2015

An Overview of Privacy Law

Daniel J. Solove
George Washington University Law School, dsolove@law.gwu.edu

Paul M. Schwartz

Daniel J. Solove & Paul M. Schwartz

PRIVACY LAW FUNDAMENTALS 2015

An IAPP Publication

PRIVACY LAW FUNDAMENTALS

This document **only contains Chapter 2 – *An Overview of Privacy Law***.

The book has 13 chapters in all.

If you are interested in purchasing the book, visit our resource website:

www.informationprivacylaw.com

At the site above, you can find links to where the book can be purchased at IAPP and Amazon.

Privacy Law Fundamentals

Daniel J. Solove
John Marshall Harlan Research Professor of Law
George Washington University Law School
and
Senior Policy Advisor
Hogan Lovells
and
President and CEO
TeachPrivacy, LLC

&

Paul M. Schwartz
Jefferson E. Peyser Professor of Law
U.C. Berkeley School of Law
and
Director
Berkeley Center for Law & Technology
and
Special Advisor
Paul Hastings LLC

An IAPP Publication

Cover design by -ing designs, llc.
Book design and layout by Tammy F. Sneddon Design.

ISBN 978-0-9885525-7-9

ABOUT PRIVACY LAW FUNDAMENTALS

"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

"There are no better-qualified authors than Professor 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 US LLP

"This book is my go-to reference for when I need quick, accurate information on privacy laws across sectors and jurisdictions. Solove and Schwartz masterfully make complex privacy law more accessible and understandable for anyone, from the most experienced practitioner to first year law student."

– Nuala O'Connor, Center for Democracy and Technology

"Professors Solove and Schwartz pack an enormous amount of privacy knowledge into a slim volume in *Privacy Law Fundamentals*. In our fast-paced practice, there's nothing better than a compact and accessible work that is curated by two of the great thinkers of the field. It is a gem."

– Kurt Wimmer, Covington & Burling LLP

"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 LLP

"This is the essential primer for all privacy practitioners. Professors Solove and Schwartz have done a remarkable job of keeping this volume current in the fast-changing environment of new technology, case law and legislation."

– David A. Hoffman, Intel Corporation

ABOUT THE AUTHORS

Daniel J. Solove is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. He is also a senior policy advisor at Hogan Lovells and the President and CEO of TeachPrivacy, http://teachprivacy.com, a company that provides privacy and data security training to organizations in a wide array of industries. One of the world's leading experts in privacy law, Solove is the author of numerous books, including *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). Professor Solove is also the co-author (with Paul Schwartz) of a textbook, *Information Privacy Law*, with Aspen Publishing Co., now in its fourth edition. Additionally, he is the author of several other textbooks, including *Privacy and the Media* (1st edition, Aspen Publishing Co. 2009) and *Privacy, Information, and Technology* (3nd edition, Aspen Publishing Co. 2012), all with Paul Schwartz. He has published nearly 40 articles and essays.

Solove has testified before the U.S. Congress and has been involved as an expert and consultant in a number of high-profile privacy cases. 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*, *Associated Press*, *Time*, *Newsweek*, *People*, *Reader's Digest*, ABC, CBS, NBC, CNN, NPR and C-SPAN's "Book TV."

For more information about Professor Solove's work go to www.danielsolove.com. He can also be followed on Twitter at http://twitter.com/DanielSolove. As one of a select group of LinkedIn "Influencers," Professor Solove blogs at LinkedIn, http://www.linkedin.com/today/post/articles/2259773, on privacy and data security issues. His blog has more than 850,000 followers.

Paul M. Schwartz is Jefferson E. Peyser Professor of Law at the University of California–Berkeley Law School 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 U.S., his articles and essays have appeared in periodicals such as the *Harvard Law Review*, *Yale Law Journal*, *Stanford 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, 5th ed., 2015) 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 issues. A member of the American Law Institute, Schwartz 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 American Law Institute and the organizing committee of the Privacy Law Salon.

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).

Schwartz received a JD degree from Yale Law School, where he was a senior editor on *The Yale Law Journal*, and a BA degree from Brown University. His homepage is www.paulschwartz.net.

