AN A.S. PRATT PUBLICATION
JANUARY 2021
VOL. 7 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 1** **JANUARY 2021**

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

(2021–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.

Can California's Privacy Initiative Revitalize U.S.-EU Commerce?

By Dominique Shelton Leipzig, David T. Biderman, Chris Hoofnagle, and Tommy Tobin [*]

The passage of the California Privacy Rights Act more closely aligns the consumer privacy standards of one of the United States' most economically important jurisdictions with those of the European Union. This may mean closer economic integration is not only possible but likely. The authors of this article discuss the issue.

COVID-19's rapid transition into remote work environments has demonstrated our increasing reliance on distance working and learning tools. As this reliance on remote platforms has increased, so too has the need for such remote environments to maintain data privacy and security.[1] The multifaceted impact that COVID-19 has wrought on societies across the globe has created knotty privacy issues for individuals, employers, and governments.[2]

The challenges facing consumers and policymakers are real and present. The onset of the COVID-19 pandemic has coincided with resonant issues of racial profiling and bias and the role of technology in promoting racial justice or, unfortunately, reinforcing harmful stereotypes and outcomes.[3] Indeed, a tremendous racial and social justice movement has emerged, spanning the globe and increasing focus on the use and sharing of personal information. Whether it is for security in a "smart city," infrared sensor cameras to detect fever, or mobile devices to assess social distancing norms, one thing is clear – we are increasingly creating an infrastructure today that we are dependent on, at least in the short term. When the pandemic ultimately fades, for what other purposes will this infrastructure be used?

---

[*] Dominique Shelton Leipzig is the firmwide co-chair of Perkins Coie LLP's Ad Tech Privacy & Data Management practice. David T. Biderman is firmwide chair of the firm's Consumer Products & Services Litigation practice. Chris Hoofnagle is faculty director at U.C. Berkeley Center for Law & Technology. Tommy Tobin is an associate in Perkins Coie LLP's Consumer Products & Services Litigation practice.

[1] *See* Dan Raywood, *Trust in remote working tools declines as need for security increases*, Infosecurity Magazine (Oct. 21, 2020), https://www.infosecurity-magazine.com/news/remote-working-tools-declines/.

[2] *See* Omer Tene, *With COVID-19, privacy is more central than ever before*, IAPP News (May 27, 2020), https://iapp.org/news/a/with-covid-19-privacy-is-more-central-than-ever-before/.

[3] *See generally* Cathy O'Neil, *Weapons of math destruction: How big data increases inequality and threatens democracy* (2016) (noting that some of the algorithms undergirding data science may reflect implicit biases and result in outcomes with pernicious outcomes).

There are some 140 existing data protection laws across the globe. One of the most notable is the EU's General Data Protection Regulation ("GDPR").[4] These laws limit the transfer of personal data out of the European Union's protected zones into other jurisdictions, such as the United States.

THE EUROPEAN HIGH COURT INVALIDATES THE EU-U.S. PRIVACY SHIELD

In the midst of the global pandemic, the EU's highest court, the Court of Justice of the European Union ("CJEU"), declared the Privacy Shield program between the United States and the EU as "invalid" on the grounds that U.S. law does not provide an equivalent level of data privacy compared to the protections in the EU.[5] This Privacy Shield program was a vehicle for businesses to responsibly move data between the two jurisdictions.

Since the ruling, the U.S. Department of Commerce and EU officials have "initiated discussions" to enhance the Privacy Shield framework to comply with the CJEU's order.[6] European authorities have also interpreted the CJEU's invalidation of the Privacy Shield as affording data transfers with no grace period, meaning that any data transferred between the United States and EU should be made only after the legal basis for such a transfer has been assessed.[7]

The EU has embraced privacy as a fundamental human right. We seem to be on the same trajectory, with Americans' concern rising over powerful intelligence systems and the scores of security incidents spilling personal data online. As people around the world increasingly worry that elections are jeopardized by misinformation and political targeting on social media, there are increased calls for federal privacy legislation in the

[4] Further detail regarding the GDPR may be found at *EU Data Protection Rules*, https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en; *see also Data Protection in the EU*, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (noting that the "EU Charter of Fundamental Rights stipulates that EU citizens have the right to protection of their personal data.").

