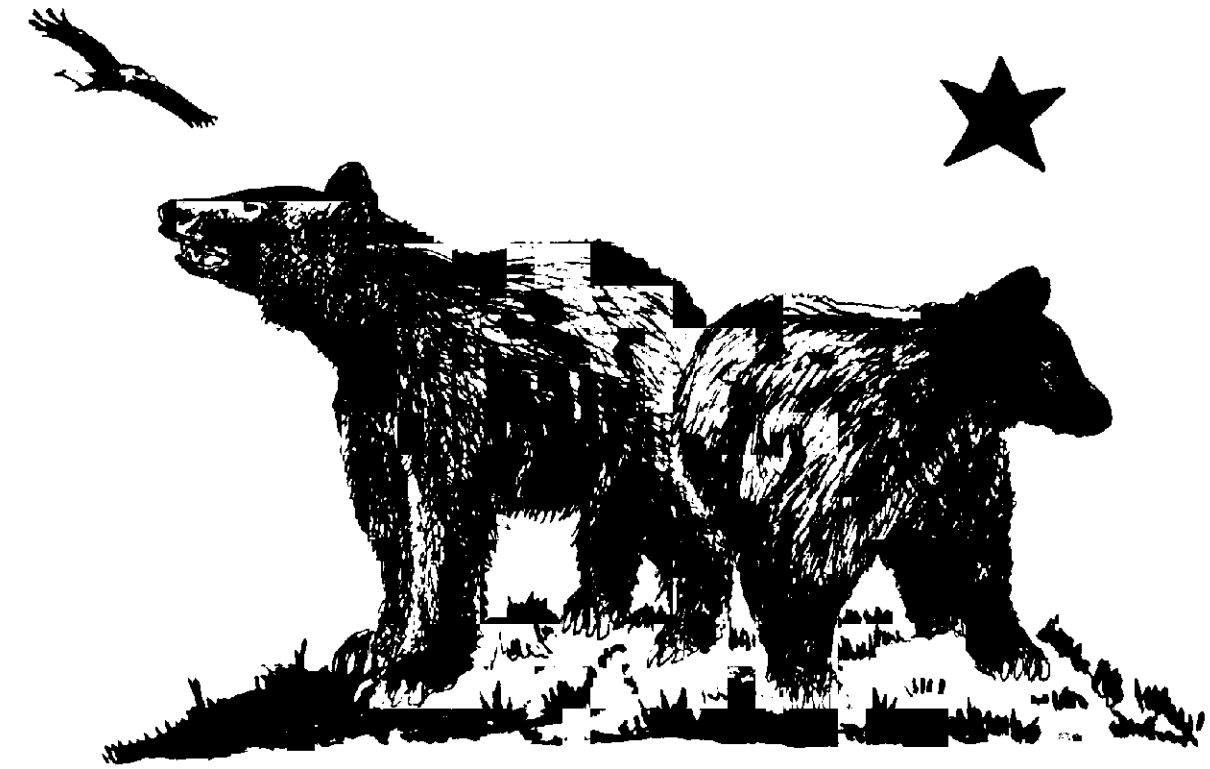
CALIFORNIA
PRIVACY LAW



Lothar Determann

Practical Guide and Commentary
U.S. Federal and California Law

Fifth Edition, 2023

An iapp publication

California Privacy Law

Practical Guide and Commentary
U.S. Federal and California Law

Fifth Edition

Lothar Determann

Published by the International Association of Privacy Professionals (IAPP)

Portrait of author by Anne Determann
Cover artwork by Lothar Determann

ISBN: 978-1-948771-73-3

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 fourth-largest economy in the world. For companies within the United States and 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 an initial example of the California Effect. Since California enacted the first data breach statute in 2002, all other states have now passed such legislation. In the HITECH Act of 2009, moreover, 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). Data breach notification is an idea from California that has swept the nation.

California privacy policy innovations have also 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 of 2016, which took effect 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]

More recently, California has enacted and amended the California Consumer Privacy Act (CCPA). In the words of Lothar Determann, this law "broke with the U.S. tradition of narrowly crafted, harm-based, sector- and situation-specific privacy laws and moved in the direction of omnibus regulation of data processing."[4] California has taken a decisive step in changing the national conversation around information privacy regulation. As Anupam Chander and co-authors have noted, this law has served as a decisive catalyst for other states.[5] In their view, California privacy law represents the efforts of individual norm entrepreneurs who have harnessed the state legislative process to produce the CCPA, which, in turn, has exercised a strong influence of this model on other states.[6]

During the current era of gridlock in Washington, the role of California is more important than ever. Until recently, the California Effect served as the first part of a regulatory cycle. Typically, after legislative action in this state and perhaps other ones, regulated entities would seek relief through a "flight to Washington."[7] Congress would respond to developments at the state level with laws that, at their best, consolidated, corrected, and improved the initial state efforts at regulation.

---

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

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 Lothar Determann, *California Privacy Law*, Chapter 2, §2.4 (4th ed. 2023).

5 Anupam Chander et al., *Catalyzing Privacy Law*, 105 Minn. L. Rev. 1733 (2021).

6 Anupam Chander et al., *Catalyzing Privacy Law*, 105 Minn. L. Rev. 1733, 1781 (2021).

7 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).

