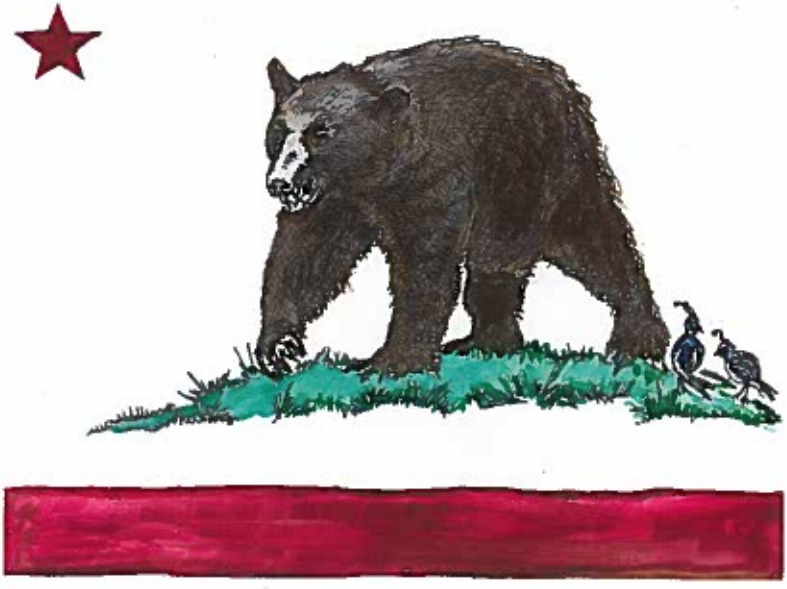
California Privacy Law

PRACTICAL GUIDE AND COMMENTARY



2017

LOTHAR DETERMANN

LJP Law Journal Press™

THE RECORDER

California Privacy Law

PRACTICAL GUIDE AND COMMENTARY
U.S. FEDERAL AND STATE LAW

2nd Edition

2017

LOTHAR DETERMANN

Suggested citation form: Determann, California Privacy Law § ___ at ___ (2017 ed.).

THE**RECORDER**

The Recorder
1035 Market Street
Suite 500
San Francisco, California 94103
800-756-8993
www.therecorder.com
alm.com
lawcatalog.com

International Standard Book Number
978-1-62881-204-6 (Print)
978-1-62881-205-3 (eBook)

Printed in the United States of America

An eBook or Online version of this publication is included as part of your purchase. To download, follow the instructions below. **Please note the 2017 eBook or Online product cannot be returned once the file has been downloaded.**

Login or register at: www.lawjournalpress.com/activate
Please enter code 547787 to download your product.

SUPPORTED DEVICES: We recommend Apple® iPad® or iPhone®, SONY® Reader. For PC or MAC users you must download a reader to view your eBook. We recommend Adobe® Digital Editions.

For help using this product, visit our FAQ page: www.lawjournalpress.com/help

For Returns:
In Care of: ALM Media
545 Wescott Road
Eagan, MN 55123
For QUESTIONS please contact Customer Service at 1-877-256-2472

Subscriptions to books are auto-renewed to avoid disruptions in service. Print editions must be returned within 30 days in resalable condition for refund. For downloadable eBook or Online products, a refund will be granted if the eBook or Online product has not been downloaded.

Other books include:

California Insurance Law
California Premises Liability Law
Library of California Business Litigation Forms
Library of California Employment Law Forms
Library of California Insurance Defense Forms
Library of California Medical Malpractice Forms
Library of California Product Liability Forms

For more information or to place an order,
please visit www.lawcatalog.com or call 800-756-8993.

Foreword

by Paul M. Schwartz

I

We are all California privacy lawyers, or soon will be.

California is the state with the largest economy in the United States. Were it an independent country, it would rank as the seventh-largest economy in the world. For companies within the United States and for participants in the global digital economy, commercial transactions with California residents are a "must." As a consequence, all privacy lawyers must be aware of the complex web of privacy and security regulations in the Golden State. Their advice to clients must be based on solid knowledge of California privacy law.

Beyond the economic significance of this state, there is a further and more subtle reason why California privacy law is important. It is due to the role of the "California Effect," which is a concept that refers to the role of California in setting a national privacy policy agenda.

Data breach notification legislation provides a leading example of the California Effect. First enacted by California in 2002, forty-six other states have now passed such legislation. In the HITECH Act of 2009, federal lawmakers required notification for leaks of health care information that falls under the jurisdiction of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

California privacy policy innovations have even had a global impact. In the European Union, the European Commission adopted a regulation in June 2013 establishing a data breach notification obligation for telecommunication companies and Internet service providers.[1] More broadly, the General Data Protection Regulation

[1] Commission Regulation (EU) No 611/2013, Official J. E.U. L 172/2 (June 24, 2013).

of 2016, which will become binding in May 2018, requires data controllers to notify supervisory authorities of data breaches and, in some instances, to inform the parties whose data is leaked.[2] As for the rest of the world, according to one estimate, one-third of nations in the Asia-Pacific region have adopted a data breach notification requirement.[3]

During the current era of gridlock in Washington, moreover, the role of California is more important than ever. Until recently, the California Effect typically served as the first part of a regulatory cycle. Typically, after legislative action in this state and perhaps others, regulated entities would seek regulatory relief through a "flight to Washington."[4] Congress would respond to legislative developments at the state level with laws that, at their best, would consolidate, correct, and improve initial efforts at regulation.