[5] Case C-311/18 - *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, Judgment (July 16, 2020), http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=9791227.

[6] *FAQs - EU-U.S. Privacy Shield Program Update* (Aug. 20, 2020), https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update.

[7] European Data Protection Board, *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (July 23, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf ("FAQs").

United States. As Congress debates a potential privacy framework at the federal level,[8] states are leading the way in how governments enforce issues of data privacy and data security.[9]

A $7 TRILLION CHALLENGE . . . AND OPPORTUNITY

In the wake of the CJEU's decision, U.S. Secretary of Commerce Wilbur Ross said the federal government would work to minimize the "negative consequences to the $7.1 trillion transatlantic economic relationship" resulting from the invalidation of the Privacy Shield framework.[10] Secretary Ross noted that it was critical for companies, including the more than 5,300 Privacy Shield participants, to be able to continue transferring data between the EU and the United States, especially as the economies of both jurisdictions wrestle with the COVID-19 pandemic.[11]

If trade is jeopardized, businesses may be forced to relocate their data operations to the EU to comply with the GDPR, and these increased costs will undoubtedly translate into lost jobs here at home. Startup and small enterprises are particularly vulnerable because they lack the resources to duplicate their infrastructure in Europe so that data stays on the continent.

European negotiators want both public and private sector reforms. The public sector reforms will require political negotiations to address the EU's concerns regarding foreign intelligence practices in the United States and abroad. Given the magnitude of the repercussions, it is hard to imagine that a political solution to the surveillance issues will be easily reached. There are many proposals for addressing U.S. government surveillance concerns with the EU.

Assuming the surveillance issues raised in the CJEU decision are resolved politically, there is an additional hurdle specific to the private sector that must be surmounted; namely, European officials following the European high court's decision that other privacy laws should be "essentially equivalent" to the GDPR.[12] Given that the United States lacks a national law of the necessary equivalence to the GDPR, the door is open for the states, and particularly California, to lead the charge in bridging transatlantic data requirements.

---

[8] *See* Ryan Chiavetta, CIPP/US, *US Senate hearing covers COVID-19, the need for a federal privacy law and familiar roadblocks*, IAPP News (Sept. 24, 2020), https://iapp.org/news/a/senate-hearing-covers-covid-19-the-need-for-a-federal-us-privacy-law-and-familiar-roadblocks/.

[9] *See* Jennifer Bryant, *Mass. attorney general stands up data privacy, security division,* IAPP News (Aug. 25, 2020), https://iapp.org/news/a/mass-ags-data-privacy-security-division-an-advocate-for-consumers/ (noting that a small number of states, including Massachusetts, New Jersey, and California, have dedicated privacy units in their state attorney generals' offices).

[10] U.S. Dep't of Commerce, *U.S. Secretary of Commerce Wilbur Ross statement on Schrems II ruling and the importance of EU-U.S. data flows* (July 16, 2020), https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.

[11] *Id.*

[12] *FAQs*, *supra* note 7, at 3.

CALIFORNIA AS THE NATION'S PRIVACY LEADER

California has enacted the nation's most stringent data privacy law, the California Consumer Privacy Act ("CCPA"). The CCPA went into effect in early 2020, with its regulations finalized over the summer. Already, the state's attorney general has sent ominous warnings to businesses that fail to comply with the CCPA's data privacy requirements: "We will look kindly, given that we are an agency with limited resources, and we will look kindly on those that . . . demonstrate an effort to comply," [but if] "they are not (operating properly) . . . I will descend on them and make an example of them, to show that if you don't do it the right way, this is what is going to happen to you."[13]

Now, California voters have expanded upon the CCPA's data privacy protections and approved the California Privacy Rights Act ("CPRA"). The CPRA fundamentally changes the way the state approaches data privacy, which, *inter alia*, includes additional rights for consumers, expands the definition of sensitive individual data to include racial and ethnic information, and establishes a state agency to enforce data privacy laws.[14] With the approval of the CPRA, California is now on its way to "essential equivalence" with the EU's GDPR. In other words, California stands to prosper as it approaches what European authorities may consider "adequate" data privacy protections for sharing of data between the EU and the state.

