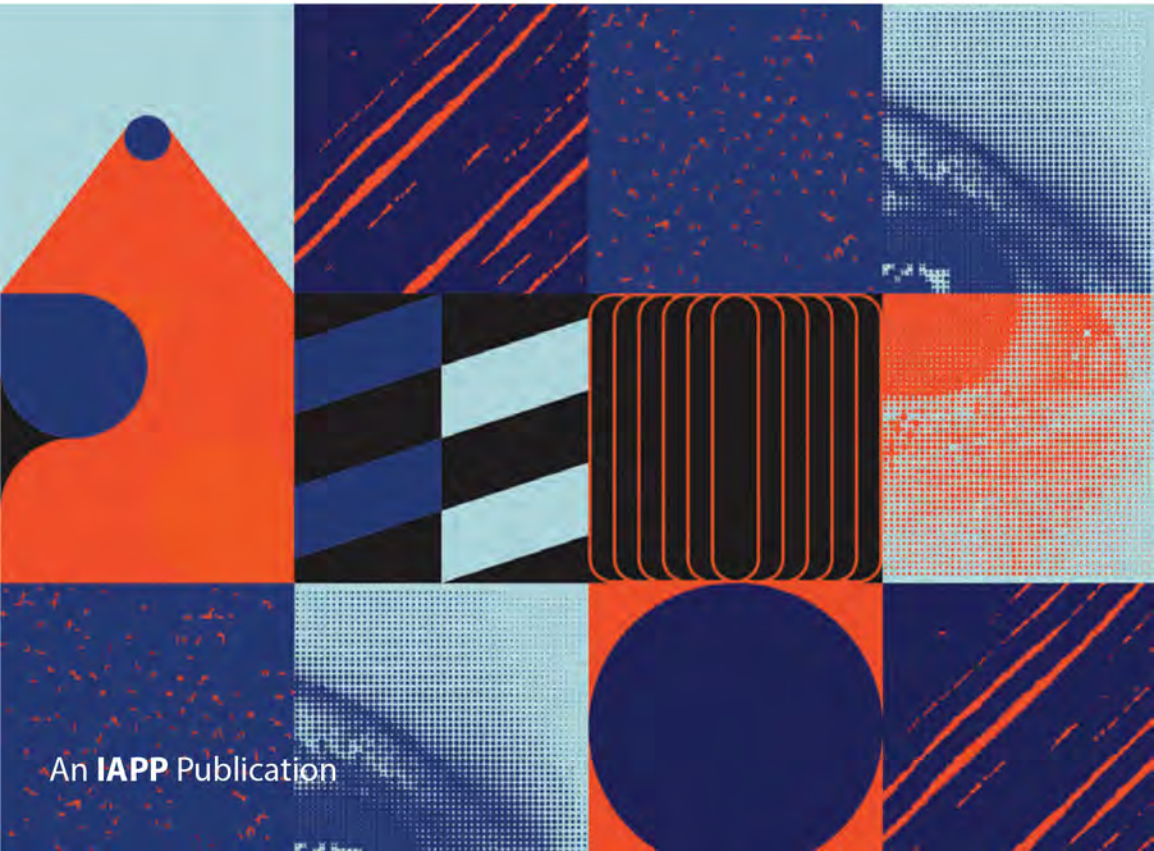
2024
Seventh Edition

Daniel J. Solove & Paul M. Schwartz

PRIVACY LAW FUNDAMENTALS



An **IAPP** Publication

Privacy Law Fundamentals

Seventh Edition, 2024

Daniel J. Solove
John Marshall Harlan Research Professor of Law
George Washington University Law School
&
Paul M. Schwartz
Jefferson E. Peyser Professor of Law
U.C. Berkeley School of Law

An IAPP Publication

ISBN 978-1-948771-78-8

ABOUT *PRIVACY LAW FUNDAMENTALS*

"This book is an indispensable guide for privacy and data protection practitioners, students, and scholars. You will find yourself consulting it regularly, as I do. It is a must for your bookshelf."

—Danielle Citron, University of Virginia

"The go-to privacy law reference that you will keep going to. Professors Schwartz and Solove manage to distill without distorting and to outline without obscuring. Part reference, part primer and part pathfinder, *Privacy Law Fundamentals* is the ultimate privacy law resource."

—Tom Counts, Paul Hastings

"Two giants of privacy scholarship succeed in distilling their legal expertise into an essential guide for a broad range of the legal community. Whether used to learn the basics or for quick reference, *Privacy Law Fundamentals* proves to be concise and authoritative."

—Jules Polonetsky, Future of Privacy Forum

"*Privacy Law Fundamentals* is a must-read for privacy practitioners to keep up and gain a clear and succinct picture of where the law is and where it is heading around the world and across different industries."

—Lindsey Tonsager, Covington & Burling

"There are no better-qualified authors than Professors Schwartz and Solove to summarize the current state of privacy law and, as a result, there is no better compact privacy law resource than *Privacy Law Fundamentals*"

—Christopher Wolf, Hogan Lovells

ABOUT THE AUTHORS

Daniel J. Solove is the Eugene L. and Barbara A. Bernard Professor of Intellectual Property and Technology Law at the George Washington University Law School. He is also the president and CEO of TeachPrivacy, www.teachprivacy.com, a company that provides privacy and data security training to organizations in an array of industries.

