few years to restore trust in transatlantic data flows.

The agreement in support of the new EU-U.S. transatlantic data transfer framework, known as the EU-U.S. Privacy Shield, was reached on February 2, 2016, between the U.S. Department of Commerce and the European Commission. Once adopted, the adequacy decision will establish that the safeguards provided when transferring personal data pursuant to the new EU-U.S. Privacy Shield are equivalent to the EU data protection standards. In addition, the European Commission has stated that the new framework reflects the requirements that were set forth by the Court of Justice of the European Union (the "CJEU") in the recent *Schrems*[4] decision.

THE EU-U.S. PRIVACY SHIELD

The new framework provides a response to the concerns that have been raised by the European Commission and the CJEU with respect to transatlantic data transfers. It contains stronger commitments that must be undertaken by companies in the commercial sector, but also significant commitments with respect to the U.S. government's access to personal data. The four most important aspects of the Privacy Shield are:

1) Enhanced Obligations on Companies and Robust Enforcement

Companies that are willing to transfer personal data from the EU to the U.S. must accept more stringent obligations regarding the processing of personal data and how

---

* Aaron P. Simpson, a partner at Hunton & Williams LLP and a member of the Board of Editors of *Pratt's Privacy & Cybersecurity Law Report*, advises clients on a range of privacy and cybersecurity matters, including state, federal, and international privacy and data security requirements as well as the remediation of large-scale data security incidents. He may be contacted at asimpson@hunton.com.

[1] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

[2] http://europa.eu/rapid/press-release_MEMO-16-434_en.htm.

[3] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.

[4] http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=84927.

individuals' rights are guaranteed. Among other limitations introduced by the new framework, onward data transfers will be subject to more onerous requirements and liability provisions.

In addition, the Privacy Shield will include stricter oversight mechanisms to help ensure companies abide by their commitments, including regular monitoring by the U.S. Department of Commerce. In addition, companies will face severe sanctions or exclusion from the framework if they fail to comply.

2) Limits and Safeguards Regarding Access to Personal Data by the U.S. Government

The European Commission has obtained written assurances from the U.S. government (*i.e.*, the Department of Justice and the Office of the Director of National Intelligence) that access to personal data by government authorities for law enforcement, national security and other public interest purposes will be subject to clear limitations, safeguards and oversight mechanisms.

3) Effective Protection of EU Citizens' Privacy Rights and Redress Possibilities

Several affordable mechanisms to obtain individual redress will be available to data subjects who think their personal data has been misused under the new framework, whether via a direct complaint to the company or to their national data protection authority ("DPA"). Complaints made to a DPA will be referred to the U.S. Department of Commerce and the Federal Trade Commission for investigation. When receiving a complaint directly from individuals, companies must reply within 45 days. Companies handling personal data in the Human Resources context about European individuals must comply with the decisions of the competent DPA. In addition, companies also must designate an independent dispute resolution body to investigate and resolve individuals' complaints and provide complimentary recourse to the individuals.

Further, in the context of a company's certification, the Department of Commerce will verify that the company complies with the Privacy Principles of the Privacy Shield, and that it has designated an independent recourse mechanism. As a last resort, individuals will be able to bring their complaints to a newly-created Privacy Shield Panel, a dispute resolution body that can take binding and enforceable action against U.S. companies that have certified their adherence to the Privacy Shield.

EU citizens also will have a redress mechanism in the national security context. In particular, an independent Ombudsperson will be responsible for handling complaints and inquiries received from EU individuals regarding access to their data by national intelligence authorities. This redress mechanism will be extended beyond the EU-U.S. Privacy Shield and will be available to individuals for all data transfers to the U.S. for commercial purposes.

4) Annual Joint Review Mechanism

The European Commission will annually monitor the functionality of all aspects of the EU-U.S. Privacy Shield, together with the U.S. Department of Commerce, EU DPAs, U.S. national security authorities and the Ombudsperson. Other sources of information, such as voluntary transparency reports, will also be used for monitoring the functionality of the framework. In the event that companies or public authorities do not comply with their commitments, the European Commission can activate a process to suspend the Privacy Shield.

GOING FORWARD

The Commission encourages companies to prepare for the Privacy Shield so that they are in a position to self-certify to the new framework as soon as an adequacy decision is adopted by the Commission. In general, the various constituents involved in the new framework will be required to take the following actions in connection with the Privacy Shield:

U.S. Companies

U.S. companies must commit to comply with seven privacy principles, including

1) the Notice Principle;
2) the Choice Principle;
3) the Security Principle;
4) the Data Integrity and Purpose Limitation Principle;
5) the Access Principle;
6) the Accountability for Onward Transfer Principle; and
7) the Recourse, Enforcement and Liability Principle.

In addition, the European Commission encourages companies to (i) select the EU DPAs as their complaint resolution mechanism under the Privacy Shield, and (ii) publish transparency reports on national security and law enforcement access requests regarding EU personal data.

U.S. Authorities

U.S. authorities will be responsible for enforcing the framework and respecting the limitations and safeguards established regarding access to personal data by law enforcement and for national security purposes. U.S. authorities also must handle complaints received from EU individuals in a timely and effective manner.

EU Data Protection Authorities

EU DPAs must ensure that individuals can exercise their rights effectively, including by transferring their complaints to the competent U.S. authority, as well as cooperating

with the relevant U.S. authority. In particular, EU DPAs must assist complainants with cases brought in front of the Privacy Shield Panel, exercise oversight over transfers of EU HR personal data and trigger the Ombudsperson mechanism.

European Commission

The European Commission will adopt an adequacy decision that will be reviewed regularly, allowing the Privacy Shield to be consistently monitored, in contrast with the previous Safe Harbor.

NEXT STEPS

An extraordinary plenary meeting of the Article 29 Working Party was organized at the end of March 2016. After obtaining the non-binding opinion of the Working Party and consulting a committee composed of representatives of the EU Member States, a final decision by the College of Commissioners will be made. In the meantime, U.S. authorities will prepare for the implementation of the new framework.

Federal Trade Commission ("FTC") chairwoman Edith Ramirez issued a statement[5] in response to the release of the new framework. She said that "[t]he EU-U.S. Privacy Shield Framework supports the growing digital economy on both sides of the Atlantic, while ensuring the protection of consumers' personal information. In providing an important legal mechanism for transatlantic data transfers, it benefits both consumers and business in the global economy." Chairwoman Ramirez also emphasized the FTC's role, saying that "the FTC will make enforcement of the new framework a high priority, and we will work closely with our European counterparts to provide robust privacy and data security protections for consumers in the United States and Europe."

[5] https://www.ftc.gov/news-events/press-releases/2016/02/statement-ftc-chairwoman-edith-ramirez-eu-us-privacy-shield-0?utm_source=govdelivery.