Today, however, there is profound gridlock in Washington. Congress is setting new records for its lack of productivity and struggling to carry out the most basic tasks, such as enacting a federal budget. It is largely silent on the privacy front. Thus, the traditional federal-state cycle for privacy legislation is missing a necessary component due to the general lack of federal inputs into the legislative process. In face of this silence from the Capitol, state privacy law in general and the California Effect in particular are more important than ever before. In turn, the California legislature has proven eager and able to enact new legislation. As Lothar Determann's masterful CALIFORNIA PRIVACY LAW demonstrates so well, the result is both highly complex as well as notably different from European Union law, which has established the template for most of the rest of the world outside of the United States.

II

Unlike the European Union, and as is typical for privacy law in the United States, California does not have an "omnibus" privacy

[2] Regulation (EU) 2016/679 (General Data Protection Regulation), 59 Official J. E.U. L 119 (May 4, 2016).

[3] Cynthia Rich, Privacy Laws in Asia, Privacy & Security Law Report, 14 PVLR 877, 2 (May 18, 2016).

[4] For the classic description of this process, *see* E. Donald Elliott, Bruce A. Ackerman & John C. Millian, Toward a Theory of Statutory Evolution: The Federalization of Environmental Law, 1. J.L. Econ. & Org. 313 (1985).

statute. In California, and elsewhere in the United States, there is a patchwork of sectoral privacy laws. The resulting pattern frequently contains both federal and state aspects. It can be quite challenging to determine basic questions such as which, if any, law applies, and the extent to which federal law completely or partially preempts state law.

As a further distinction with the European Union, California does not generally require a statutory basis for processing information. In the European Union, as summed up in a famous phrase from German data protection law, the fundamental principle is that of a "*Verbot mit Erlaubnisvorbehalt*" (a "Ban with Permission Proviso"). This concept means that the legal starting point forbids any processing of personal data unless a legal basis exists for this activity. GDPR Article 6 holds that the "[p]rocessing of personal data shall be lawful only if and to the extent" at least one of a list of enumerated conditions applies. In California, however, and elsewhere in the U.S., and as Determann makes clear, "companies are generally allowed to process personal data."[5] He writes, "Unless a particular restriction or prohibition applies, data processing is permitted."[6]

The contrast between the two legal systems is stark. A privacy lawyer in the U.S. must assess a patchwork of regulation and determine the extent to which her client is covered by any legal requirement. In the absence of any regulation, the use of personal data is generally permitted. In the European Union, however, the lawyer must find a specific legal justification that allows personal data processing to take place.

The risk in the European Union is that too much effort will be wasted on routine privacy compliance and too little attention will be devoted to areas of greatest danger to individuals. The first Federal Data Protection of Germany, Hans Peter Bull, has offered a stern warning concerning the approach that requires a legal basis for all processing or "handling" of personal data. Bull states: "To want to legally regulate any kind of communication between individuals represents a monstrous, downright delusional claim. To rigorously apply this claim would lead to a total regulation of

[5] Lothar Determann, California Privacy Law, Chapter 1 §1-5:4 (2nd Ed. 2017).
[6] Lothar Determann, California Privacy Law, Chapter 1 §1-5:4.

all of human life."[7] Regarding the European Union's approach, including that of German law, Bull adds that this orientation has led to "an excess of legislation" regulating data use.[8]

United States privacy law operates, however, on a "harm principle" rather than a "prevention principle."[9] It generally awaits a compelling case for regulatory action and defers to market forces—at least in the first instance. Without the safety net of an omnibus data protection law, the danger in the United States is that potential gaps in legal protections may exist as technology finds new ways to collect and use personal data.

A further risk in the United States is that the sheer complexity and volume of different statutes, federal and state, will overwhelm even the most determined privacy lawyer. Determann's CALIFORNIA PRIVACY Law proves indispensable in navigating this difficult landscape through the depth and clarity of its coverage as well as by its seamless integration of California law with federal law. Determann carefully reviews California's requirements for data security, location tracking, online privacy, and, of course, data breach notification. He explains the state's anti-paparazzi laws and its "Shine the Light" law, which requires mandatory disclosures to consumers when businesses transfer consumer information to third parties for direct marketing purposes.