One of the world's leading experts in privacy law, Solove is the author of numerous books, including *Breached: Why Data Security Fails and How to Improve It* (2022)(with Woodrow Hartzog), *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale 2011), *Understanding Privacy* (Harvard 2008), *The Future of Reputation: Gossip and Rumor in the Information Age* (Yale 2007; winner of the 2007 McGannon Award), and *The Digital Person: Technology and Privacy in the Information Age* (NYU 2004). Solove is also the co-author (with Paul Schwartz) of a textbook, *Information Privacy Law,* with Aspen Publishing Co., now in its eighth edition.

Additionally, he is the author of several other textbooks, including *Privacy and the Media* (Aspen 2024), *Privacy, Law Enforcement, and National Security* (Aspen 2024), *Consumer Privacy and Data Protection* (Aspen 2024), and *EU Data Protection and the GDPR* (Aspen 2024), all with Paul Schwartz. He has published more than 100 articles and essays.

Solove has testified before the US Congress and has been involved as an expert and consultant in a number of high-profile privacy cases. His work has been cited by many federal and state courts, including the US Supreme Court. He has been interviewed and featured in several hundred media broadcasts and articles in publications and on networks, including *The New York Times, The Wall Street Journal, The Washington Post, Chicago Tribune, USA Today, Time, Newsweek, People, Reader's Digest,* The Associated Press, ABC, CBS, NBC, CNN, NPR, and C-SPAN's "Book TV."

More information about Solove's work can be found at www.danielsolove.com. He blogs at Privacy+Security Blog, www.teachprivacy.com/privacy-security-training-blog/. As one of a select group of "Influencers," Solove has more than 1 million LinkedIn followers.

Paul M. Schwartz is the Jefferson E. Peyser Professor of Law at the UC Berkeley School of Law and a director of the Berkeley Center for Law & Technology. A leading international expert on informational privacy and information law, he has published widely on these topics. In the United States, his articles and essays have appeared in periodicals such as the *Harvard Law Review, Yale Law Journal, Stanford Law Review, Columbia Law Review, California Law Review, N.Y.U. Law Review,* and *Chicago Law Review.* With Daniel Solove, he has published the leading casebook *Information Privacy Law* (Aspen, 8th edition, 2024) and other books.

Schwartz has testified as an expert before congressional committees in the United States and provided legal reports to the Commission of the European Community and Department of Justice, Canada. He has assisted numerous corporations in the United States and abroad with information privacy and cybersecurity issues.

A member of the American Law Institute (ALI), Schwartz was co-reporter with Daniel Solove on the ALI's Principles of Law, Data Privacy (2020). He has received scholarships and grants from the American Academy in Berlin, where he was a Berlin Prize Fellow; the Alexander von Humboldt Foundation; German Marshall Fund; Fulbright Foundation; the German Academic Exchange; and the Harry Frank Guggenheim Foundation. He is a member of the organizing committee of the Privacy Law Salon and co-organizer with Daniel Solove of the Privacy + Security Forum.

Schwartz belongs to the editorial boards of *International Data Privacy Law, the International Journal of Law and Information Technology,* and the *Zeitschrift für Datenschutz* (Data Protection Journal). His homepage is www.paulschwartz.net.

DEDICATION

In memory of Joel Reidenberg and Kurt Wimmer,
two great figures in privacy law and two cherished friends.

To Pamela and Griffin —DJS

To Steffie, Clara, and Leo —PMS

PREFACE

This book provides a concise guide to privacy law. *Privacy Law Fundamentals* is designed to serve as a primer of the essential information one needs to know about the field. For the student of privacy law or the beginning privacy professional, the book will provide an overview that can be digested readily. For the more seasoned and experienced, the book will serve as a handy reference guide, a way to refresh one's memory of key components of privacy laws and central cases. It will help close gaps in knowledge and inform on areas of the field about which one wants to know more.

In writing this book, we have aimed to avoid the "too much information" problem by singling out the essential provisions of law, regulations, and judicial decisions. A frequent risk in law books is that key definitions, provisions, and concepts will become lost in a litany of long and dense statutes and in a mass of cases. We have endeavored to distill the field down to its fundamentals and present this information in as clear and useful a manner as we could. Wherever possible, we have developed charts and lists to convey the material. The book is organized in twelve chapters:

- Chapter 1—an overview of privacy law in all its varied types and forms and a timeline with key points in the development of privacy law.

- Chapter 2—privacy law involving the media, including the privacy torts, defamation, and the First Amendment.

- Chapter 3—the law of domestic law enforcement, focusing on the Fourth Amendment and the statutes regulating electronic surveillance.

- Chapter 4—national security law, including the US Foreign Intelligence Surveillance Act (FISA).

- Chapter 5—laws and regulations that pertain to health and genetic data, including the US Health Insurance Portability and Accountability Act (HIPAA).

- Chapter 6—government records and laws, such as the Privacy Act and the Freedom of Information Act (FOIA).

- Chapter 7—laws concerning financial information, including the Fair Credit Reporting Act (FCRA) and Gramm-Leach-Bliley Act (GLBA).

- Chapter 8—legal regulation of the privacy of consumer data and business records, involving statutes, tort protections, and US Federal Trade Commission (FTC) enforcement actions.