DEDICATION

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 that 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 very 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 possible. Wherever possible, we have developed charts and lists to convey the material.

The book is organized in thirteen chapters:

- Chapter One—a review of the key privacy developments since the last edition of this book.

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

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

- Chapter Five—national security law, including the Foreign Intelligence Surveillance Act.

- Chapter Six—the laws and regulations that pertain to health and genetic data, including HIPAA.

- Chapter Seven—government records and laws, such as the Privacy Act and the Freedom of Information Act.

- Chapter Eight—the laws concerning financial information, including the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act.

- Chapter Nine—legal regulation of the privacy of consumer data and business records, involving statutes, tort protections and FTC enforcement actions.

- Chapter Ten—data security law, including the varying laws in a majority of the states.

- Chapter Eleven—school privacy, including the Family Educational Rights and Privacy Act.

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

- Chapter Thirteen—international privacy law, including the EU Data Protection Directive, the OECD Guidelines, the APEC Privacy Framework and rules of international data transfers.

For his suggestions on our chapter about school privacy, we wish to thank Steven McDonald. This book also benefitted greatly from the research assistance of Henry Becker, Benedikt Burger, Sarah Chai, Leah Duranti, Yan Fang, Bill Friedman, Thad Houston, Jesse Koehler, Lea Mekhneche, Devon Mongeluzzi, Joseph Mornin, and Lourdes Turrecha.

For further references, including books, websites, statutes and other sources of news and legal materials, visit our website (http://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 to finding additional ways to make it as useful as possible. Please feel free to contact us with any suggestions and feedback about the book.

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

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

TABLE OF CONTENTS

CHAPTER 2

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 the 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 will 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*, 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 Warren & Louis 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 privacy was protected by the common law as "the right to be let alone."

William Prosser, *Privacy,* 48 Cal. L. Rev. 383 (1960)
The 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 an express or implied contractual term 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 U.S. CONSTITUTION PROTECTS PRIVACY

- The First Amendment right to speak anonymously
- The First Amendment freedom of association, which protects privacy of one's associations
- The Third Amendment's protection of the home from the quartering of troops
- The Fourth Amendment's protection against unreasonable searches and seizures
- The Fifth Amendment's 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
AZ	Ariz. Const. art. II, § 8
CA	Cal. Const. art. I, § 1
FL	Fla. Const. art. I, § 23
HI	Haw. Const. art. I, § 23
IL	Ill. Const. art. I, § 12
LA	La. Const. art. I, § 5
MT	Mt. Const. art. II, § 10
SC	S.C. Const. art. I, § 10
WA	Wash. Const. art. I, § 7

Federal Statutory Law

- Fair Credit Reporting Act 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, such as the right to see one's records and to ensure that the information in them is accurate.

- Family Educational Rights and Privacy Act 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 of 1978, 15 U.S.C. §§ 1801–1811—regulates foreign intelligence gathering within the U.S.

- Privacy Protection Act of 1980, 42 U.S.C. § 2000aa—restricts the government's ability to search and seize the work product of the press and the 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 of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709—updates federal electronic surveillance law to respond to the new developments in technology.

- Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a—regulates automated investigations conducted by government agencies comparing computer files.

- Employee Polygraph Protection Act of 1988, 29 U.S.C. §§ 2001–2009—governs the use of polygraphs by employers.

- Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710–2711—protects the privacy of videotape rental information.

- Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227—provides certain remedies from 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 in their motor vehicle records.

- Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414—requires telecommunication 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 deadbeat parents.

- Health Insurance Portability and Accountability Act of 1996—gives the Department of Health and Human Services the authority to promulgate regulations governing the privacy of medical records.

- Identity Theft and Assumption Deterrence Act 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 of 1998, 15 U.S.C. §§ 6501–6506—restricts the use by Internet websites of information gathered from children under age 13.

- Gramm-Leach-Bliley Act 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.

- USA Patriot Act of 2001—amends a number of electronic surveillance statutes and other statutes to facilitate law enforcement investigations and access to information.