California law from decades past can also take on new meaning in the Twenty-First Century, and Determann is sensitive to this turning of the legal tides. The California Song-Beverly Credit Card Act of 1971 is an example of an old law that has taken on new significance. The statute prohibits companies in California from requesting and recording personal information from consumers who use a credit card to pay for goods and services. It does not generally prohibit companies from collecting data from their customers, only from doing so in connection with credit card transactions, and it contains numerous statutory exceptions, such

---

[7] Hans Peter Bull, Sinn und Unsinn des Datenschutzes 57 (2015). "Es bedeutet einen ungeheuren, geradezu größenwahnsinnigen Anspruch, jede Art von Kommunikation zwischen Individuen rechtlich regeln zu wollen, und die konsequente Befolgung dieses Anspruchs würde zu einer totalen Durchnormierung des gesamten menschlichen Lebens führen."

[8] Hans Peter Bull, Sinn und Unsinn des Datenschutzes 57 (2015) at 76. "ein Übermass an Rechtsvorschriften."

[9] For a discussion of these principles in a context other than privacy, *see* Cass R. Sunstein, Laws of Fear: Beyond the Precautionary Principle 23-25 (2005).

as for cash advance transactions. In 2011, the California Supreme Court in *Pineda v. Williams-Sonoma Stores, Inc.* declared that ZIP codes were personal identification information pursuant to the Song-Beverly Act.[10] The ZIP codes were collected in *Pineda* so the defendant merchant could use "customized computer software to perform reverse services from databases that contain millions of names, e-mail addresses, telephone numbers, and streets addresses, and that are indexed in a manner resembling a reverse telephone book."[11] The resulting database was used to market products to the customers and to allow the merchant to sell the complied data to other businesses. The *Pineda* Court decided that the Song-Beverly Act defined ZIP Code as part of its definition of "information concerning the cardholder."[12] Determann ably traces the many twists-and-turns in this frequently amended statute.

As a further matter, understanding California law requires setting it in the context of federal law. Health care and financial privacy law demonstrate why such an integrated analysis is necessary. HIPAA, the federal regulation for health care privacy, places numerous obligations on "covered entities," which include health plan operators, health care providers, employers who operate health insurance plans, and many other parties who have access to electronic health care insurance. HIPAA does not preempt stricter state laws, however, and California's Confidentiality of Medical Information Act (CMIA), which predates HIPAA by over a decade, is one such statute. CMIA also extends far more broadly than HIPAA; it covers "[a]ny business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information" as a "provider of health care."[13] This state health care privacy statute contains specific requirements for employee health information as well as detailed obligations for valid authorization for disclosure of health information, including typeface-size requirements.

10. *Pineda v. Williams-Sonoma Stores*, 246 P.3d 612 (Cal. 2011).
11. *Pineda v. Williams-Sonoma Stores*, 246 P.3d 615 (Cal. 2011).
12. *Pineda v. Williams-Sonoma Stores*, 246 P.3d 616 (Cal. 2011).
13. Cal. Civ. Code § 56.06(b).

A similar interplay occurs between federal and state law for financial privacy. At the federal level, the Gramm-Leach-Bliley Act ("GLB Act") regulates the use by "financial institutions" of the "nonpublic personal information" of consumers. It does not generally preempt state laws that provide greater privacy protection, and California's Financial Privacy Act ("FIPA") does have stricter requirements in certain areas. Unlike the federal law, FIPA requires opt-out notices before information sharing with affiliated institutions. As in California's CMIA, FIPA contains highly specific requirements for the mandated forms in which information is to be provided to consumers.

In its final sections, Determann's CALIFORNIA PRIVACY LAW provides a host of practical suggestions regarding privacy compliance; drafting policy policies and other privacy documentation; and risk mitigation. One of the most interesting aspects of the compliance part of this book is the author's perceptive analysis of consent issues. Pursuant to both Californian and federal statutes, the consent of affected parties is needed before certain specific kinds of personal data use. Under other laws, consent is optional but can release a company from extensive disclosure requirements. Determann points out both the benefits of obtaining consent and the possible risks of such a seemingly risk-averse policy.[14] As he notes, consent, once obtained, must be documented and may even require authentication steps regarding the identity of the party from whom consent is sought.[15] An existing business relationship may be disrupted if consent is sought. Seeking consent may require development of a process to seek new or additional consent should the terms of processing change. In short, there can be considerable costs to obtaining consent where it is not strictly required by law.

III

Privacy lawyers are well advised to keep an eye on developments in Sacramento, the California state capitol. Determann's CALIFORNIA PRIVACY LAW is a tour-de-force guide to the most important state

14. Lothar Determann, California Privacy Law, Chapter 5 § 5-2:1 (2nd Ed. 2017).
15. Lothar Determann, California Privacy Law, Chapter 5 § 5-2:1 (2nd Ed. 2017).

privacy law in the world. It also provides a host of practical advice into do's and don't's in a broad range of compliance issues. Privacy lawyers and practitioners are fortunate to have this up-to-date treasure of insight and advice.

Paul M. Schwartz
Professor of Law
Berkeley Law School