Adequacy is a one-way certification from the EU, detailing that another country (or territory within a country) has a legal regime that provides an "adequate level of protection" for EU citizens' data processed in that country. Currently, there is no such law in United States at the national or individual state level. Now that the CPRA has passed, European authorities may find California's privacy law "adequate," which would allow companies adhering to this law to process EU citizens' data legally in the United States.

---

[13] Nandita Bose, *California AG says privacy law enforcement to be guided by willingness to comply*, Reuters (Dec. 10, 2019), https://www.reuters.com/article/us-usa-privacy-california/california-ag-says-privacy-law-enforcement-to-be-guided-by-willingness-to-comply-idUSKBN1YE2C4.

[14] *See generally* Dominique Shelton Leipzig & David Biderman, *California Privacy Dreaming: The CCPA and the New Ballot Initiative CPRA (Proposition 24) Break New Ground: A Conversation with Alastair Mactaggart*, Decrypted Unscripted (Oct. 8, 2020), https://www.spreaker.com/user/pcpodcast/decrypted-e5; Dominique Shelton Leipzig, Bo W. Kim, Laura Mujenda, *A CPRA/CCPA 2.0 Conversation With Alastair Mactaggart and Dominique Shelton Leipzig*, Perkins Coie Webinar (Jun. 30, 2020), https://perkinscoie.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=b210bcc3-be31-4a90-aef3-abf001479f6a.

WHAT NEXT?

Allied to a political discussion regarding foreign surveillance, the CPRA provides a concrete set of goals and standards for a newly reinvigorated Privacy Shield. Hopes for any meaningful update to the Privacy Shield program between the July CJEU decision and the November 2020 general election were slim.[15] Now that the election has occurred and the CPRA has passed, the CPRA's provisions provide new guideposts for forging ahead on EU-U.S. data privacy discussions.

American businesses will come to address and incorporate California's new standards in the coming years, and these new California standards were modeled off their European counterparts. Privacy professionals are fully aware of the so-called "California effect,"[16] meaning that California's stringent data privacy standards tend to influence those standards applicable to other jurisdictions, especially for businesses that sell to California consumers.

The new CPRA demonstrates a path forward for establishing "essential equivalence" between an American jurisdiction and the EU. In the months ahead, California will enact regulations to flesh out the CPRA, its expanded consumer rights, and a new state privacy agency. At the same time, efforts to establish and approve a federal privacy protocol may take years in these politically divisive times. Critically, the CPRA is now part of the body of American law and applicable to one of the world's most innovative technological hubs, Silicon Valley.

The CJEU decision also adversely affects other methods for transferring data to the United States, such as standard contractual clauses and binding corporate rules that now suddenly require a case-by-case analysis of "additional safeguards" for personal data transfers to the United States. The CPRA could help to make those other transfer vehicles easier to use as well.

American and European negotiators should look to California for a path forward for reinvigorated negotiations to bridge data transfers between these jurisdictions. In the absence of federal action, California stands to emerge even more prominently as the nation's leader in data privacy and to create a framework poised to establish "adequacy" with the EU's stringent GDPR protocols. The CPRA could anchor a new Privacy Shield, perhaps called a Privacy Accord, as our nation will increasingly be able to represent that the United States has embraced privacy rules that are "essentially equivalent" as those used in the EU.

---

[15] Brian Hengesbaugh, CIPP/US & Elisabeth Dehareng, CIPP/E, *7 predictions for the road ahead after 'Schrems II,'* IAPP News (July 28, 2020), https://iapp.org/news/a/seven-predictions-for-the-road-ahead-after-schrems-ii/.

[16] *See* Josephine Williams & Kristina Irion, *Dream of Californication: Welcome to the Californian Consumer Privacy Act*, Internet Policy Review (Oct. 16, 2018), https://policyreview.info/articles/news/dream-californication-welcome-californian-consumer-privacy-act/1351.