- Chapter 9—data security law, including the varying laws in all the states.

- Chapter 10—school privacy, including the Family Educational Rights and Privacy Act (FERPA).

- Chapter 11—regulation of employment privacy, including the different rules for government and private sector employees.

- Chapter 12—international privacy law, including the EU General Data Protection Regulation (GDPR), the Organisation for Economic Co-operation and Development (OECD) Guidelines, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, and rules of international data transfers.

Through its different editions, this book benefitted greatly from the research assistance of a dream team of students. These are Lorraine Abdulahad, Deborah Choi, Luisa Domenichini, Robert Fairbanks, David Fang, Russell Fink, Natalie Heim, Joey Kingerski, Charlotte Kress, Annie Lee, Brittany Johnson, Harris Mateen, Meet Mehta, Gregory Merchant, Michelle Park, Sanjana Parikh, Amelie Raepple, Sarah Suwanda, Sophia Wallach, Kevin Yang, and Andy Zachrich.

For further references, including books, websites, statutes, and other sources of news and legal materials, visit our website (www.informationprivacylaw.com), and for our casebooks, click on the "Resources" tab at the top.

We look forward to keeping this book up to date and finding additional ways to make it as useful as possible. Please feel free to contact us with any suggestions and feedback about the book.

In 2021, Joel Reidenberg and Kurt Wimmer, two leaders of data privacy law, passed away. Both were cherished friends of the authors of this volume and of so many in our field. Joel Reidenberg was a distinguished professor at Fordham Law School and a leader in international privacy law. Kurt Wimmer led the privacy and cybersecurity practice at Covington and advanced press freedom in his pro bono work. We wish to dedicate this volume to them.

Daniel J. Solove
Washington, DC
dsolove@law.gwu.edu

Paul M. Schwartz
Berkeley, CA
pschwartz@law.berkeley.edu

TABLE OF CONTENTS

CHAPTER 1

An Overview of Privacy Law

ESSENTIAL POINTS

- Information privacy law is a relatively youthful area of law. New developments are still shaping it and changing its form. For example, data breach notification statutes in the United States date only to 2003.
- The development of privacy law in the United States may also be viewed as a dialogue between the courts and legislature about the scope and application of the legal concept of privacy. In some matters, courts will define new privacy rights. In others, the courts will leave the job to the legislature.
- Privacy problems occur in particular contexts, and different types of problems involve different trade-offs and concerns.
- Technology plays an especially important role in shaping the kinds of privacy concerns that society faces and the role of the law.
- In Europe and most of the rest of the world, this area is called data protection law. International developments have played a highly visible and important part in shaping the role of privacy professionals and the privacy dialogue within the United States.

TYPES OF PRIVACY LAW

Torts

In the United States, tort law is primarily state law. As a result, the particular boundaries of this area of law differ from state to state—sometimes dramatically. For example, some states recognize all four privacy interests, but Minnesota accepts only three of the four. It does not recognize the false light tort. *Lake v. Wal-Mart Stores, Inc.,* 582 N.W.2d 231 (Minn. 1998).

TORTS MOST COMMONLY INVOLVED IN PRIVACY CASES

- Invasion of privacy (a collective term for the four privacy torts)
  - Public disclosure of private facts
  - Intrusion upon seclusion
  - False light
  - Appropriation of name or likeness
- Breach of confidentiality
- Intentional infliction of emotional distress
- Defamation
  - Libel
  - Slander
- Negligence

ORIGINS OF THE PRIVACY TORTS

Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890)

This foundational article, which inspired the development of privacy law in the twentieth century, argued that the common law protected privacy as "the right to be let alone."

William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960)
Legendary torts scholar William Prosser surveyed all the common law privacy tort cases and identified the central four interests protected. His formulations of the privacy torts remain in widespread use today. The states have widely adopted Prosser's four privacy torts.

Contract/Promissory Estoppel

Confidentiality or other privacy protections can be express or implied contractual terms in a relationship. Promises to protect privacy might be enforced through promissory estoppel.

Criminal Law

Many privacy laws have criminal penalties. Many states have criminalized blackmail, "Peeping Tom" activity, or the surreptitious capture of nude images.

Evidentiary Privileges

In evidence law, many privileges protect the confidentiality of information shared within certain relationships, such as attorney-client and patient-physician.

Federal Constitutional Law

WAYS THE US CONSTITUTION PROTECTS PRIVACY

- The First Amendment right to speak anonymously
- The First Amendment freedom of association, which protects the privacy of one's associations
- The Third Amendment protection of the home from the quartering of troops
- The Fourth Amendment protection against unreasonable searches and seizures
- The Fifth Amendment privilege against self-incrimination
- The constitutional right to privacy
- The constitutional right to information privacy

State Constitutional Law

A number of states have directly provided for the protection of privacy in their constitutions. For example, Cal. Const. art. I, § 1 stipulates: "All people are by their nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness and privacy."