- CAN-SPAM Act of 2003—provides penalties for the transmission of unsolicited e-mail.

- 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.

State Statutory Law

Much of privacy law is found in state law. Privacy tort law and data breach notification statutes are all 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 U.S. regulation of privacy is best thought of as a dual federal-state system for information privacy law.

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
- Spam
- Spyware and phishing
- Telecommunications privacy
- Pretexting
- Use of Social Security numbers
- Data disposal
- Video privacy
- RFID and tracking devices
- Restrictions on ISPs
- Unauthorized access to computers and networks

Data Security
- Identity theft
- Data security breach notification

Employment
- State employee personal information
- Restrictions on employment application questions

For a more detailed analysis of these laws, consult Andrew B. Serwin's *Information Security and Privacy* (2014).

International Law

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

1. *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.

2. *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.

In contrast, the United States has generally relied on regulation of information use on a sector-by-sector basis. For example, the Children's Online Privacy Protection Act provides privacy protection for children on the Web, but there is no such law that generally regulates privacy for adults on the Web.

Outside of Europe and the United States, there are many information privacy statutes in the rest of the world. Most countries have adopted the omnibus approach.

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)
- The Safe Harbor Privacy Principles (2000) established between the United States and the European Commission
- Asia-Pacific Economic Cooperative (APEC) Privacy Framework (2004)

THE CHIEF PRIVACY OFFICER

The chief privacy officer (CPO) is becoming a mainstay at many large organizations. Among other things, a CPO ensures that the organization is complying with the law, that employees are trained about privacy and security practices and that the organization has an effective privacy policy.

In the public sector, the Homeland Security Act of 2002 established a privacy officer within the Department of Homeland Security. 6 U.S.C. § 142. This statute created the first explicit legal requirement in a federal law for a privacy officer in the United States government. Previously, the Clinton administration had appointed a chief counselor for privacy and located this position in the Office of Management and Budget's 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 the Health Insurance Portability and Accountability Act of 1996 (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 Gramm-Leach-Bliley Act, the Federal Trade Commission issued a Safeguards Rule that requires designation of an employee or employees to coordinate the company's information security program. This requirement can encourage introduction of a chief privacy officer position at organizations that do not yet have one. 16 C.F.R. Part 314.4(a), 67 Federal Register 36484 (2002).

In addition, the Safe Harbor Agreement, negotiated by the U.S. Department of Commerce with the European Commission, calls for U.S. companies to engage in either "self-assessment or outside compliance review" of their privacy practices. By mandating these requirements, the Safe Harbor creates the

obligation for a certain amount of compliance work and an incentive for U.S. organizations that register under it to designate a CPO to take care of these tasks.

It is fair to say that most large companies that handle personal data now have a CPO.

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*, 77 Eng. Rep. 194 (K.B. 1604) declares that "the house of everyone is to him as his castle and fortress."

1700 – 1799

1763 *Wilkes v. Wood*, 98 Eng. Rep. 489 (K.B.), 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*, 95 Eng. Rep. 807 (K.B.), is another repudiation of general warrants in a seditious libel case. Influential in the creation of the Fourth Amendment.

1789 U.S. Constitution—First, Third, Fourth, and Fifth Amendments.

1800 – 1899

1860 U.S. Census becomes more inquisitive. Public outcry for greater census privacy.

1877 *Ex Parte Jackson*, 96 U.S. 727 (1877)—U.S. Supreme Court holds that the Fourth Amendment protects sealed letters in the mail.

1886 *Boyd v. United States*, 116 U.S. 616 (1886)—U.S. Supreme Court holds that the government cannot compel people to turn over documents.

1890 Samuel Warren & Louis 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.

1900 – 1959

1903 States begin to recognize privacy torts. New York enacts law creating Warren and Brandeis tort of appropriation. N.Y. Civ. Rts. L. §§ 50-51. Georgia Supreme Court recognizes appropriation tort. *Pavesich v. New England Life Insurance Company*, 50 S.E. 68 (Ga. 1905).

