

AN A.S. PRATT PUBLICATION

OCTOBER 2021

VOL. 7 NO. 8

PRATT'S
**PRIVACY &
CYBERSECURITY
LAW**
REPORT



EDITOR'S NOTE: QUESTIONS AND ANSWERS

Victoria Prussen Spears

**FIVE THINGS YOU SHOULD EXPECT TO BE ASKED
AFTER A CYBER SECURITY INCIDENT**

Kelly Blair, James Lloyd, Aravind Swaminathan,
and Laura Nonninger

**FTC SETTLES COPPA ACTION AGAINST
"COLORING BOOK FOR ADULTS"**

Tracy Shapiro and Libby J. Weingarten

**SECOND CIRCUIT ARTICULATES INJURY
STANDARD IN DATA BREACH SUITS**

Rahul Mukhi and JD Colavecchio

**SUED FOR A DATA BREACH OUT OF STATE?
DON'T FORGET A PERSONAL JURISDICTION
DEFENSE**

Timothy J. St. George, Ronald I. Raether, and
David N. Anthony

**FIFTH CIRCUIT LATEST TO CRY TAINT ON DOJ
TAINT TEAM**

Elliot S. Rosenwald, Marcus A. Asner, and
Alexis Gannaway

**RECENT CYBERSECURITY AND RANSOMWARE
GUIDANCE THAT EVERY BUSINESS SHOULD BE
REVIEWING**

Elizabeth F. Hodge and Christy S. Hawkins

**FRENCH COURT PROVIDES GUIDANCE ON DATA
TRANSFER SAFEGUARDS AND SUFFICIENT
PROTECTIONS AGAINST ACCESS REQUESTS
FROM U.S. AUTHORITIES**

Ricky C. Benjamin and Christy S. Hawkins

**PRC DATA SECURITY LAW: WHAT YOU NEED TO
KNOW**

Clarice Yue, Michelle Chan, Sharon Zhang, and
Tiantian Ke

**CHINA PUBLISHES NEW DRAFT REGULATIONS
ON DATA SECURITY MANAGEMENT OF
AUTOMOBILE OPERATORS TO PROTECT PRIVACY**

Jenny (Jia) Sheng, Chunbin Xu, and
Esther Tao

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7

NUMBER 8

October 2021

Editor's Note: Questions and Answers

Victoria Prussen Spears 251

Five Things You Should Expect to Be Asked After a Cyber Security Incident

Keily Blair, James Lloyd, Aravind Swaminathan, and Laura Nonninger 254

FTC Settles COPPA Action Against "Coloring Book for Adults"

Tracy Shapiro and Libby J. Weingarten 259

Second Circuit Articulates Injury Standard in Data Breach Suits

Rahul Mukhi and JD Colavecchio 264

Sued for a Data Breach Out of State? Don't Forget a Personal Jurisdiction Defense

Timothy J. St. George, Ronald I. Raether, and David N. Anthony 267

Fifth Circuit Latest to Cry Taint on DOJ Taint Team

Elliot S. Rosenwald, Marcus A. Asner, and Alexis Gannaway 271

Recent Cybersecurity and Ransomware Guidance That Every Business Should Be Reviewing

Elizabeth F. Hodge and Christy S. Hawkins 274

French Court Provides Guidance on Data Transfer Safeguards and Sufficient Protections Against Access Requests from U.S. Authorities

Ricky C. Benjamin and Christy S. Hawkins 279

PRC Data Security Law: What You Need to Know

Clarice Yue, Michelle Chan, Sharon Zhang, and Tiantian Ke 283

China Publishes New Draft Regulations on Data Security Management of Automobile Operators to Protect Privacy

Jenny (Jia) Sheng, Chunbin Xu, and Esther Tao 287

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 [251] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2021 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

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

EDITOR-IN-CHIEF

STEVEN A. MEYEROWITZ

President, Meyerowitz Communications Inc.

