PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

EDITOR'S NOTE: WHAT KEEPS YOU UP AT NIGHT?
Steven A. Meyerowitz

CYBERSECURITY: WHAT KEEPS US UP AT NIGHT
Jonathan S. Kolodner, Rahul Mukhi, and Megan Medeiros

CALIFORNIA CONSUMER PRIVACY ACT PROPOSED RULES: MODIFIED TO RECOGNIZE BUSINESS REALITIES?
Quyen T. Truong

THE EVOLVING PRIVACY LANDSCAPE AT A GLANCE: COMPLIANCE CONSIDERATIONS FOR A NEW DECADE
Daniel Ilan, Emmanuel Ronco, Natascha Gerlach, and Megan Medeiros

TRACED ACT TARGETS ILLEGAL ROBOCALLS
Ronald G. London

PHISHING SCAM DOES NOT IMPLICATE FORGERY COVERAGE, COURT REQUESTS FURTHER BRIEFING FOR COMPUTER FRAUD COVERAGE
Joshua A. Mooney

FROM THE COURTS
Jay D. Kenigsberg
Editor’s Note: What Keeps You Up at Night?
Steven A. Meyerowitz

Cybersecurity: What Keeps Us Up at Night
Jonathan S. Kolodner, Rahul Mukhi, and Megan Medeiros

California Consumer Privacy Act Proposed Rules: Modified to Recognize Business Realities?
Quyen T. Truong

The Evolving Privacy Landscape at a Glance: Compliance Considerations for a New Decade
Daniel Ilan, Emmanuel Ronco, Natascha Gerlach, and Megan Medeiros

TRACED Act Targets Illegal Robocalls
Ronald G. London

Phishing Scam Does Not Implicate Forgery Coverage, Court Requests Further Briefing for Computer Fraud Coverage
Joshua A. Mooney

From the Courts
Jay D. Kenigsberg
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/

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, [6] PRATT’S PRIVACY & CYBERSECURITY LAW REPORT [99] (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 © 2020 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
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

DAVID KALAT
Director, Berkeley Research Group

JAY D. KENIGSBERG
Senior Counsel, Rivkin Radler LLP

DAVID C. LASHWAY
Partner, Baker & McKenzie 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
The Evolving Privacy Landscape at a Glance: Compliance Considerations for a New Decade

By Daniel Ilan, Emmanuel Ronco, Natascha Gerlach, and Megan Medeiros*

The authors discuss recent changes in data privacy laws and note that boards and management will need to continue to monitor the evolving privacy compliance landscape to ensure that they are considerate of privacy obligations and attendant risks when implementing their business objectives and oversight into 2020.

Increased regulation continues to be the trend in data privacy law, with 2019 bringing forth a host of new regulations and guidance on existing laws. This year, the pace will not likely slow, with January 1, 2020 having marked the official arrival of robust data privacy law in the United States as the California Consumer Privacy Act ("CCPA") came into effect. Boards and management will need to continue to monitor the evolving privacy compliance landscape to ensure that they are considerate of privacy obligations and attendant risks when implementing their business objectives and oversight going into 2020.

CCPA

In its 2019 session, the California legislature amended the CCPA and the California Attorney General issued a set of regulations that implement, clarify and impose new obligations under the CCPA. Commentators expect that the law and regulations will be further amended, but as of now, if the CCPA applies to your business,1 notable obligations include:

• Updating websites, mobile applications and other locations where consumers’ personal information is collected in order to provide the consumer with meaningful understanding of the information collected about them at or before collection, as well as the purposes for which the information will be used.

---

* Daniel Ilan (dilan@cgsh.com) is a partner at Cleary Gottlieb Steen & Hamilton LLP focusing his practice on intellectual property law, as well as cybersecurity and privacy. Emmanuel Ronco (eronco@cgsh.com) is counsel at the firm focusing on intellectual property and technology, as well as privacy, personal data protection, and cybersecurity. Natascha Gerlach (ngerlach@cgsh.com) is a senior attorney at the firm specializing in electronic discovery and European data protection law. Megan Medeiros (mmedieiros@cgsh.com) is a practice development lawyer at the firm concentrating her practice in intellectual property law.

1 The Act applies to any entity doing business in California that meets any of the following thresholds: (i) it has annual gross revenues in excess of $25 million; (ii) it annually buys, receives for its commercial purposes, sells, or shares for commercial purposes personal information relating to 50,000 or more consumers, households, or devices; or (iii) it derives 50 percent or more of its annual revenue from selling consumer personal information.
If information is sold (as defined broadly under the CCPA), providing the consumer with a “Do Not Sell My Personal Information” link at the point of collection.