1908 FBI is formed. Originally called the Bureau of Investigation.

1928 *Olmstead v. United States*, 277 U.S. 438 (1929). In a decision later overruled, the U.S. Supreme Court holds that Fourth Amendment protections do not extend to wiretapping. Now on the Supreme Court, Justice Louis Brandeis writes a famous dissent to the majority opinion.

1934 In response to *Olmstead*, Congress enacts § 605 of the Federal Communications Act of 1934 to limit wiretapping.

1936 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 Central Intelligence Agency (CIA) is created.

1948 The Universal Declaration of Human Rights is adopted by the UN, 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 President Truman creates the National Security Agency (NSA).

1953 Origins of the "right of publicity" tort in *Haelan Laboratories v. Topps Chewing Gum, Inc.*, 202 F.2d 866 (2d Cir. 1953).

1960 – 1979

1960 William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960).

1961 In *Mapp v. Ohio*, 367 U.S. 643 (1961), the U.S. 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 U.S. Supreme Court prevents the government from banning contraceptives. The Griswold Court finds that the Constitution protects a right to privacy through the "penumbras" of many of the 10 amendments of the Bill of Rights.

1966 Congress enacts the Freedom of Information Act (FOIA).

1967 In *Katz v. United States*, 389 U.S. 347 (1967), the U.S. Supreme Court reverses Olmstead. The concurrence in the case by Justice John Marshall Harlan articulates the "reasonable expectation of privacy test," the current approach for determining the Fourth Amendment's applicability.

1967 Alan Westin publishes *Privacy and Freedom*.

1968 Title III of the 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 The Fair Credit Reporting Act.

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 U.S. Department of Health, Education and Welfare (HEW) issues a report, *Records, Computers, and the Rights of Citizens*, articulating the FIP.

1974 The Privacy Act.

1974 The Family Educational Rights and Privacy Act.

1975 Congress's Church Committee conducts a thorough investigation of surveillance abuses by the government.

1975 In *Cox Broadcasting v. Cohn*, 420 U.S. 469 (1975), the U.S. Supreme Court recognizes some First Amendment limitations on the privacy torts.

1976 In *United States v. Miller*, 425 U.S. 435 (1976), the U.S. 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 The 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.

1979 In *Smith v. Maryland*, 442 U.S. 735 (1979), the U.S. Supreme Court rules that 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 Organisation of Economic Co-operation and Development (OECD) Guidelines.

1981 Israel's Protection of Privacy Law.

1986 Congress passes the Electronic Communications Privacy Act (ECPA), creating the contemporary statutory approach to regulating the electronic surveillance of communications.

1986 Computer Fraud and Abuse Act (CFAA).

1988 Australia passes the Privacy Act, which is based on the OECD Guidelines.

1988 Video Privacy Protection Act (VPPA).

1990 – 1999

1992 The UK begins implementing its CCTV video surveillance system.

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 Driver's Privacy Protection Act (DPPA).

1995 Communications Decency Act (CDA).

1996 Congress passes the Health Insurance Portability and Accountability Act (HIPAA). Title II of HIPAA requires the establishment of national standards for electronic data exchange and addresses issues concerning the privacy and security of healthcare 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.

1998 Children's Online Privacy Protection Act (COPPA).

1998 The UK Human Rights Act.

1998 The UK Data Protection Act.

1998 Sweden's Personal Data Act.

2000 – 2009

2000 The Safe Harbor Agreement is established between the U.S. and EU for data sharing under the EU Data Protection Directive.

2000 Argentina becomes the first country in South America to adopt 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 In *Kyllo v. United States*, 523 U.S. 27 (2001), the U.S. 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 Department of Health and Human Services issues final modifications to the HIPAA Privacy Rule.

2003 Japan enacts the Personal Data Protection Act.

2004 Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

2004 The European Court of Human Rights decides *Von Hannover v. Germany*, ECHR 294 (2004), recognizing privacy rights in certain public settings.

2005 ChoicePoint, one of the largest data brokers, announces that 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 began disclosing data security breaches. A vast majority of states enacted data security breach notification legislation in response.