EDITOR

VICTORIA PRUSSEN SPEARS

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

EMILIO W. CIVIDANES

Partner, Venable LLP

CHRISTOPHER G. CWALINA

Partner, Holland & Knight LLP

RICHARD D. HARRIS

Partner, Day Pitney LLP

JAY D. KENISBERG

Senior Counsel, Rivkin Radler LLP

DAVID C. LASHWAY

Partner, Baker & McKenzie LLP

CRAIG A. NEWMAN

Partner, Patterson Belknap Webb & Tyler LLP

ALAN CHARLES RAUL

Partner, Sidley Austin LLP

RANDI SINGER

Partner, Weil, Gotshal & Manges LLP

JOHN P. TOMASZEWSKI

Senior Counsel, Seyfarth Shaw LLP

TODD G. VARE

Partner, Barnes & Thornburg LLP

THOMAS F. ZYCH

Partner, Thompson Hine

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. Copyright 2021 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. 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, 631.291.5541. 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.

French Court Provides Guidance on Data Transfer Safeguards and Sufficient Protections Against Access Requests from U.S. Authorities

*By Ricky C. Benjamin and Christy S. Hawkins**

France’s Conseil d’État recently issued an opinion that found sufficient “supplementary measures” were in place to protect personal data from public authority access requests, and discussed the measures that were key to its finding. The authors of this article discuss the opinion.

In the wake of the Court of Justice of the European Union’s (“CJEU”) decision in *Schrems II*, companies have had few real-world examples of how they can provide “supplementary measures” to protect personal data from overbroad access requests by public authorities. Going beyond advisories and FAQs, France’s Conseil d’État recently issued an opinion that found sufficient “supplementary measures” were in place to protect personal data from public authority access requests, and discussed the measures that were key to its finding.

The court’s perspective is a must-read for companies struggling with the risks of international data transfers following *Schrems II*, and evaluates factors we can use to protect personal data from overbroad personal data access requests from public authorities – both to meet the standards of EU Supervisory Authorities and the data subjects whose personal data is in play.

BACKGROUND

In July 2020, the CJEU decision in a case referred to the CJEU from the Irish Data Protection Commissioner, colloquially referred to as “*Schrems II*,” had global implications for the transfer and processing of personal data subject to the EU’s General Data Protection Regulation (“GDPR”). Specifically, one major point of *Schrems II* was the CJEU’s invalidation of the EU-U.S. Privacy Shield as an approved data transfer mechanism under the GDPR. Months later, in March 2021, U.S. Secretary of Commerce Gina Raimondo and European Commissioner for Justice Didier Reynders announced in a joint press statement¹ that they had decided to intensify negotiations

* Ricky C. Benjamin is a partner at Akerman LLP, focusing his practice on healthcare regulatory, transactional, and litigation. Christy S. Hawkins (CIPP/US, CIPP/E, CIPM, FIP, PLS) is a litigation associate at the firm focusing her practice on privacy, cybersecurity, and incident response. The authors may be reached at ricky.benjamin@akerman.com and christy.hawkins@akerman.com.

¹ <https://www.commerce.gov/news/press-releases/2021/03/intensifying-negotiations-trans-atlantic-data-privacy-flows-joint-press>.

on an enhanced EU-U.S. Privacy Shield Framework. But the joint press statement said little else, and unless/until an enhanced EU-U.S. Privacy Shield Framework is adopted, businesses must continue to rely on other mechanisms to transfer personal data to the United States under the GDPR.

In the wake of *Schrems II*, many businesses have been left with more questions than answers – not only concerning if or when a new EU-U.S. Privacy Shield Framework will be adopted, but also whether transfers to the United States based on other data transfer mechanisms – including Standard Contractual Clauses – can be lawfully made consistent with the GDPR. Many are wondering whether lawful transfers are even possible in cases where the data processing is or might be subject to U.S. law. This question goes beyond the obvious situation where personal data of persons located in the European Economic Area (“EEA”) is transferred to or processed in the United States. What about data processing that may be subject to U.S. law because one of the data processors is a subsidiary of a U.S. company, even though the controller and processors are based in and processing personal data in the EEA? For at least this limited situation, France’s highest administrative court, the Conseil d’État, has provided helpful guidance.