STATES WITH EXPRESS CONSTITUTIONAL PRIVACY PROTECTION			
AK	Alaska Const. art. I, § 22	**IL**	Ill. Const. art. I, § 6
AZ	Ariz. Const. art. II, § 8	**LA**	La. Const. art. I, § 5
CA	Cal. Const. art. I, § 1	**MT**	Mt. Const. art. II, § 10
FL	Fla. Const. art. I, § 23	**SC**	S.C. Const. art. I, § 10
HI	Hawai'i Const. art. I, § 23	**WA**	Wash. Const. art. I, § 7

Federal Statutory Law

- **Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C. §§ 1681 *et seq.*—** provides citizens with rights regarding the use and disclosure of their personal information by consumer reporting agencies.
- **Bank Secrecy Act of 1970, Pub. L. No. 91-508**—requires banks to maintain reports of people's financial transactions to assist in government white-collar investigations.
- **Privacy Act of 1974, 5 U.S.C. § 552a**—provides individuals with a number of rights concerning their personal information maintained in government record systems by federal agencies, such as the right to see one's records and ensure the information in them is accurate.
- **Family Educational Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. §§ 1221 note, 1232g**—protects the privacy of school records.
- **Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422**—requires a subpoena or search warrant for law enforcement officials to obtain financial records.
- **Foreign Intelligence Surveillance Act (FISA) of 1978, 15 U.S.C. §§ 1801–1811**—regulates foreign intelligence gathering within the United States.
- **Privacy Protection Act (PPA) of 1980, 42 U.S.C. § 2000aa**—restricts the government's ability to search and seize the work product of the press and media.
- **Cable Communications Policy Act of 1984, 47 U.S.C. § 551**—mandates privacy protection for records maintained by cable companies.
- **Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709**—contains three distinct statutes that regulate electronic surveillance law: the Wiretap Act, Stored Communications Act, and Pen Register Act. The Wiretap Act was first enacted in 1968 as Title III of the Omnibus Crime Control and Safe Streets Act.
- **Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a**—regulates automated investigations conducted by federal agencies carrying out automatic matching on computer files with other federal agencies or non-federal entities.
- **Employee Polygraph Protection Act of 1988, 29 U.S.C. §§ 2001–2009**—governs the use of polygraphs by employers.
- **Video Privacy Protection Act (VPPA) of 1988, 18 U.S.C. §§ 2710–2711**—protects the privacy of prerecorded videotapes, cassette tapes, or similar audio visual materials.
- **Telephone Consumer Protection Act (TCPA) of 1991, 47 U.S.C. § 227**—provides certain remedies for repeat telephone calls by telemarketers.
- **Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725**—restricts the states from disclosing or selling personal information from their motor vehicle records.

- **Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103–414**—requires telecommunications providers to help facilitate government interceptions of communications and surveillance.
- **Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104–193**—requires the collection of personal information (including Social Security numbers, addresses, and wages) of all people who obtain a new job anywhere in the nation. The resulting information is placed into a national database to help government officials track down parents with outstanding child support payments.
- **Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104–191**—gives the Department of Health and Human Services (HHS) the authority to promulgate regulations governing the privacy of medical records. These regulations, the HIPAA Privacy Rule, were initially finalized in 2000 with modifications made in subsequent years. 45 C.F.R. 160, 162, and 164.
- **Identity Theft and Assumption Deterrence Act (ITADA) of 1998, 18 U.S.C. § 1028**—criminalizes the transfer or use of fraudulent identification with the intent to commit unlawful activity.
- **Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. §§ 6501–6506**—restricts internet websites' use of information gathered from children under age 13.
- **Gramm-Leach-Bliley Act (GLBA) of 1999, 15 U.S.C. §§ 6801–6809**—requires privacy notices and provides opt-out rights when financial institutions seek to disclose personal data to other companies.
- **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) of 2001, Pub. L. No. 107–56**—amends a number of electronic surveillance statutes and other statutes to facilitate law enforcement investigations and access to information.
- **Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) of 2003, Pub. L. No. 180–187**—provides penalties for the transmission of unsolicited email.
- **Video Voyeurism Prevention Act of 2004, 18 U.S.C § 1801**—criminalizes the capturing of nude images of people (when on federal property) under circumstances where they have a reasonable expectation of privacy.
- **FISA Amendments Act of 2008, Pub. L. No. 110–261**—amends FISA to add a new title creating additional procedures concerning the acquisition of information about certain persons outside the United States.

State Statutory Law

Much of privacy law is found in state law. Privacy tort law and data breach notification statutes are predominately state law. In addition, numerous federal statutes permit state laws to exceed their specifications. This issue is regulated under the rubric of "preemption." In Chapter 9, we provide a chart that lists the federal statutes that preempt state laws and those that do not. The US regulation of privacy is best thought of as a dual federal-state system.

Areas of State Legislation on Privacy

Substantial state legislation on privacy exists in the following areas:

Law Enforcement

- Wiretapping and electronic surveillance

Medical and Genetic Information

- Confidentiality of medical information
- Genetic privacy

Government Records

- Public records
- State agency use and disclosure of personal information

Financial Privacy

- Banking privacy
- Consumer reports
- Security freeze

Consumer Data and Business Records

- Biometrics
- Sale of personal data
- Spam
- Spyware and phishing
- Telecommunications privacy
- Pretexting
- Use of Social Security numbers
- Data disposal
- Video privacy
- Radio frequency identification (RFID) and tracking devices
- Restrictions on internet service providers (ISPs)
- Unauthorized access to computers and networks

Data Security

- Identity theft
- Data security breach notification
- Substantive security standards
- Data disposal

Employment

- State employee personal information
- Restrictions on employment application questions

International Law

Around the world, numerous countries have endeavored to protect privacy in their laws. There are two general approaches toward protecting privacy:

Omnibus: A comprehensive approach to protecting privacy that covers personal data across all industries and most contexts. Sometimes a single omnibus law will also regulate the public and private sectors.

