AN A.S. PRATT PUBLICATION
NOVEMBER-DECEMBER 2020
VOL. 6 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 **NUMBER 9** **NOVEMBER - DECEMBER 2020**

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 [245] (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

(2020–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.

Schrems Strikes Again: Battery of New Data Privacy Complaints Raise Compliance Questions for EU-U.S. Data Transfers

By Angelo A. Stio III, Sharon R. Klein, and Jason J. Moreira *

Privacy activist Max Schrems has filed 101 complaints with 30 different EU regulatory bodies alleging that dozens of well-known companies are improperly continuing to transmit data to U.S. companies like Google and Facebook in violation of the Schrems II *decision and EU data privacy laws. The authors of this article discuss the complaints and compliance matters for EU-U.S. data transfers.*

Barely one month after the Court of Justice of the European Union ("CJEU") issued its *Schrems II* decision[1] striking down the EU-U.S. Privacy Shield Framework ("Privacy Shield"), Austrian privacy activist Max Schrems has filed 101 complaints[2] with 30 different EU regulatory bodies alleging that dozens of well-known companies in e-commerce, telecommunications, banking, higher education, and other industries are improperly continuing to transmit data to U.S. companies like Google and Facebook in violation of the *Schrems II* decision and EU data privacy laws. The complaints represent an effort by Mr. Schrems and his nonprofit organization, NOYB (None of Your Business), to leverage the *Schrems II* decision to prohibit transfers of personal data from the EU to the United States and other countries, which he argues do not have adequate levels of protection in place.

Given the number of European regulatory bodies involved and the complexity of the legal questions at issue, it is possible that a patchwork of regulatory responses could develop across the continent over the coming months and years.

As a result, companies seeking to navigate this rapidly changing legal landscape – especially large technology companies and cloud-based service providers – should perform a thorough internal risk assessment, consult experts to develop comprehensive compliance strategies, and identify and implement best practices as they develop over time.

---

* Angelo A. Stio III (angelo.stio@troutman.com) is a partner at Troutman Pepper Hamilton Sanders LLP focusing his practice on financial services issues, higher education law, and data privacy and security. Sharon R. Klein (sharon.klein@troutman.com) is a partner at the firm advising businesses on privacy, security, and data protection matters. Jason J. Moreira (jason.moreira@troutman.com) is an associate at the firm focusing on complex commercial litigation.

[1] https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

[2] https://noyb.eu/en/eu-us-transfers-complaint-overview.

BACKGROUND

The 101 regulatory complaints represent the most recent examples of coordinated legal action by Mr. Schrems and NOYB to advance EU privacy protections over personal data. Leading up to these filings, Mr. Schrems had litigated two important decisions in *Schrems I* and *Schrems II*, which raised concerns about the adequacy of protection afforded to EU citizens whose information is transferred to the United States.

In *Schrems I*, decided on October 6, 2015, Mr. Schrems successfully petitioned the CJEU to invalidate the U.S.-EU Safe Harbor Framework ("Safe Harbor"), which had been in place since 2000, and provided a legal basis for EU entities to transfer personal data to the United States. The CJEU invalidated Safe Harbor, finding U.S. legislation:

(1) Failed to afford EU data subjects sufficient legal remedies;

(2) Authorized the storage of all EU personal data without differentiation or limitation based on specific objectives; and

(3) Failed to limit interference with individual privacy rights to what is strictly necessary, among other reasons.

Following the invalidation of Safe Harbor, the United States and EU adopted the EU-U.S. Privacy Shield Framework, in order to ensure adequate protections were in place for the transfer of personal data sent from the EU to the United States. U.S. companies participated in EU-US Privacy Shield by self-certifying with the Department of Commerce and publicly committing to compliance with Privacy Shield's safety and security principles. Before *Schrems II*, more than 5,300 companies were using the EU-U.S. Privacy Shield Framework as the legal basis to transfer personal data from the EU to the United States.

In *Schrems II*, decided on July 16, 2020, Mr. Schrems petitioned the CJEU to invalidate EU-U.S. Privacy Shield. The CJEU invalidated EU-U.S. Privacy Shield on the basis that the Privacy Shield failed to provide protections that were "essentially equivalent" to the protections afforded to EU residents, including "effective administrative and judicial redress for the EU data subjects whose personal data are being transferred."