Today, however, there is entrenched gridlock in Washington for privacy and other policy areas. Congress is setting new records for its lack of productivity and struggling to carry out the most basic tasks, including, at times, the task of enacting a federal budget. Congress has also been 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 lack of activity in D.C., state privacy law, in general, and the California Effect, in particular, are more important than ever. In turn, the California legislature has proven eager and able to enact new legislation. As Determann's *California Privacy Law* demonstrates, the resulting legal approach in the Golden State is both highly complex and 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

In California and elsewhere in the United States, information privacy law traditionally consisted of a patchwork of sectoral privacy laws. A sectoral law, whether state or federal, typically regulates only a narrow area of the use of personal data processing. The game changer in this regard has been the CCPA, which took effect in 2020. This new California law represents a significant movement towards a European-style "omnibus" privacy statute – at least in certain regards. And, as noted above, this statute already is playing a strong role in catalyzing and influencing other state privacy laws.[8]

The CCPA broadens the typical approach of federal and state privacy law. It extends the classic sectoral orientation of the United States by reaching more entities than the typical sectoral law and by expanding the set of required fair information practices. It regulates personal information use by for-profit businesses that satisfy one or more of an enumerated threshold list. Its jurisdictional triggers look to whether a company has gross revenues over $25 million; buys, sells, or shares the information of 100,000 or more consumers; or derives 50 percent

8 Anupam Chander et al., Catalyzing Privacy Law, 105 Minn. L. Rev. 1733 (2021).

or more of annual revenues through the sale or sharing of personal information.

The CCPA also guarantees an expanded range of consumer rights compared to a typical U.S. privacy law or the preceding regulations in California or other states. Under the CCPA, a consumer has legal rights to access and correct her information; to "port" personal information from one company to another; and to opt-out from processing and from the sale of her personal information. The CCPA also guarantees a right to deletion, subject to certain exceptions, of the personal information that a business stores on a consumer. Further, it prohibits a business from discriminating against a consumer who exercises her rights under the law. The CCPA provides protection for children's information by prohibiting the selling of personal information of a consumer who is under 16 years of age without consent. Finally, the definition of "personal information" in the CCPA is quite broad—indeed, it reaches more data than even the GDPR.

One of the most important aspects of the CCPA is how it navigates the complicated terrain between anti-discrimination provisions and the permissibility of data sale. The CCPA generally prohibits discrimination against California residents who exercise their interests under the statute, including their rights of access, data erasure and data portability. But regulated companies may provide a different price, rate or quality in their services to a consumer when the difference is reasonably related to the value of a consumer's data.[9] Regulations are currently being formulated to provide guidelines as to when such data trades meet this test. In this area, California is in advance of the GDPR and European law in structuring a privacy-promotive framework for data trade.

As for private rights of action, the CCPA permits this kind of enforcement only as regards its data breach provisions. The CCPA gives the essential role for enforcement to both the California Attorney General and a new entity, the California Privacy Protection Agency. As Determann explains, the California Attorney General has the power to bring civil enforcement actions in court, and the CPPA to bring administrative enforcement actions.[10] The law permits significant

9 Lothar Determann, California Privacy Law, Chapter 2 §2-4.2.5 (4th ed. 2023).

10 Lothar Determann, *California Privacy Law*, Chapter 2 §2-2.2.2.1 (4th ed. 2023).

civil enforcement penalties of up to $2,500 for each violation and up to $7,500 "for each intentional violation." The CCPA also permits regulated entities to request an attorney general opinion on CCPA compliance.

In Determann's view, this law places considerable new burdens on businesses. He observes that in its aftermath businesses face a California law that combines the worst aspects of EU and U.S. regulatory approaches; he points to "extremely broad regulation of data processing in the CCPA plus myriad sector-, situation- and harm-specific privacy laws, which overlap with the CCPA."[11] Adding to the high stakes, regulations for the CCPA are still being finalized.

III

A further compliance 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. 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.

As a further matter, understanding California law requires setting it in the context of federal law. One of the strongest aspects of Determann's California Privacy Law is its seamless integration of federal and California privacy law. In myriad areas, it proves impossible to understand one without the other. Health care and financial privacy law alike demonstrate why such an integrated analysis is indispensable. 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

11 Lothar Determann, *California Privacy Law*, Chapter 1 §1-5:4 (4th ed. 2023).

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."[12] 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.

A similar interplay occurs between federal and state law for financial privacy. At the federal level, the Gramm-Leach-Bliley Act (GLBA) 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, for example, FIPA requires opt-out notices before information sharing with affiliated institutions. As in California's CMIA, FIPA also contains highly specific requirements for the mandated forms in which information is to be provided to consumers.

Determann's *California Privacy Law* also provides a host of practical suggestions regarding privacy compliance; the drafting of policy policies and other privacy documentation; and achieving risk mitigation. One of the most interesting aspects of the compliance section 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.[13] As he notes, consent, once obtained, must be documented and may require authentication steps regarding the identity of the party from whom consent is sought.[14] But there can be considerable costs to obtaining consent where it is not strictly required by law. An existing business relationship may be disrupted

12 Cal. Civ. Code § 56.06(b).

13 Lothar Determann, *California Privacy Law*, Chapter 5 § 5-2:1 (4th Ed. 2023).

14 Lothar Determann, *California Privacy Law*, Chapter 5 § 5-2:1 (4th Ed. 2023).

if consent is sought. Seeking consent may require development of a process to seek new or additional consent should the terms of processing change.

IV

Privacy lawyers are well advised to keep an eye on developments in Sacramento, the California state capital. Determann's *California Privacy Law* provides peerless assistance in doing so; it is a tour-de-force guide to the most important state privacy law in the world. It also provides a host of practical advice through dos and don'ts regarding 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
Jefferson E. Peyser Professor of Law
Berkeley Law School