1. *Sectoral*: Regulates information on a sector-by-sector basis. Different industries receive different regulation, and some contexts are not regulated at all. Different statutes regulate the public and private sectors.

The world's first comprehensive information privacy statute was a state law; the Hessian Parliament enacted this statute in Wiesbaden, Germany, on September 30, 1970. Like most European data protection laws, this statute is an omnibus law. Note, however, that the European Union today relies on a mixture of omnibus and sectoral laws. The General Data Protection Regulation (GDPR) is an omnibus law and one that is supplemented by sectoral laws from the European Union, such as the ePrivacy Directive, and from the member states.

In contrast, the United States has generally relied on regulation of information use on a sector-by-sector basis. For example, COPPA provides privacy protection for children on the web, but there is no such federal law that generally regulates privacy for adults on the web. An important recent trend in the United States, however, has been state privacy laws that more generally protect consumer privacy.

Outside of Europe and the United States, there are many information privacy statutes in the rest of the world. Most countries have adopted the European Union's approach by enacting omnibus laws that are similar to the GDPR and supplementing their omnibus statutes with targeted sector laws.

There are also important international and transnational accords, guidelines, treaties, directives, and agreements. These include:

- Organisation of Economic Co-operation and Development (OECD) Guidelines (1980), with additional, supplemental OECD Guidelines (2013)

- Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data (1981), modernized in 2018
- Asia-Pacific Economic Cooperative (APEC) Privacy Framework (2004)

THE CHIEF PRIVACY OFFICER OR DATA PROTECTION OFFICER

The chief privacy officer (CPO) is now a mainstay at many large organizations. Among other things, a CPO ensures the organization is complying with the law, employees are trained about privacy and security practices, and the organization has an effective privacy policy. In the European Union and other countries around the world, there are data protection officers (DPOs), which have similar functions to CPOs.

In the public sector, the Homeland Security Act of 2002 established a privacy officer within the Department of Homeland Security (DHS). 6 U.S.C. § 142. This statute created the first explicit legal requirement in federal law for a privacy officer in the US government. Previously, the Clinton administration had appointed a chief counselor for privacy and located this position in the Office of Management and Budget's (OMB) Office of Information and Regulatory Affairs (OIRA).

In 2002, Congress also enacted the E-Government Act, which requires administrative agencies to conduct privacy impact assessments (PIAs).

In the private sector, regulations enacted pursuant to HIPAA require "a covered entity" to "designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity." 45 C.F.R. 164.30(a)(1)(i).

As part of its role implementing the GLBA, the Federal Trade Commission (FTC) issued a Safeguards Rule that requires the designation of an employee or employees to coordinate the company's information security program. This requirement can encourage the introduction of a CPO position at organizations that do not yet have one. 16 C.F.R. Part 314.4(a), 67 Federal Register 36484 (2002). In the European Union, the General Data Protection Regulation requires public authorities and certain kinds of private sector entities to appoint a DPO. GDPR, Art. 37.

In sum, most large companies that handle personal data now have a CPO or DPO.

THE CHIEF INFORMATION SECURITY OFFICER

Similar to the development of legal requirements for CPOs, there are now data security laws that call for the naming of a single employer to be responsible for a written security plan in the organization. As a prominent example, in 2017, the New York Superintendent of Financial Services (NYSFS) promulgated a regulation establishing cybersecurity requirements for financial services companies. Due to the prominence of New York state as a center for the financial service industry, there has been a far-reaching impact for this cybersecurity regulation. Among its provisions is a requirement that all "covered entities … designate a qualified individual responsible for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policy." This individual, termed the "chief information security officer" (CISO) in the regulations, can be provided by the covered entity or by a third-party service provider. 23 CRR-NY 500.4(a).

Federal law also takes this approach. As previously noted, the FTC's Safeguards Rule, promulgated under authority granted to it by the GLBA, requires financial institutions to designate an employee or employees to coordinate the company's information security program. 16 C.F.R. 314.4(a). Revisions to the Safeguards Rule in 2017 term this individual, the "Qualified Individual." This federal requirement will continue to encourage not only the appointment of CPOs, but also of CISOs. Indeed, the Safeguards Rule spells out a long list of mandated tasks for the Qualified Individual to oversee, which will encourage appointment of a CISO and investment in an information security program at regulated entities.