In particular, the CJEU found that U.S. surveillance programs conducted pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA") or Executive Order 12333 do not grant surveilled individuals adequate rights of redress before an independent and impartial judicial body, as required by Article 47 of the EU Charter of Fundamental Rights.

The CJEU also found that the bulk data collection practices by or on behalf of U.S. intelligence agencies pursuant to Section 702 of FISA and Executive Order 12333 lacked proportionality, as required by EU law, including the General Data Protection Regulation ("GDPR").

The CJEU also concluded in *Schrems II* that although Standard Contractual Clauses ("SCCs") remain a valid alternative mechanism for transferring personal data outside of the EU, companies relying on SCCs must nevertheless self-police to ensure adequate protections for EU data subjects, as required under the GDPR. SCCs are a set of contractual agreements between the exporter and importer of personal data that are issued by the European Commission and require each party to provide adequate protections for the personal data transferred between them. If an importer of EU data is not able to comply with the SCCs, the importer must inform the data exporter, at which point the data exporter must suspend data transfers if there are no other safeguards in place that would provide an adequate level of protection.

In other words, any EU organizations that use SCCs have an affirmative obligation to proactively ensure, before any transfer of data, that there is in fact an adequate level of protection as informed by EU law.

NEW REGULATORY COMPLAINTS

Mr. Schrems's new regulatory complaints are intended to leverage the CJEU's holdings in *Schrems II*, with respect to both the invalidation of EU-U.S. Privacy Shield and the affirmative obligations of companies relying on SCCs to provide adequate data privacy protections, in order to further expand the privacy rights and protections afforded to EU data subjects.

The complaints allege that the named EU companies are erroneously continuing to rely on the invalid EU-U.S. Privacy Shield, to engage in cross-border data transfers. The complaints also allege that, based on an analysis of the HTML source code contained in their webpages, the named EU companies are improperly continuing to use Google Analytics or Facebook Connect, despite the fact that both Facebook and Google are subject to U.S. surveillance laws, again contrary to the CJEU's decision in *Schrems II*.

Specifically, the complaints contend that EU companies continuing to rely on SCCs when transferring personal data to Google and/or Facebook servers in the United States cannot be doing so lawfully because Google and Facebook are subject to U.S. surveillance laws such as FISA 702, which violate fundamental privacy rights recognized in the EU.

Over the coming months and possibly years, the EU Data Protection Authorities ("DPA") located in each EU member state will be tasked with investigating the complaints and determining whether to take action against any of the named data-exporting companies. The new complaints should put pressure on DPAs to provide further guidance on the use of SCCs going forward. They also should serve as motivation for EU and U.S. regulators to agree upon a new framework for the lawful cross-border transfer of data from the EU to the United States.

That said, a consistent and coordinated response to the complaints is unlikely. Given the number of European regulatory bodies involved and the complexity of the legal questions at issue, it is possible that a patchwork of regulatory responses could develop over the coming months and years. In the interim, affected companies may be forced to continue operating with significant uncertainty as they attempt to navigate the EU regulatory landscape.

The CJEU's *Schrems II* decision and the recent wave of regulatory complaints that Mr. Schrems filed may prompt the European Commission to release updated SCCs with additional protections for EU data being transferred to the United States. The European Commission last issued SCCs applicable to transfers of data from EU controllers to non-EU or EEA controllers in 2004, and issued SCCs applicable to transfers of data from EU controllers to non-EU or EEA processors in 2010, so both are due for an update. The issuance of updated SCCs, if sufficiently comprehensive, could help to ameliorate the current uncertainty surrounding whether and under what circumstances reliance on SCCs will be sufficient to comply with *Schrems II*, the GDPR, or other aspects of EU privacy law.

CONCLUSION

Ultimately, *Schrems II* and the recently filed regulatory complaints will force the EU and United States to develop and implement a successor to EU-U.S. Privacy Shield.

In the interim, however, without the benefit of predictable data protection framework, companies involved with importing personal data from the EU face significant regulatory risks and compliance challenges. To address these risks and compliance challenges, companies should seek the use of lawful means to effectuate cross-border transfers including the expanded use of SCCs with protocols for internal risk assessments to ensure adequate protections exist for EU data subjects whose data is transferred to the United States.

Other alternatives include keeping EU data on servers in the EU as well as scrutinizing and limiting the data of EU subjects transferred to the United States only to what is minimally necessary and/or de-identify or anonymize personal data prior to such transfer.