2009 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 – Present

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.

2010 Mexico enacts the Federal Law for the Protection of Personal Data.

2011 In *United States v. Jones*, 131 S. Ct. 1207 (2011), the U.S. 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 Commission proposes EU General Data Protection Regulation.

2013 HHS issues HIPAA Omnibus Final Rule.

2013 Edward Snowden leaks classified documents detailing numerous broad surveillance programs by the NSA.

2013 In *Clapper v. Amnesty Intern*. USA, 133 S. Ct. 1138 (2013), the U.S. Supreme Court denies standing to challengers to NSA surveillance lacked standing to bring their case.

2013 FTC issues Amendments to the COPPA Rule (July 2013).

2013 Supplemental, additional OECD Privacy Guidelines released.

2014 FTC celebrates 100th birthday.

2014 Several prominent 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 U.S. Supreme Court holds that a warrant is generally required to search digital information on a cell phone seized pursuant to an individual's arrest.

2014 InBloom closed (in part) due to privacy concerns. Numerous states enact new privacy laws for K-12 students.

2014 In *Google Spain v. AEPD*, C-131/12 (ECJ, May 13, 2014), the European Court of Justice (ECJ) requires a search engine to remove a link to a search result that violates the "right to be forgotten."

(2014) FTC announces Safe Harbor settlements with twelve U.S. companies.

FOR FURTHER REFERENCE

Treatises

Kristin J. Matthews, *Proskauer on Privacy* (2006)
(originally created and edited by Christopher Wolf).

Andrew B. Serwin, *Information Security and Privacy* (2009)

Lisa Sotto, *Privacy and Data Security Law Deskbook* (2010)

General Sources

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

Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground,* 63 Stan. L. Rev. 247 (2011)
An insightful study comprised of interviews of chief privacy officers.

Colin Bennett & Charles Raab, *The Governance of Privacy* (2003)
A thoughtful study of the political landscape of privacy policymaking around the world.

Michelle Finneran Dennedy, Jonathan Fox, & Thomas R. Finneran, T*he Privacy Engineer's Manifesto* (2014)
A detailed and concrete discussion about Privacy by Design and how to implement privacy in the development of technology.

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

Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2009)
An illuminating theory for understanding privacy in its social context.

Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (2014)
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 re 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)
One of the most compelling critiques of privacy.

Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 Cal. L. Rev. 957 (1989)
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)
Illuminating study of how and why Congress has passed certain privacy laws.

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

Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (2000)
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 Solove, *Understanding Privacy* (2008)
A theory of what privacy is and why it is valuable.

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.

PRIVACY LAW FUNDAMENTALS

This document **only contains Chapter 2 – *An Overview of Privacy Law***.

The book has 13 chapters in all.

If you are interested in purchasing the book, visit our resource website:

www.informationprivacylaw.com

At the site above, you can find links to where the book can be purchased at IAPP and Amazon.

"There are no better-qualified authors than Professor 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 US LLP

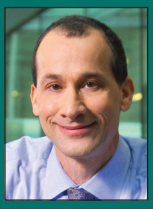
"This book is my go-to reference for when I need quick, accurate information on privacy laws across sectors and jurisdictions. Solove and Schwartz masterfully make complex privacy law more accessible and understandable for anyone, from the most experienced practitioner to first year law student."
– Nuala O'Connor, Center for Democracy & Technology

"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 LLP

"This is the essential primer for all privacy practitioners. Professors Solove and Schwartz have done a remarkable job of keeping this volume current in the fast-changing environment of new technology, case law and legislation."
– David A. Hoffman, Intel Corporation

ABOUT THE AUTHORS

DANIEL J. SOLOVE is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. He is also President and CEO of TeachPrivacy, a privacy and security training company.



PAUL M. SCHWARTZ is Jefferson E. Peyser Professor of Law at Berkeley Law School and a director of the Berkeley Center for Law & Technology. He is also a special advisor at Paul Hastings.

$40.00
ISBN 978-0-9885525-7-9
54000>
9 780988 552579

An iapp publication