THE DEVELOPMENT OF PRIVACY LAW: A TIMELINE	
Antiquity	
400 B.C.	Hippocratic Oath provides the first recorded expression of a duty of medical confidentiality.
1000–1699	
1361	England's Justices of the Peace Act criminalizes eavesdropping and peeping toms.
1604	*Semayne's Case* (1604), 77 Eng. Rep. 194, declares "the house of everyone is to him as his castle and fortress."
1700–1799	
1763	*Wilkes v. Wood* (1763), 98 Eng. Rep. 489, repudiates the use of a general warrant to search for documents relating to a pamphlet involving seditious libel. Influential in the creation of the Fourth Amendment.
1765	*Entick v. Carrington* (1765), 95 Eng. Rep. 807, is another repudiation of general warrants in a seditious libel case. Influential in the creation of the Fourth Amendment.
1789	US Constitution—the First, Third, Fourth, and Fifth Amendments safeguard different aspects of privacy.
1800–1899	
1860	US Census becomes more inquisitive. Public outcry for greater census privacy.
1877	*Ex parte Jackson*, 96 U.S. 727 (1877)—US Supreme Court holds that the Fourth Amendment protects sealed letters in the mail.
1886	*Boyd v. United States*, 116 U.S. 616 (1886)—US Supreme Court holds that the government cannot compel people to turn over documents.
1890	Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890). This article inspires the recognition during the twentieth century of privacy torts in the majority of the states.

THE DEVELOPMENT OF PRIVACY LAW: A TIMELINE	
1900–1959	
1903	US states begin to recognize privacy torts. New York enacts a law similar to Warren and Brandeis's tort of appropriation. N.Y. Civ. Rights Law §§ 50-51. Georgia Supreme Court recognizes the appropriation tort. *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68 (Ga. 1905).
1908	The US Federal Bureau of Investigation (FBI) is formed. Originally called the Bureau of Investigation.
1928	*Olmstead v. United States*, 277 U.S. 438 (1928). The US Supreme Court holds that Fourth Amendment protections do not extend to wiretapping unless there is a "trespass" involved in this activity. Now on the Supreme Court, Justice Louis Brandeis writes a famous dissent to the majority opinion.
1934	In response to *Olmstead*, US Congress enacts § 605 of the Federal Communications Act of 1934 to limit wiretapping.
1936	US Social Security system begins. Creation of the Social Security number, which is not intended to be used in other programs or as a form of identification.
1947	The US Central Intelligence Agency (CIA) is created.
1948	The Universal Declaration of Human Rights is adopted by the United Nations, protecting a right to privacy in Article 12.
1949	Publication of George Orwell's *1984*. Birth of "Big Brother."
1950	European Convention on Human Rights (ECHR) is adopted, protecting the right to privacy in Article 8.
1952	US President Harry Truman creates the National Security Agency (NSA).
1953	Seminal "right of publicity" case, *Haelan Laboratories v. Topps Chewing Gum, Inc.*, 202 F.2d 866 (2d Cir. 1953), is decided.
1960–1979	
1960	William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960).
1961	*Mapp v. Ohio*, 367 U.S. 643 (1961)—the US Supreme Court holds that the exclusionary rule for Fourth Amendment violations applies to the states.
1965	In *Griswold v. Connecticut*, 381 U.S. 479 (1965), the US Supreme Court prevents the government from banning contraceptives. The *Griswold* Court finds the Constitution protects a right to privacy through the "penumbras" of many of the ten amendments of the Bill of Rights.
1966	The US Freedom of Information Act (FOIA) is enacted, which provides for access to information held by federal agencies as well as some exceptions to disclosure, included for reasons of privacy.

THE DEVELOPMENT OF PRIVACY LAW: A TIMELINE	
1967	In *Katz v. United States*, 389 U.S. 347 (1967), the US Supreme Court finds police surveillance of a telephone booth violated the Fourth Amendment. The concurrence in the case by Justice John Marshall Harlan articulates the "reasonable expectation of privacy test," a current leading approach for determining the Fourth Amendment's applicability.
1967	Alan Westin publishes *Privacy and Freedom*.
1968	Title III of the US Omnibus Crime and Control and Safe Streets Act is passed, a major revision of electronic surveillance law. Title III is now known as the Wiretap Act.
1970	In Wiesbaden, Germany, the Hessian Parliament enacts the world's first comprehensive information privacy statute.
1970	FCRA.
1973	According to *Roe v. Wade*, 410 U.S. 113 (1973), the right to privacy "encompass[es] a woman's decision whether or not to terminate her pregnancy."
1973	The US Department of Health, Education and Welfare (HEW) issues a report, *Records, Computers, and the Rights of Citizens*, articulating the Fair Information Practices (FIPs).
1974	US Privacy Act.
1974	Federal Educational Rights and Privacy Act.
1974	Swedish Data Act.
1975	In the US Senate, the Church Committee conducts a thorough investigation of surveillance abuses by the government. A similar investigation is carried out in the House of Representatives by the Pike Committee.
1975	In *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975), the US Supreme Court recognizes some First Amendment limitations on the privacy torts.
1976	In *United States v. Miller*, 425 U.S. 435 (1976), the US Supreme Court holds that financial records possessed by third parties are not protected by the Fourth Amendment. The court articulates the "third party doctrine"—people lack a reasonable expectation of privacy in information conveyed to third parties.
1977	US Supreme Court recognizes the constitutional right to information privacy—the "individual interest in avoiding disclosure of personal matters" in *Whalen v. Roe*, 429 U.S. 589 (1977) and *Nixon v. Administrator of General Services*, 433 U.S. 425 (1977).
1977	German Federal Data Protection Act.
1978	French Data Protection Act.