WHAT SUPPLEMENTARY MEASURES ARE ENOUGH?

In a recent case, the French court examined a claim filed by professional associations against Doctolib, an e-health service company in Europe, seeking to stop Doctolib’s processing of personal data because one of Doctolib’s data processors, AWS Sarl, is a subsidiary of U.S.-based Amazon Web Services. Doctolib is an online platform being used in France as authorized by the ministry of Solidarity and Health to schedule COVID-19 vaccinations. The data at issue was hosted by AWS Sarl, a subsidiary of U.S. company Amazon Web Services. The associations claimed that because AWS Sarl was a subsidiary of a U.S. company, it was subject to U.S. law and, even in the absence of data transfer to the U.S., may be the subject of an access request by U.S. authorities. The court referenced the *Schrems II* decision and found that although there was a risk of access by U.S. authorities, there were appropriate protections in place so that the data processing could still proceed lawfully under the GDPR.

The court examined three factors in finding that the data processing at issue provided sufficient safeguards against access by U.S. authorities:

- (1) Legal safeguards;
- (2) Technical safeguards; and
- (3) Administrative safeguards.

Legal Safeguards

In assessing the legal safeguards in place, the court evaluated the contract between Doctolib and AWS Sarl, and more specifically, AWS Sarl’s contractual obligations if

faced with an access request. Because the contract contained a precise procedure that AWS Sarl must follow in the event of an access request by a public authority, specifically requiring it to challenge access requests from public authorities, this procedure weighed in favor of finding sufficient safeguards to protect such data from being disclosed in response to an access request in the United States.

Technical Safeguards

The court also emphasized that Doctolib set up a device for securing data hosted by AWS Sarl – the data at issue was encrypted and the key was entrusted to a third party located in France to prevent data from being read by third parties. With this measure in place, there was an added layer of protection against inquiries from public authorities.

Administrative Safeguards

The court further examined two administrative safeguards in place which strengthened the protections against potential access requests from U.S. public authorities.

First, the court noted that the data was limited to contact information and did not include medical information on grounds for vaccination eligibility. Under the principle of data minimization, the collection had been strictly limited to the information necessary to fulfill the purposes of the contract: identifying people and making vaccination appointments.

Second, the court noted that the data was only retained for a limited time. In furtherance of the storage limitation principle, personal data was kept for a maximum of three months after the date of the appointment and could be deleted online sooner by the persons whose personal data is involved.

KEY TAKEAWAYS

While the French court's decision applies in a very limited context, there are some key takeaways that companies can utilize to better protect personal data transfers that are at risk following *Schrems II*.

First, the parties here went beyond the baseline contractual guarantees to protect personal data from access requests by a public authority. When incorporating additional contractual safeguards, companies should have an eye toward procedures that either or both parties will follow in the event of a public authority's access request.

Second, the parties evaluated practical technical measures to protect the data at issue from such a request. Here, the parties ensured that the encryption key was stored and retained separately from the encrypted data, and moving forward outside this specific case, there may be other comparable technical solutions to achieve a similar goal.

Third, the court evaluated administrative safeguards in place in furtherance of two core privacy principles: data minimization and storage limitation. Companies assessing

administrative safeguards would do well to ensure they are implementing privacy by design, including the principles relating to processing of personal data set forth in Article 5 of the GDPR.

In any case, it is clear that a “check the box” approach to personal data transfers from the EU will not be sufficient to support data transfers going forward. This minimal approach will not satisfy regulators or data subjects that personal data is protected from overbroad government access requests. Rather, companies must thoughtfully evaluate the protections in place for transfers outside of the EU and consider supplemental measures that may be needed to safeguard personal information, and in particular, from access requests by public authorities.