- Updating privacy policies to apply to online and offline (brick-and-mortar) practices. The policies must detail the categories of information that are collected, the sources of the information, how such information may be used and with whom, as well as the consumers’ rights under the CCPA and how to exercise those rights, including the right to opt out of sale of data and the right to access and delete data. If no notice of the right to opt out of sale is provided, companies must expressly state that they do not and will not sell personal information.

- Updating contracts with vendors that receive personal information to ensure your vendors qualify under certain exceptions under the law (such that sharing information with them does not constitute a “sale”) and collaborate with respect to consumers’ access or deletion requests.

- Training employees who are responsible for handling consumer inquiries about your business’ privacy practices, the requirements of the CCPA and how to direct consumers to exercise their rights.

- Implementing methods for complying with the rights granted by the CCPA, including:
  - Designating an official contact for questions about your company’s privacy policies.
  - Offering two or more designated methods for receiving consumer requests under the CCPA.
  - Establishing, documenting and complying with a method for verifying that the person making a request for access or deletion is indeed the subject consumer.
  - Ensuring your business can identify an individual consumer’s data to provide that individual with access to that data, delete it from your records or remove such data from data sets that are sold to third parties.

**OTHER PRIVACY LEGISLATION**

- *Other U.S. state laws.* Many states followed California’s lead, and last year 16 other states introduced legislation offering comprehensive consumer privacy reform. However, only Maine and Nevada passed legislation, and the Maine law applies only to internet service providers operating in Maine when providing internet access service to customers physically located in Maine,
while the law in Nevada is focused solely on data sales. Connecticut, Texas, and a few other states passed legislation to enact advisory councils or task forces to study and recommend data privacy laws.

- **International laws.** China and India each had notable legislative action over the past year. In May 2019, the Cyberspace Administration of China issued draft Measures on Administration of Data Security that, when issued in final form, will constitute binding regulations on network operators who collect, store, transmit, process and use data within Chinese territory. In December 2019, India was poised to pass a General Data Protection Regulation (“GDPR”)-inspired data privacy law that would require express consent for most uses of an individual’s personal data and allow for individuals to request their personal information be deleted.

- **Biometric laws.** In two separate rulings in 2019, the Illinois Supreme Court and a three-judge panel in the U.S. Court of Appeals for the Ninth Circuit sided with the plaintiffs in cases regarding alleged breaches of the Illinois Biometric Information Privacy Act (“BIPA”). While the Ninth Circuit federal case, Patel, et al. v. Facebook, is stayed to allow Facebook to petition to the U.S. Supreme Court, the Illinois Supreme Court decision in Rosenbach v. Six Flags found plaintiffs need only show violation of their rights under BIPA – as opposed to actual injury – to bring a claim for violation of BIPA. In addition, a bipartisan federal bill to regulate facial recognition and state biometric privacy laws in New York, Florida, Massachusetts, and Arizona was introduced in 2019. Many states have also amended the definition of personal information in their existing privacy or data breach notification laws to include biometric information.

**NOTABLE ENFORCEMENT**

Early in 2019, the French Data Protection Authority announced a €50 million fine against Google for alleged GDPR violations for allegedly not properly disclosing to users how personal data is collected and used across its personalized ads services.

Additionally, in October of 2019, the Berlin Commissioner for Data Protection and Freedom of Information issued a €14.5 million fine against a German real estate company, die Deutsche Wohnen SE, for its failure to maintain a GDPR-compliance data retention policy and consequently storing tenants’ personal information longer than necessary for the purposes for which the data was initially collected, and without a legal basis for such excessive retention. This shows that a seemingly minor offense – over retention of data – can also bring serious penalties.

These two actions differ from those enforcement actions highlighted in “Cybersecurity: What Keeps Us Up at Night,” also in this issue of *Pratt’s Privacy & Cybersecurity Law Report*, in that these actions did not arise out of a cybersecurity incident, but relate
solely to privacy violations – an alleged failure to obtain adequate consent from users prior to collecting and processing their information and improper retention of personal data, respectively.

KEY TAKEAWAYS

- The 2019 GDPR enforcement action against Google and legislative proposals demonstrate that authorities and legislatures are focused on consumer privacy – and not just cyberattacks.

- Legislative and enforcement trends indicate that companies need to continue to stay abreast of their data collection, processing and sharing activities and compliance obligations as this landscape evolves in 2020.