THE DEVELOPMENT OF PRIVACY LAW: A TIMELINE	
1979	In *Smith v. Maryland*, 442 U.S. 735 (1979), the US Supreme Court rules the Fourth Amendment does not apply to a pen register (the telephone numbers a person dials) because of the third-party doctrine—people cannot expect privacy in their phone numbers since they expose the information to the phone company.
1980–1989	
1980	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
1981	Israel's Protection of Privacy Law.
1981	In Strasbourg, the Council of Europe releases its Convention No. 108 for the Protection of Individuals with Regard to Automatic Processing of Data, a treaty and the first binding international instrument to protect individuals "against abuses which may accompany the collection and processing of personal data."
1983	The Federal Constitutional Court of Germany identifies a "right of informational self-determination" in the Basic Law, the German constitution.
1984	UK Data Protection Act.
1986	US Congress passes the ECPA, creating the still binding statutory framework in the United States for regulating the electronic surveillance of communications.
1986	US Computer Fraud and Abuse Act (CFAA).
1988	Australia passes the Privacy Act, which is based on the OECD Guidelines.
1988	US Video Privacy Protection Act (VPPA).
1990–1999	
1992	Switzerland's Federal Law on Data Protection.
1992	Israel's Basic Law on Human Dignity and Freedom provides for a right to privacy.
1994	US Driver's Privacy Protection Act (DPPA).
1995	US Communications Decency Act (CDA).
1996	US Congress passes HIPAA. Title II of HIPAA requires the establishment of national standards for electronic data exchange and addresses issues concerning the privacy and security of health care information.
1996	The European Union promulgates the EU Data Protection Directive.
1996	Hong Kong Personal Data Ordinance.
1998	The FTC begins to bring actions against companies that violate their privacy policies.

THE DEVELOPMENT OF PRIVACY LAW: A TIMELINE	
1998	COPPA.
1999	Chile becomes the first country in South America to enact a data protection law.
2000–2009	
2000	The Safe Harbor Agreement is established between the United States and European Union for data sharing under the EU Data Protection Directive.
2000	Argentina enacts a comprehensive data protection statute: the Law for the Protection of Personal Data. The EU Data Protection Directive strongly influences the Argentinean statute.
2001	USA Patriot Act.
2001	Personal Information Protection and Electronic Documents Act (PIPEDA) takes effect in Canada.
2001	*Kyllo v. United States*, 533 U.S. 27 (2001)—the US Supreme Court holds that the Fourth Amendment requires a warrant and probable cause before the government can use thermal sensors to detect activity in people's homes.
2002	HHS issues final modifications to the HIPAA Privacy Rule.
2003	Japan enacts the Personal Data Protection Act (PDPA).
2004	APEC Privacy Framework.
2004	The European Court of Human Rights decides *Von Hannover v. Germany*, 2004-VI Eur. Ct. H.R. 41, recognizing privacy rights in certain public settings.
2005	ChoicePoint, one of the largest data brokers, announces it sold personal data on more than 145,000 people to fraudulent companies established by a ring of identity thieves. Subsequently, numerous companies and organizations begin disclosing data security breaches. States begin to enact data security breach notification legislation in response.
2009	US Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009, establishes a breach notification requirement for "covered entities" under HIPAA. It also extends HIPAA's requirements for privacy and information security to the business associates of covered entities.
2010–2019	
2010	32nd International Conference of Data Protection and Privacy Commissioners held in Jerusalem. One adopted resolution, proposed by the Information and Privacy Commissioner of Ontario (Canada), calls for adoption of privacy by design within organizations in order to make privacy a default mode of operation.

THE DEVELOPMENT OF PRIVACY LAW: A TIMELINE	
2010	Mexico enacts the Federal Law for the Protection of Personal Data.
2012	In *United States v. Jones*, 132 S. Ct. 945 (2012), the US Supreme Court finds that law enforcement's installation of a GPS device to a car without a warrant is a search under the Fourth Amendment.
2012	European Commission proposes GDPR.
2013	HHS issues HIPAA Omnibus Final Rule.
2013	In *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), the US Supreme Court denies standing to challengers of NSA surveillance.
2013	Edward Snowden leaks classified documents detailing numerous broad surveillance programs by the NSA.
2013	FTC issues Amendments to the COPPA Rule (July 2013).
2013	Supplemental, additional OECD Privacy Guidelines released.
2014	FTC celebrates 100th birthday.
2014	Several large data security breaches are announced by major retailers, including Target, Neiman Marcus, Home Depot, Kmart, and others.
2014	In *Riley v. California,* 134 S. Ct. 2473 (2014), the US Supreme Court holds that a warrant is generally required to search digital information on a cellphone seized pursuant to an individual's arrest.
2014	InBloom closes (in part) due to privacy concerns. Numerous states enact new privacy laws for K-12 students.
2014	In Case C-131/12, *Google Spain SL v. Agencia Española de Protección da Datos* (May 13, 2014), the Court of Justice of the European Union (CJEU) requires a search engine to remove a link to a search result that violates the "right to be forgotten."
2015	In *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015), the FTC wins a case posing the most significant challenge thus far to the FTC's regulatory authority. The US Court of Appeals for the Third Circuit holds that the FTC has broad powers to regulate data security under the FTC Act.
2015	In Case C-362/14, *Schrems v. Data Protection Commissioner* (Oct. 6, 2015) (*Schrems I*), the CJEU invalidates the Safe Harbor agreement.
2016	The GDPR is published in the EU Office Journal on May 24, 2016.
2016	The EU-US Privacy Shield, the successor to the Safe Harbor, enters into force on July 12, 2016.
2018	The GDPR becomes binding on May 25, 2018.
2018	California enacts the California Consumer Protection Act (CCPA).

THE DEVELOPMENT OF PRIVACY LAW: A TIMELINE	
2018	In *Carpenter v. United States*, 138 S. Ct. 2206 (U.S. 2018), the US Supreme Court provides limits to the third-party doctrine under the Fourth Amendment.
2019	The FTC issues a $5 billion fine against Facebook in connection with the Cambridge Analytica incident, the largest fine the FTC has issued for privacy violations.
2020–Present	
2020	In Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (July 16, 2020) (*Schrems II*), the CJEU invalidates the EU-US Privacy Shield Framework and holds that even with standard contractual clauses (SCCs) or binding corporate rules (BCRs), additional measures might be needed to address government surveillance.
2020	In August 2020, Brazil's comprehensive privacy law, the Lei Geral de Proteção de Dados Pessoais (LGPD), goes into effect.
2020	California passes the California Privacy Rights Act (CPRA) by referendum. The act strengthens the CCPA and creates an independent privacy enforcement agency, the California Privacy Protection Agency (CPPA).
2021	Virginia and Colorado pass broad consumer privacy laws using the CCPA as a model.
2021	China enacts its first comprehensive privacy law, the Personal Information Protection Law (PIPL).
2022	EU Digital Services Act and Digital Markets Act enacted.
2022	In *Dobbs v. Jackson Women's Health Organization,* 597 U.S. 215 (2022), the US Supreme Court overturns *Roe v. Wade* and the right to reproductive freedom.
2022	More US states pass broad consumer privacy laws. These states include Connecticut and Utah.
2023	The EU-US Data Privacy Framework is established for cross-border data transfers.
2023	Additional US states pass broad consumer privacy laws, including Delaware, Florida, Montana, Indiana, Iowa, Tennessee, and Texas. Washington and other states enact broad health privacy laws.
2023	India enacts the Digital Personal Data Protection Act (DPDPA).

FOR FURTHER REFERENCE

Treatises

Lothar Determann, *California Privacy Law* (5th ed. 2023)

Andrew B. Serwin, *Information Security and Privacy: A Guide to International Law and Compliance* (2023)

Lisa J. Sotto, *Privacy and Cybersecurity Law Deskbook* (2022)

General Sources

Anita L. Allen, *Uneasy Access: Privacy for Women in a Free Society* (1988)
Allen provides a valuable overview of philosophical accounts of privacy's definition and value.

Danielle Keats Citron, *The Fight for Privacy* (2022)
Citron discusses threats to intimate privacy and how the law should combat them.

Danielle Keats Citron, *Sexual Privacy*, 128 Yale L.J. 1870 (2019)
Citron discusses the importance of privacy for people's intimate lives and why protecting privacy is essential for protecting women.

Michelle Finneran Dennedy, Jonathan Fox, and Thomas R. Finneran, *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value* (2014)
This book provides a detailed and concrete discussion about privacy by design and how to implement privacy in the development of technology.

Sarah Igo, *The Known Citizen: A History of Privacy in Modern America* (2018)
Igo traces the rise of modern American concepts of privacy, and depicts how Americans have viewed the line between private matters and public identity over the nineteenth and twentieth centuries.

Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (2009)
This is a powerful depiction of the legal, social and cultural implications of a world that no longer remembers how to forget. Advocates, among other solutions, for an expiration date for information in different settings and contexts.

Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2010)
This is an illuminating theory for understanding privacy in its social context.

Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (2015)
Pasquale argues that the detailed profiles that companies are creating about people have profound implications for their reputations and opportunities, as well as for society. The algorithms used to make automated decisions based on personal data are often hidden, and they should be more transparent. The law should also ensure that important decisions be made fairly and in a non-discriminatory manner.

Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393 (1978)
This article offers a critique of privacy from a pioneer of law and economics.

Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 Cal. L. Rev. 957 (1989)
Post provides a valuable argument about how privacy is a social value, not just an individual right.

Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (1995)
An illuminating study of how and why Congress enacted certain privacy laws.

Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (2015)
Richards argues that surveillance—by both the government and private sector entities—threatens freedom of speech, belief, and intellectual exploration.

Neil Richards, *Why Privacy Matters* (2021)
A philosophical and concrete account of the importance of privacy.

Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (2000)
Rosen views privacy as protecting "a space for negotiating legitimately different views of the good life" and examines the loss of private spaces in modern life.

Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1609 (1999)
An account of the importance of protecting the privacy of digital communications.

Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 Geo. Wash. L. Rev. 1 (2021)
Explaining why the privacy paradox is not really a paradox.

Daniel J. Solove, *Understanding Privacy* (2008)
Solove discusses a theory of what privacy is and why it is valuable.

Ari Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (2021)
A hard-hitting critique of why current privacy programs and compliance with privacy law fail to provide adequate protection.

Alan Westin, *Privacy and Freedom* (1967)
An early classic work about information privacy, providing an insightful account of the value privacy contributes to individuals and society.

Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019)
Zuboff analyzes the "new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales."