The right to respect for private life: digital challenges, a comparative-law perspective

The United States

STUDY

EPRS | European Parliamentary Research Service

Comparative Law Library Unit
PE 628.240 – October 2018

EN

THE RIGHT TO RESPECT FOR PRIVATE LIFE: DIGITAL CHALLENGES, A COMPARATIVE-LAW PERSPECTIVE

The United States

STUDY

October 2018

Abstract

This study forms part of a wider-ranging project which seeks to lay the groundwork for comparisons between legal frameworks governing the right to respect for private life in different legal systems, and between the ways in which the systems address the challenges that the 'digital age' poses to the exercise of that right.

The following pages will analyse, with reference to the United States and the subject at hand, the legislation in force, the most relevant case law and the nature of the right to respect for private life, ending with some conclusions on the challenges discussed.

Unlike jurisdictions that have adopted an omnibus approach to privacy protection, the US takes a sectoral approach to regulating privacy, with different regulatory regimes for different contexts and sectors of the economy. This report provides an overview of the different areas of law addressing privacy, including constitutional, statutory, and common law, as well as of relevant scholarly commentary. The report concludes with a summary of the current legislative outlook.

AUTHOR

This study has been written by **Mr Luis Acosta, Chief, Foreign, Comparative, and International Law Division II, Law Library of Congress, of the US Library of Congress**, at the request of the Comparative Law Library Unit, Directorate-General for Parliamentary Research Services (DG EPRS), General Secretariat of the European Parliament.

CONTACT PERSON

Prof. Dr. Ignacio Díez Parra, Head of the Comparative Law Library Unit.

To contact the Unit, please send an email to: EPRS-ComparativeLaw@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

Translations: DE, ES, FR, IT

This document is available on the internet at: http://www.europarl.europa.eu/thinktank

DISCLAIMER

Manuscript completed in September 2018.

PE 628.240

Print	ISBN 978-92-846-3910-6	DOI:10.2861/66217	QA-04-18-838-EN-C
PDF	ISBN 978-92-846-3903-8	DOI:10.2861/096079	QA-04-18-838-EN-N

Table of Contents

List of abbreviations

2d	Second
3d	Third
A.2d	Atlantic Second, the second series of a private publication of published appellate court case decisions by the state courts of Delaware, the District of Columbia, Maryland, New Jersey, and Pennsylvania.
Amend.	Amendment
Am. Law Inst.	American Law Institute
Am. U. L. Rev.	American University Law Review
Anne	English statutes from the reign of Queen Anne
Assemb.	Assembly (as in the California State Assembly, a branch of the California Legislature)
Cal.	California
Cal. Civ. Code	California Civil Code
Calif. L. Rev.	California Law Review
C.F.R.	Code of Federal Regulations
Ch.	Chapter. An early designation for public laws published in United States Statutes at Large.
Cl.	Clause
Co.	Company
Colo.	Colorado
Cong. Research Serv.	Congressional Research Service
Conn.	Connecticut
Conn. J. Int'l L.	Connecticut Journal of International Law
Ct.	Court
Ed.	Edition
Eds.	Editors
F.2d & F.3d	Federal Reporter Second and Federal Reporter Third, the second and third series of a private publication of published decisions by the federal courts of appeals of the U.S.
FCC	U.S. Federal Communications Commission
Fed.	Federal
Fed. Comm. L.J.	Federal Communications Law Journal
Fed. Reg.	Federal Register

Fla. L. Rev.	Florida Law Review
Ga.	Georgia
Geo III	English statutes from the reign of George III
Geo. L. Rev.	Georgetown Law Review
Harv. J. L. & Pub. Pol'y	Harvard Journal of Law & Public Policy
Harv. L. Rev.	Harvard Law Review
Id.	*Idem*, used to refer to the immediately preceding authority cited.
Ill. L. Rev.	Illinois Law Review
Inc.	Incorporated
Int'l	International
J.	Justice, or Journal
Kan.	Kansas
Ky.	Kentucky
L. Rev.	Law Review
Mass.	Massachusetts
Mass. Gen. Laws	General Laws of Massachusetts
Mich.	Michigan Law Review
Minn.	Minnesota
N.C. L. Rev.	North Carolina Law Review
N.E.	North Eastern Reporter, a private publication of published appellate court case decisions by the state courts of Illinois, Indiana, Massachusetts, New York, and Ohio.
N.J. Eq.	New Jersey Equity Reports
Mo. Ct. App.	Missouri Court of Appeal
N.W.2d	North Western Reporter Second, the second series of a private publication of published appellate court case decisions by the state courts of Iowa, Michigan, Minnesota, Nebraska, North Dakota, South Dakota, and Wisconsin
Nw. L. Rev.	Northwestern University Law Review
N.Y.	New York
N.Y. Gen. Bus. Law	New York General Business Law
Org.	Organization
P.2d	Pacific Reporter Second, the second series of a private publication of published appellate court case decisions by the state courts of Alaska,

	Arizona, California, Colorado, Hawaii, Idaho, Kansas, Montana, Nevada, New Mexico, Oklahoma, Oregon, Utah, Washington, and Wyoming
Pol. Sci. Q.	Political Science Quarterly
S.	Senate
§	Section
S. Cal. L. Rev.	Southern California Law Review
S. Ct.	West's Supreme Court Reporter, a private publication of Supreme Court opinions and orders that is cited if an opinion is not yet in United States Reports.
S.E.	South Eastern Reporter, a private publication of published appellate court case decisions by the state courts of Georgia, North Carolina, South Carolina, Virginia, and West Virginia.
S.W.	South Western Reporter, a private publication of published appellate court case decisions by the state courts of Arkansas, Kentucky, Missouri, Tennessee, and Texas.
Slip op.	Slip opinion, a term used for the form of publication of a court decision before it is published in a bound volume of decisions that is cited if an opinion is not yet published in a bound reporter.
Stan. L. Rev.	Stanford Law Review
Stat.	United States Statutes at Large, the official chronological publication of laws passed by the Congress.
Supp.	Supplement
S.W.2d	South Western Reporter Second, the second series of a private publication of published appellate court case decisions from the state courts of Arkansas, Kentucky, Missouri, Tennessee, and Texas.
Tex. L. Rev.	Texas Law Review
U.	University
U. Chi. L. Rev.	University of Chicago Law Review
U. Pa. L. Rev.	University of Pennsylvania Law Review
U.S. or US	United States. Also, United States Reports, the official publication of U.S. Supreme Court opinions and orders.
U.S.C.	United States Code, the official compilation of federal laws of a permanent and general nature. Comprises 52 subject titles. Most of the sections pertaining to the judiciary are found in title 28.
U.S. Const.	United States Constitution. Cited by Amendment (amend.), Article (art.), Section (§ or sec.), and Clause (cl.).
v.	versus
Wis.	Wisconsin
Wis. Stat.	Wisconsin Statutes

Executive summary

Unlike jurisdictions that have adopted an omnibus framework for regulating privacy, the United States takes a sectoral approach, with separate laws addressing privacy matters in fields like health, financial services, and education. This study provides an overview of the multiple areas of US law affecting privacy. It includes a historical overview of how the right to privacy developed in the US, discusses the US Constitution and relevant federal and state statutory law, summarizes major constitutional and tort law developments, discusses relevant legal commentary, and describes current legislative initiatives.

I. Introduction

Privacy law in the United States is not a unitary doctrine, but rather embodies multiple theories and bodies of law, including constitutional law, common-law tort, and a disparate body of primarily sector-based statutory law. This article provides an overview of the multiple concepts and areas of US law affecting privacy.

Because this report is part of a comparative study, it follows a structure prescribed for the broader study for purposes of harmonization, with the Constitution and statutes, case law, and scholarly commentary addressed in separate sections. While privacy law has developed in the US dialectically, with scholarly commentary affecting the development of case law and case law sometimes prompting the enactment of statutes, this report follows the prescribed structure of the broader study.

Section I presents a brief historical overview of the development of the right to privacy in the US, and introduces the challenges that the digital era presents for privacy. Section II outlines the textual provisions of the US Constitution that relate to privacy, and identifies the many privacy-related federal statutes and the categories of regulation addressed by state statutory law. Section III covers case law, including US constitutional case law concerning the right to privacy, as well as case law on privacy torts. Section IV describes legal commentary on the right to privacy relevant to the preceding sections, as well as commentary on the nature of the right to privacy in US law. The concluding section V discusses the current state of play with respect to legislative initiatives.

I.1. Historical development of the right to privacy in the United States

Privacy was a matter of concern for North American British colonialists. Laws providing for we would now call information privacy predate the establishment of the United States. In British colonial America, an intercolonial postal system was established.[1] An English postal statute that applied in the colonies, the Post Office Act of 1710, stated that "[n]o Person or Persons shall presume wittingly, willingly, or knowingly, to open, detain, or delay, or cause, procure, permit, or suffer to be opened, detained, or delayed, any Letter or Letters, Packet, or Packets."[2] Postal employees were required to sign an oath stating:

> I, A.B., do swear, That I will not wittingly, willingly, or knowlingly open ... or cause, procure, permit, or suffer to be opened ... any Letter or Letters ... which shall come into my Hands, Power, or Custody, by Reason of my Employment in or relating to the Post Office; except ... by an express Warrant in Writing under the Hand of one of the Principal Secretaries of State for that purpose.[3]

Postmasters general in the colonies established regulations to ensure the integrity and privacy of the mail, including requiring local postmasters to keep post offices separate from homes, requiring that no unauthorized persons handled the mail, requiring mail for each town to be separately sealed in bags that were unsealed only when they reached the destination town, and requiring persons to provide identification before retrieving posted letters.[4]

Grievances against British rule in the American colonies included privacy-related concerns. British law provided for writs of assistance – a means of customs enforcement that authorized officers "to enter and go into any House, Warehouse, Shop, Cellar, or other Place, in the British

---

1 FREDERICK S. LANE, AMERICAN PRIVACY: THE 400-YEAR HISTORY OF OUR MOST CONTESTED RIGHT 5-7 (2009).

2 9 Anne ch. 11 § XLI (1710).

3 *Id.* § XLII.

4 LANE, *supra* note 1, at 8.

Colonies or Plantations in America, to search for and seize prohibited or uncustomed Goods."[5] Such writs once issued remained in force through the lifetime of the monarch and six months thereafter.[6]

After a series of well-publicized controversies arising from the use of such writs, the colonists declared independence from Britain, partly in reaction to abuses of writs of assistance.[7]

Concern for informational privacy was demonstrated when the Continental Congress passed an ordinance regulating the post office in 1782 stating that postal employees shall not knowingly "open, detain, delay, secrete, embezzle or destroy ... any letter" except by consent of the addressee or by warrant of the President, or of the commanding officer of the Army in times of war.[8]

The US Constitution was ratified by the states in 1788 with the understanding in several state conventions that a Bill of Rights would be offered as an amendment. In 1791 the Bill of Rights, containing the first ten amendments to the Constitution, was ratified. As discussed in section II.1 below, the Bill of Rights included several amendments affirming the value and sanctity of privacy. While the word "privacy" does not appear in the Constitution, privacy concerns were central to the founding of the US.[9]

The Congress of the new republic enacted a comprehensive statute governing the post office in 1792, and made it a criminal offense for a postal employee to "unlawfully detain, delay, or open, any letter, packet, bag or mail of letters, with which he shall be entrusted."[10]

As noted in section III.1.1 below, in 1878, information privacy was affirmed as a central concern when the Supreme Court stated that the Fourth Amendment required the privacy of sealed mail.

Concepts of privacy law evolved as new technologies developed. With the advent of the telegraph, states began to enact laws prohibiting the disclosure of telegrams, as noted in section II.3.2 below. With the development of photography, courts came to recognize a privacy tort to address unauthorized use of a person's image, as discussed in section III.2 below. The invention of the telephone gave rise to the ability to wiretap communications, and the law responded with case law, as described in section III.1.1 below.

With the development of computers and the capacity of government gather personal data, Congress responded with a number of statutes addressing privacy. These statutes are summarized in section II.2. State legislatures responded as well, as discussed in section II.3.2.

The privacy tort developed in the latter half of the twentieth century to encompass causes of action for four separate torts, namely intrusion on seclusion, public disclosure of embarrassing private facts, placing the plaintiff in a false light in the public eye, and appropriation of the plaintiff's name or likeness.

---

5 Townshend Act of 1767, 7 Geo. III, ch. 46 § 10 (Eng.) (reauthorizing prior acts permitting use of writs of assistance).

6 CONG. RESEARCH SERV., THE CONSTITUTION OF THE UNITED STATES OF AMERICA: ANALYSIS AND INTERPRETATION 1382 (cases decided through August 26, 2017), https://www.congress.gov/content/conan/pdf/GPO-CONAN-2017-10-5.pdf.

7 These controversies are recounted in Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1240-80 (2016), https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=5941&context=uclrev.

8 An Ordinance for Regulating the Post Office of the United States of America, 23 JOURNALS OF THE CONTINENTAL CONGRESS 1774-1789, at 670-71 (Oct. 18, 1782).

9 Donahoe, *supra* note 7, at 1280-324; *see also* Anuj C. Desai, *Wiretapping before the Wires: The Post Office and the Rebirth of Communications Privacy*, 60 STAN. L. REV. 553 (2007), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1079958 (arguing that the principle of communications policy derives from early postal policymakers who incorporated the principle in postal ordinances and statutes in the late eighteenth century).

10 Act of Feb. 20, 1792, § 16, 1 STAT. 232, 236.

US privacy law also came to encompass the principle of personal autonomy. As noted in section III.1.2 below, beginning in 1965, a series of Supreme Court cases recognized a right of privacy to prevent government interference with personal decisions like using birth control, abortion, and sexual intimacy.

I.2. Challenges to the the right to respect for private life in the digital era

The sectoral approach to privacy law that has prevailed in the US is largely reactive in nature, with laws often enacted only after well-publicized incidents highlight regulatory inadequacies. With rapidly changing technology, social media applications, and continued development of private acquisition and collection of personal data, US law has struggled to adapt to new conditions. Scholars have debated whether an omnibus regulatory framework should replace US law's traditional sectoral approach. Efforts at providing a legislative solution to these problems are discussed in section V below.

II. The concept of right to respect for private life in US legislation

This section discusses, first, provisions in the US Constitution that relate to privacy, and second, the disparate collection of federal statutes addressing the right to privacy. As noted above, the US approach to privacy is sectoral, generally regulating privacy on a sector-by-sector basis, such as health care, education, consumer finance, and the like, and the legislation discussed here reflects that approach.

II.1. The US Constitution

The Bill of Rights — the first ten amendments to the Constitution — includes several amendments pertain to privacy, even though the word "privacy" is nowhere used therein.

The First Amendment provides that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble ..."[11] As discussed in section III.1.4 below, the freedom of religion and of assembly protect the right of organizations to meet privately and to protect their membership lists from seizure by the government. The First Amendment also has been held to protect the right to possess literature, including materials the government considers obscene, in the privacy of one's home.

The Third Amendment states that "[n]o soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."[12] This amendment demonstrates the founders' desire to preserve the sanctity and privacy of the home.

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[13]

The Fourth Amendment is the subject of extensive case law, some of the highlights of which are described in section III.1.1.

The Fifth Amendment states that "[n]o person ... shall be compelled in any criminal case to be a witness against himself ..."[14] It thus protects individual privacy with respect to potentially inculpatory information.

Also relevant to the constitutional right to privacy is the Ninth Amendment, which states that "[t]he enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people."[15] The list of rights in the Bill of Rights thus is not exclusive, and the absence of the word "privacy" in the Constitution does not mean it is not a constitutional right.

The Fourteenth Amendment, a post-Civil War amendment, states in part that no state shall "deprive any person of life, liberty, or property, without due process of law; nor deny to any

---

[11] U.S. CONST. amend. I.

[12] U.S. CONST. amend. III.

[13] U.S. CONST. amend. IV.

[14] U.S. CONST. amend. V.

[15] U.S. CONST. amend. IX.

person within its jurisdiction the equal protection of the laws."[16] The Fourteenth Amendment is often invoked as a source of substantive rights against state deprivations of freedom.

The case law on the constitutional right of privacy discussed in section III.1 builds upon these amendments.

II.2. Federal Statutes Providing for Privacy Rights

II.2.1. Omnibus Crime Control and Safe Streets Act of 1968

Congress enacted provisions to address wiretapping in title III of the Omnibus Crime Control and Safe Streets Act of 1968.[17] It generally prohibited wiretapping and electronic eavesdropping, but permitted federal and state law enforcement officers to conduct surveillance after obtaining a warrant demonstrating probable cause.[18]

II.2.2. Fair Credit Reporting Act of 1970

An early federal privacy statute is the Fair Credit Reporting Act of 1970. It provides limited protection to individuals regarding the use and disclosure of personal financial information by credit reporting agencies.[19] The statute responded to the need for privacy and consumer protection with respect to the mechanisms developed by private credit reporting agencies for investigating and evaluating consumers' credit information.[20] The statute requires credit reporting agencies to adopt procedures to adopt procedures regarding the confidentiality, accuracy, relevancy, and proper utilization of individuals' credit information.[21]

The law specifies the circumstances under which a credit reporting agency can provide an individual's credit report, such as in conjunction with a credit transaction, for an employment purpose (in controlled circumstances), for insurance underwriting, and other specified purposes.[22] The law establishes procedures for consumers to gain access to their credit reports and to dispute or correct erroneous information.[23]

The law was substantially amended in 2003 in order to, inter alia, establish protections against identity theft,[24] and provide greater protection with respect to medical information[25] and Social Security numbers in credit reports.[26]

---

16 U.S. CONST. amend. XIV.

17 Public Law 90–351, title III, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (2012)). Congress previously had prohibited wiretapping in section 605 of the 1934 Communications Act, Pub. L. No. 73-416, 48 Stat. 1064 (1934) (codified as amended at 47 U.S.C. § 605 (2012)), which made it illegal to divulge or publish the existence, contents, substance, purport, effect or meaning of intercepted communication to any person. As noted *infra* at note 133, the government interpreted the 1934 provision narrowly and continued to conduct significant domestic surveillance.

18 The 1968 warrant requirements as currently amended are codified at 18 U.S.C. §§ 2516-2518.

19 15 U.S.C. § 1681 (2012).

20 15 U.S.C. § 1681(a).

21 15 U.S.C. § 1681(b).

22 15 U.S.C. § 1681b(a).

23 15 U.S.C. §§ 1681g, 1681i.

24 Fair and Accurate Credit Transactions Act of 2003, codified in part at 15 U.S.C. §§ 1681c-1, 1681c-2.

25 15 U.S.C. § 1681b(g).

26 15 U.S.C. § 1681g(a)(1)(A).

II.2.3. Privacy Act of 1974

The Privacy Act of 1974[27] regulates the collection, use, and disclosure of personal information by federal agencies. It states that "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to written request by, or with the prior written consent of, the individual to whom the record pertains."[28] Various exceptions are provided.[29] The Privacy Act also gives individuals the right to find out what information a federal agency has collected,[30] request correction of wrong information,[31] and request administrative review or bring a civil action in court.[32] The Privacy Act also required federal agencies, and state and local governments, to curtail use of Social Security numbers as an indentification number.[33]

II.2.4. Family Educational Rights and Privacy Act of 1974

The Family Educational Rights and Privacy Act of 1974 (FERPA)[34] regulates the privacy and disclosure of the education records of students. It gives parents the right to inspect and review the education records of their children.[35] It also gives them the right to correct inaccurate information.[36] When the student turns eighteen or enrolls in college, the rights under FERPA transfer from the parent to the student.[37] Schools and educational agencies are generally prohibited from disclosing education records to other other people or organizations without written consent of the parents (or student).[38] There are certain exceptions to the consent requirement, such as when a student transfers to a different school, in connection with a student's financial aid, for program auditing purposes, when an agency social worker has a lawful right to view such records, for law enforcement purposes, and the like.[39]

II.2.5. Right to Financial Privacy Act of 1978

The Right to Financial Privacy Act of 1978 (RFPA) provides privacy protection over financial records.[40] Enacted in reaction to the Supreme Court's decision in *United States v. Miller* (discussed in section III.1.1 *infra*), it provides that law enforcement must obtain a warrant or subpoena to obtain financial information, and must make a showing that there is "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry."[41] It provides that the consumer is usually entitled to advance notice, subject to certain exceptions.[42]

---

27 5 U.S.C. § 552a (2012).

28 5 U.S.C. § 552a(b).

29 *Id.*

30 5 U.S.C. § 552a(d)(1).

31 5 U.S.C. § 552a(d)(3).

32 5 U.S.C. § 552a(g)(1).

33 Pub. L. 93–579, § 7, Dec. 31, 1974, 88 Stat. 1909, reproduced at 5 U.S.C. § 552a note. That section is the only part of the Privacy Act that applies to state and local governments in addition to the federal government.

34 20 U.S.C. § 1232g (2012).

35 20 U.S.C. § 1232g(a)(1).

36 20 U.S.C. § 1232g(a)(2).

37 20 U.S.C. § 1232g(d).

38 20 U.S.C. § 1232g(b)(1).

39 *Id.*

40 12 U.S.C. §§ 3401-3422 (2012).

41 12 U.S.C. § 3407.

42 12 U.S.C. § 3409.

II.2.6. Privacy Protection Act of 1980

The Privacy Protection Act of 1980 protects journalists from having their research and work product materials searched and seized in criminal investigations.[43] The law provides that:

> it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication ...[44]

Certain exceptions apply, such as where there is probable cause that the journalist is the target of a criminal investigation, or where immediate seizure of such materials is necessary to prevent a person's death or injury.[45]

II.2.7. Cable Communications Policy Act of 1984

The Cable Communications Policy Act of 1984 regulates the cable television industry nationally.[46] It includes a provision protecting the privacy of subscribers of cable television.[47] That provision sets forth requirements to give notice to the subscriber regarding the personally identifiable information collected,[48] and provides that cable operators shall not collect or disclose personally identifiable information concerning any subscriber without prior consent of the subscriber (except to the extent required to provide services to the subscriber or detect unauthorized reception).[49]

II.2.8. Computer Matching and Privacy Protection Act of 1988

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act of 1974 to regulate the use of computer matching of federal records, a practice involving the use of computers to cross-check data sets of of persons receiving government benefits.[50] The act imposes procedural requirements on computer-matching activities, provides affected beneficiaries with opportunities to receive notice and to refute adverse information before having a benefit denied or terminated, and requires that agencies engaged in matching activities establish Data Protection Boards to oversee those activities.[51]

II.2.9. Employee Polygraph Protection Act of 1988

The Employee Polygraph Protection Act of 1988 prohibits most private employers from using lie detector tests for pre-employment screening or during the course of employment.[52] Employers generally may not request any employee or job applicant to take a lie detector test, or make employment determinations against an employee or applicant for refusing to take a test or on the basis of the results of a test.[53] Some employers in sensitive fields, such as national security and pharmaceuticals, are allowed to administer polygraph tests. The Act also permits

---

43 42 U.S.C. §§ 2000aa–2000aa-12 (2012). This law was enacted to respond to the Supreme Court decision in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), in which the Court ruled that a warranted search of a newspaper to gather evidence for a police investigation was permissible.

44 42 U.S.C. § 2000aa.

45 42 U.S.C. § 2000aa(a).

46 47 U.S.C. §§ 521-573 (2012).

47 47 U.S.C. § 551.

48 47 U.S.C. § 551(a).

49 47 U.S.C. § 551(b) & (c).

50 5 U.S.C. § 552a(a)(8)-(13), (e)(12), (o), (p), (q), (r), (u) (2012).

51 5 U.S.C. § 552a(o), (p).

52 29 U.S.C. §§ 2001-2009 (2012).

53 29 U.S.C. § 2002.

polygraph testing of certain employees of private firms who are reasonably suspected of involvement in theft or embezzlement.[54] Where polygraph examinations are allowed, they are subject to strict standards.[55]

II.2.10. Video Privacy Protection Act of 1988

The Video Privacy Protection Act of 1988 generally prohibits video service providers from unauthorized disclosure of personally identifiable information such as customer video rental information.[56]

II.2.11. Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 prohibits the government from engaging in the unauthorized interception of electronic communications.[57] It was enacted to extend the wiretapping restrictions of title III of the Omnibus Crime Control and Safe Streets Act of 1968 to new forms of communication and storage. It requires the government to obtain a court order, based upon probable cause, in order to intercept data communications.[58] The law also requires that the government obtain a search warrant in order to compel a third-party service provider to disclose the content of email, or other electronic communications, that the provider maintains in electronic storage.[59] However, this search warrant requirement for email applies only if the email is 180 days old or less. The law allows the government to compel the disclosure of older email with either a subpoena or a court order that is issued upon a finding that there are specific and articulable facts demonstrating that the information sought is relevant to a criminal investigation. It also allows the government to use a subpoena or court order to compel disclosure of documents stored in the Internet cloud.[60]

II.2.12. Telephone Consumer Protection Act of 1991

The Telephone Consumer Protection Act of 1991 restricts telemarketing calls and the use of automatic telephone dialing systems and prerecorded voice messages.[61] This act provided the authority for the Federal Communications Commission and the Federal Trade Commission to implement regulations to create a "Do-Not-Call" registry, which allows individuals to register their phone numbers as numbers that telemarketers are not allowed to call.[62]

II.2.13. Driver's Privacy Protection Act of 1994

The Driver's Privacy Protection Act of 1994 restricts the disclosure of personal information by state motor vehicle departments.[63] It prohibits disclosure of personal information about any individual obtained by a department in connection with a motor vehicle record without the express consent of the person to whom such information applies, except for certain specified

54 29 U.S.C. § 2006.

55 29 U.S.C. § 2007.

56 18 U.S.C. §§ 2710-2711 (2012).

57 Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C §§ 2510–22, 2701–11, 3121–27).

58 18 U.S.C. §§ 2510-2522 (2012).

59 18 U.S.C §§ 2701–11.

60 18 U.S.C. Sec. 2703.

61 47 U.S.C. § 227 (2012).

62 47 C.F.R. §§ 64.1200-.1202 (2017) (Federal Communications Commission rule); 16 C.F.R. § 310.4 (2018) (Federal Trade Commission rule).

63 18 U.S.C. §§ 2721-25 (2012).

permissible uses.[64] It also makes it unlawful for any person knowingly to obtain or disclose personal information from a motor vehicle record for any impermisible use.[65]

II.2.14. Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the primary statute providing for regulation of medical privacy in the US. HIPAA is a wide-ranging statute intended to address issues arising from the US's largely employment-based system of health insurance, such a requirement enabling persons between jobs to not be denied the opportunity to purchase insurance even if they have preexisting conditions.[66] Apart from that, HIPAA included a subtitle on "Administrative Simplication," which called for the US Department of Health and Human Services (HHS) to develop electronic data standards for transactions between health care providers and health insurance plans, and to establish regulations to ensure the integrity and confidentiality of electronic health information.[67] HHS became responsible for promulgating regulations to protect health information.

II.2.14.1 HIPAA Privacy Rule

The HIPAA Privacy Rule was promulgated in 2000, and republished with modifications in 2002.[68] It requires health insurance plans and health providers to establish procedures to protect personal health information from unauthorized disclosure.[69] It authorizes use or disclosure of "Protected Health Information" (PHI) in certain circumstances, but otherwise prohibits covered entities from disclosing such information.[70] For circumstances not listed as those in which disclosure is authorized, covered entities must obtain the subject's written authorization before disclosing PHI.[71] The Privacy Rule also gives individuals certain rights, including the right to obtain a copy of their medical information and the right to correct erroneous information.[72]

Covered entities may use or disclose PHI for their own treatment, payment, or health care operations, and may disclose PHI for another entity's health care operations if the subject of the PHI has a relevant relationship to the entity.[73] Disclosure of PHI may also be made for certain "national priority purposes" not related to the subject's treatment, such as public health activities, evidence of neglect or domestic violence, law enforcement, research approved by an Inistutitonal Review Board, or workers' compensation administration.[74]

Covered entities must meet various administrative requirements, such as providing subjects with written notice of their rights, and administrative safeguards to protect PHI from unauthorized use or disclosure.[75]

Because so much health insurance in the US is sponsored by employers, the Privacy Rule addresses the circumstances under which an insurer can disclose PHI to an employer. PHI may

---

64 18 U.S.C. § 2721.

65 18 U.S.C. § 2722.

66 Public Law No. 104-191, 110 Stat. 1936 (1996), codified in scattered provisions throughout the U.S. Code.

67 Public Law No. 104-191, title II, subtitle F, sections 261-264, codified at 42 U.S.C. §§ 1320d-1320d-9.

68 U.S. Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462 (2000); Standards for Privacy of Individually Identifiable Health Information, as amended, 67 Fed. Reg. 53,182 (2002).

69 45 C.F.R. § 164.530(c).

70 45 C.F.R. § 164.502(a).

71 45 C.F.R. § 164.508(a).

72 45 C.F.R. §§ 164.524, 164.526.

73 45 C.F.R. § 164.522(a).

74 45 C.F.R. § 164.512.

75 45 C.F.R. §§ 164.520, 164.530(c).

be disclosed to an employer for plan administration purposes, but prohibits disclosure for employment-related actions like promotion or termination. Employers must establish procedures to ensure that the only personnel who have access to PHI are those who need the information for authorized administrative purposes.[76]

II.2.14.2 HIPAA Security Rule

A separate set of regulations called the HIPAA Security Rule governs electronic Protected Health Information (ePHI).[77] The Security Rule requires covered entities to implement safeguards to protect ePHI from unauthorized access, alteration, deletion, and transmission.[78] The rules set forth standards, some of which are required, others of which are "addressable" (which covered entities must consider whether they are appropriate in their environment).[79]

The standards are categorized as administrative safeguards, physical safeguards, or technical safeguards. Adminstrative safeguards include implementing policies to prevent and correct security violations, appointing a responsible security official, establishing policies to ensure the right employees have access to ePHI and that other employees cannot gain access, establishing procedures for authorizing access, implementing a security awareness and training program, implementing policies to address security incidents, establishing a contingency plan for responding to emergencies, performing periodic evaluations, and obtaining contractual assurances that business associates will comply with safeguards.[80]

Physical safeguards include implementing procedures to limit physical access to ePHI systems and facilities and policies on procedures at workplaces.[81]

Technical safeguards include implementing technical policies to allow access to ePHI systems only to those persons or programs with access rights, establishing auditing control mechanisms for recording and examining activity in ePHI systems, implementing procedures to protect ePHI from improper destruction, implementing procedures to verify the identity of persons or entities seeking access, and implementing technical security measures to guard against unauthorized access to ePHI transmitted over communications networks.[82]

II.2.15. Children's Online Privacy Protection Act of 1998

The Children's Online Privacy Protection Act of 1998 authorizes the Federal Trade Commission (FTC) to promulgate regulations to protect children under the age of thirteen from the collection of personal information on the internet.[83] The statute provides for regulations requiring operators of websites directed at children under thirteen to post an online privacy policy describing their information practices for collecting personal information from children online, and to provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children.[84] The regulations must provide parents access to their child's personal information to review or have the information deleted, and to prevent further use or online collection of a child's personal

---

76 45 C.F.R. § 164.504(f).

77 U.S. Department of Health and Human Services, Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (2003), https://www.gpo.gov/fdsys/pkg/FR-2003-02-20/pdf/03-3877.pdf.

78 *Id*. at 8335.

79 45 C.F.R. § 164.306(d)(3).

80 45 C.F.R. § 164.308.

81 45 C.F.R. § 164.310.

82 45 C.F.R. § 164.312.

83 15 U.S.C. §§ 6501-6506 (2012). The FTC's regulations implementing this statute appear at 16 C.F.R. §§ 312.1-.13 (2018).

84 15 U.S.C. § 6502(b)(1).

information.[85] They must also maintain the confidentiality and security of information they collect from children.[86]

II.2.16. Gramm-Leach-Bliley Act of 1999

The Gramm-Leach-Bliley Act of 1999 (GLB Act) was intended to "modernize" the regulation of financial institutions, most notably by removing legal barriers that previously existed preventing the mergers of different categories of financial institutions like commercial banks, securities firms and insurance companies.[87] Because of concerns about the impact of mergers of these financial institutions on financial privacy, the GLB Act included privacy provisions.[88] It requires financial institutions to give annual privacy notices informing customers of their privacy practices.[89] It requires financial institutions to allow customers to opt out from permitting their personal information from being shared between non-affiliated companies.[90] It also requires financial institutions to develop data security practices.[91]

II.2.17. Federal Trade Commission Act

In addition to the foregoing sectoral privacy laws, another source of privacy regulation is a general consumer protection provision in the Federal Trade Commission Act (FTC Act), which is the organic statute originally enacted 1914 to establish the FTC and empower it.[92] The FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce,"[93] and the FTC has authority to enforce this prohibition on unfair or deceptive commercial practices both administratively and judicially.[94] The FTC has used this general authority to undertake enforcement actions against companies for deceptive practices with respect to their privacy policies or for failing to maintain security for sensitive consumer information.[95]

In the US sectoral framework for privacy regulation, the FTC is the closest version the US has to an agency with general enforcement responsibility.

II.3. State Privacy Laws

In addition to the foregoing federal laws on privacy, states have their own privacy laws. In the US federal system, federal law sets a floor below which privacy protections may not go, but states may impose greater protection that provided in federal law.

II.3.1. Privacy Provisions in State Constitutions

Ten states — Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington — have explicit privacy provisions in their constitutions.[96] For

---

85 15 U.S.C. § 6502(b)(2).

86 15 U.S.C. § 6502(b)(1)(D).

87 Public Law No. 106-102, 113 Stat. 2338 (1999) (codified in scattered sections of titles 12 and 15 of the U.S. Code).

88 15 U.S.C. §§ 6801-09 (2012).

89 15 U.S.C. § 6803.

90 15 U.S.C. § 6802.

91 15 U.S.C. § 6801.

92 15 U.S.C. §§ 41-58 (2012).

93 15 U.S.C. § 45(a)(1).

94 15 U.S.C. §§ 45(b), 53(b), 57b.

95 *See* FEDERAL TRADE COMMISSION, PRIVACY AND SECURITY ENFORCEMENT, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Sept. 2, 2018) (compiling press releases describing privacy and security enforcement settlements).

96 The state constitutional clauses on privacy are compiled in *Privacy Provisions in State Constitutions*, NATIONAL CONFERENCE OF STATE LEGISLATURES (May 5, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

example, California's Constitution, in the very first clause after the preamble, states: "All people are by 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*."[97] These state constitutional provisions provide a textual basis for these states' courts to provide broader privacy protection than granted under federal constitutional law.

II.3.2. State Privacy Statutes

While only ten states have constitutional provisions explicitly addressing privacy, all states have enacted various legislation affecting privacy. An early type of state privacy statute prohibited interception or disclosure of disclosing telegraph messages.[98] In more recent years it has become common for state governments to enact statutes on various contemporary aspects of privacy, including laws prohibiting spyware,[99] the criminalization of identity theft,[100] remedies for victims of identity theft,[101] notification of security breaches,[102] regulation of the privacy practices of internet service providers,[103] protection of the privacy of financial information,[104] prohibiting the disclosure of Social Security numbers,[105] privacy of social media accounts,[106] and authorizing tort law causes of action for invasions of privacy.[107]

As this list illustrates, US states, like the federal government, have typically approached privacy rights in a piecemeal, sectoral manner. However, one state, California, recently enacted a comprehensive privacy act, known as the California Consumer Privacy Act of 2018 (CCPA).[108]

---

97 CAL. CONST. art. 1, § 1 (emphasis added).

98 *See, e.g.*, Law of May 9, 1867, ch. 871, 1867 N.Y. LAWS 2186 ("If any person shall willfully open, read or cause to be opened or read, any sealed letter or telegraphic dispatch or message not addressed to himself, without the permission of the person to whom it shall be addressed or of the writer thereof, or other person having the right to give such permission, he shall, upon conviction thereof, be adjudged guilty of a misdemeanor ... .").

99 Twenty states and two US territories that have laws targeting spyware are listed in *State Spyware Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 25, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-spyware-laws.aspx.

100 *See, e.g.*, N.Y. PENAL LAW §§ 190.77-.84 (2018) (defining offenses involving identity theft, including first degree, second degree, third degree, and aggravated identity theft).

101 *See, e.g.*, CAL. PENAL LAW § 530.6 (2018) (providing for expedited judicial determination of the factual innocence of a victim of identity theft); CAL. CIVIL CODE § 1798.93 (2018) (providing for the right of identity theft victim sued for non-payment of debt to file a cross-complaint to establish the debt was created by identity theft).

102 *See, e.g.*, N.Y. GEN. BUS. LAW § 899-aa (2018) (requiring any business possessing computerized data with private information to expeditiously disclose any breach of the security of the system following discovery or notification of the breach to any resident whose private information was acquired by a person without valid authorization).

103 Information on states that have enacted measures requiring internet service providers to keep specified information confidential appears in *Privacy Legislation Related to Internet Service Providers - 2018*, NATIONAL CONFERENCE OF STATE LEGISLATURES (May 8, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx.

104 *See, e.g.*, MASS. GEN. LAWS ch. 167B, § 16 (2018) (prohibiting disclosure of information regarding any bank account or electronic fund transfer to any person except under specified circumstances).

105 *See, e.g.*, MASS. GEN. LAWS ch. 167B, § 14 (2018) ("The consumer's United States Social Security number shall not be used as a central information file number, personal identification number, primary financial account number, or a subpart thereof.").

106 State laws preventing employers and educational institutions from requiring access to employees' or students' social media accounts are compiled in *State Social Media Privacy Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 2, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx.

107 *See, e.g.*, WIS. STAT. § 995.50 (2018) (authorizing civil action for damages resulting from an invasion of privacy).

108 Assemb. Bill 375, 2017-2018 Reg. Sess., Ch. 55, Sec. 2 (Cal. 2018), adding CAL. CIV. CODE §§ 1798.100-.198.

The law, which will grant consumers a number of new privacy rights and will impose significant new responsibilities on businesses, is scheduled to become effective January 1, 2020.[109]

The CCPA grants new rights to "consumers," defined as natural persons who are California residents, with respect to their "personal information," which is defined very broadly to include all personal information collected in any manner, not just electronically, by a business from consumers.[110] The CCPA imposes responsibilities on businesses meeting certain size thresholds.[111]

The rights granted by the CCPA to consumers include:

> (1) The right of Californians to know what personal information is being collected about them.
>
> (2) The right of Californians to know whether their personal information is sold or disclosed and to whom.
>
> (3) The right of Californians to say no to the sale of personal information.
>
> (4) The right of Californians to access their personal information.
>
> (5) The right of Californians to equal service and price, even if they exercise their privacy rights.[112]

The CCPA will require businesses to affirmatively make disclosures to consumers regarding what personal information businesses will collect about consumers and the purpose for which the information will be used.[113] It will also require businesses to provide the consumer upon request the specific personal information the business has collected.[114]

The CCPA will give consumers the right to request the deletion of personal information from a business's records and to request the business to direct any service providers to delete the consumer's personal information from their records.[115] Certain categories of personal information will be exempt from the obligation of the business to delete, such as information needed to complete a transaction or maintain a customer relationship, to maintain data security, or to comply with other legal requirements.[116]

The CCPA will give consumers the right to opt out of the sale of their personal information to third parties.[117] It makes it illegal to sell personal information of children unless their parents (in the case of children under 13) or the children themselves (in the case of children between 13 and 16) have affirmatively opted in.[118]

The CCPA will prohibit businesses from discriminating in terms of service or price against individuals who exercise their privacy rights.[119] Businesses will, however, be allowed to provide

---

[109] CAL. CIV. CODE § 1798.198(a).

[110] CAL. CIV. CODE §§ 1798.140(o). The broad definition of personal information includes numerous categories of information about a person, including browsing history and search history, and inferences drawn from other information to create a consumer profile. It excludes public information.

[111] CAL. CIV. CODE § 1798.140(c).

[112] Assemb. Bill 375, § 2(i).

[113] CAL. CIV. CODE § 1798.100(b).

[114] CAL. CIV. CODE §§ 1798.100(c), (d); 1798.110.

[115] CAL. CIV. CODE § 1798.105.

[116] CAL. CIV. CODE § 1798.105(d).

[117] CAL. CIV. CODE § 1798.120(a).

[118] CAL. CIV. CODE § 1798.120(d).

[119] CAL. CIV. CODE § 1798.125(a)(1).

different levels of service or charge different prices where there is a relationship to the "value provided to the consumer by the consumer's data."[120]

The law generally will be enforced by the California Attorney General.[121] However, there will be a private right of action by consumers in the case of security breaches caused by a business's negligence in implementing reasonable security procedures and practices.[122]

[120] CAL. CIV. CODE § 1798.125(b).

[121] CAL. CIV. CODE § 1798.155.

[122] CAL. CIV. CODE § 1798.150.

III. The most relevant US case law

The United States is a common law country where law often develops through the evolution of case law (sometimes interpreting constitutional or statutory text). There are two primary types of privacy law that have developed through case law: the constitutional right to privacy and privacy tort law.

III.1. Constitutional Right to Privacy

The Supreme Court has established that among the rights established by the US Constitution are certain rights to privacy. Constitutional rights in the US generally preserve liberty only against governmental action.

The forms of constitutional rights to privacy recognized in the US include:

- the right to be free of unreasonable searches and seizures;
- privacy in the nature of personal autonomy to make decisions without governmental interference, which protects autonomous decisions regarding contraception, abortion, intimate relations, and family life;
- informational privacy; and
- privacy with respect to freedom of association.

III.1.1. Privacy as Freedom from Unreasonable Searches and Seizures

The Fourth Amendment right to be free from unreasonable searches and seizures is the source of a rich privacy jurisprudence.

In an 1878 decision, *Ex parte Jackson*, the Supreme Court stated that the Fourth Amendment protected sealed letters and packages in the mail, which could not be opened by the government: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be," including the mail.[123]

Another early case on the Fourth Amendment right to privacy was the 1886 case of *Boyd v. United States*,[124] which involved a federal statute that authorized federal courts, in suits for forfeitures under revenue and customs laws, to require production of private documents or have the allegations of the government deemed to be admitted. The law did not involve an actual search and seizure, but the Court ruled that compulsory production of a person's private papers to be used in evidence against him in a forfeiture proceeding amounted to the same thing.[125] It ruled that the law violated the Fourth Amendment, as well as the Fifth Amendment's clause against self-incriminaton.[126]

In the 1914 case of *Weeks v. United States*, the Court ruled that papers illegally obtained by federal officers could not be used in federal trials.[127]

A Court majority backtracked from a robust reading of a Fourth Amendment right to privacy in the 1928 case of *Olmstead v. United States*.[128] That case involved defendants' effort to suppress evidence gained by wiretapping — in violation of state law — conversations of defendants involved in a scheme to illegally transport alcoholic beverages into the United States from

---

123 *Ex parte Jackson*, 96 U.S. 727, 733 (1878).

124 *Boyd v. United States*,116 U.S. 616 (1886).

125 *Id.* at 634-35.

126 *Id.*

127 *Weeks v. United States*, 232 U.S. 383 (1914).

128 *Olmstead v. United States*, 277 U.S. 438 (1928).

British Columbia. (This was during America's failed experiment with alcohol prohibition.) The majority ruled the wiretaps were not unconstitutional because the Fourth Amendment concerns searches of material things, like homes, papers, and personal effects, while a wiretap is done without entry into a house.[129]

Four justices dissented,[130] including Justice Brandeis, the co-author decades before of a famous law review article, *The Right of Privacy*, discussed in section IV.1 *infra*. Just as *The Right of Privacy* is one of the most important law review articles in US legal history, Justice Brandeis's dissent in Olmstead is considered one of the most important dissenting opinions.[131] He took the opportunity to give a stirring defense of privacy as a constitutional right rooted in fundamental US values:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.[132]

For several decades following Olmstead, Fourth Amendment doctrine continued to focus on intrusions to the home and searches of physical objects like papers. Under the *Olmstead* test, wiretapping by the Federal Bureau of Investigation became widespread, and the FBI used wiretapping to gather Intelligence on civil rights and political organizations.[133]

There were instances where Fourth Amendment violations were found using that test. For example, in the 1961 case of *Silverman v. United States*, the Court ruled that where the defendants' conversations were listened to by police by placement of an electronic listening device through a heating duct and into the premises occupied by the defendants, this unauthorized physical penetration into the premises violated the Fourth Amendment.[134]

That same year, in *Mapp v. Ohio*, the Supreme Court ruled that in all criminal proceedings (not just federal ones), evidence gathered in violation of the Fourth Amendment could not be used at trial.[135] This extended the holding of *Weeks v. United States* to state court proceedings.

A shift to a focus from intrusions upon property to the principle of privacy came in the landmark 1967 case of *Katz v. United States*.[136] *Katz* involved a defendant convicted of an illegal gambling

---

[129] *Id*. at 464 ("There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.").

[130] *Id*. at 469-71 (Holmes, J.); *id*. at 471-85 (Brandeis, J.); *id*. at 485-88 (Butler, J.); *id*. at 488 (Stone, J.).

[131] William C. Heffernan, *Privacy Rights*, 29 SUFFOLK U. L. REV. 737, 772 (1995) ("the origin of modern constitutional privacy law is to be found in a passage Justice Louis Brandeis included in his 1928 dissent in Olmstead v. United States ... .").

[132] 277 U.S. at 478-79.

[133] Congress prohibited wiretapping in the 1934 Communications Act, which made it illegal to divulge or publish the existence, contents, substance, purport, effect or meaning of such intercepted communication to any person. The Supreme Court affirmed that the prohibition applied to federal agents in *Nardone v. United States*, 302 U.S. 379 (1937). However, the government interpreted the law to permit it to use wiretapping for intelligence purposes, and the FBI surveilled domestic targets under that authority. Athan Theoharis, *FBI Wiretapping: A Case Study of Bureaucratic Autonomy*, 107 POL. SCI. Q. 102 (1992).

[134] *Silverman v. United States*, 365 U.S. 505, 511-12 (1961).

[135] *Mapp v. Ohio,* 367 U.S. 643 (1961).

[136] *Katz v. United States*, 389 U.S. 347 (1967). *Katz* was foreshadowed by a decision a few months earlier in *Berger v.*

offense based on the government's warrantless wiretap of a public telephone booth. In determining whether this violated the Fourth Amendment, the Court ruled that it was not necessary for a search to involve a physical intrusion on property. It stated that "the Fourth Amendment protects people, not places," and rights under the Fourth Amendment may extend to that which one "seeks to preserve as private, even in an area accessible to the public."[137]

Justice Harlan wrote a concurring opinion elaborating that "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[138] Justice Harlan's test became the standard for evaluating Fourth Amendment claims.[139]

While *Katz* changed the method of analysis, the Supreme Court sometimes read the *Katz* test quite narrowly. For example, in the case of *United States v. Miller*, the Court held that a bank depositor had no reasonable expectation of privacy in financial records, including copies of checks held by his bank, because they only contained information voluntarily conveyed to the bank in the ordinary course of business.[140] Congress enacted a statute, the Right to Financial Privacy Act of 1978, discussed in section II.2.4 *supra*, partly in response to the *Miller* decision, but the *Miller* decision stands more generally for the principle that one cannot have a reasonable expectation of privacy in documents voluntarily turned over to third parties.

The Supreme Court continues to apply the *Katz* reasonable expectation of privacy test as technological advances increase the government's ability to conduct surveillance. In *Kyllo v. United States*, the Court held that police use of a thermal imager to detect heat from a home required a warrant.[141] In *Riley v. California*, the Court held that police typically needed a warrant to search the contents of a cell phone.[142] In *United States v. Jones*, the Court held that the placement of a GPS tracker on a car to track a car's movement constituted a search requiring a warrant, observing that *Katz*'s reasonable expectation of privacy test did not foreclose government trespasses onto property as a Fourth Amendment violation.[143] In 2018, in *Carpenter v. United States*, the Court again reaffirmed *Katz* — and again invoked Justice Brandeis's *Olmstead* dissent — in ruling that the government's acquisition without a warrant of cell-site records from wireless carriers to track a suspect's location over the course of several weeks violated the Fourth Amendment.[144]

III.1.2. Privacy as Personal Autonomy

The Supreme Court has ruled that the right of privacy protects the right to make personal decisions on matters involving personal autonomy or intimate or familial relations free from government interference.

The Supreme Court recognized privacy as freedom from bodily intrusions as early as 1891 in *Union Pacific Railway Co. v. Botsford*.[145] That case involved a woman who sued Union Pacific Railway for personal injuries. The railway sought to compel the woman to be examined by a

---

New York, 388 U.S. 41 (1967), in which the Court ruled that a New York law that authorized electronic eavesdropping approved by warrant with insufficient procedural safeguards violated the Fourth Amendment.

137 *Id.* at 351.

138 *Id.* at 361.

139 Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. L. REV. 139, 144-47 (2016), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1264&context=nulr.

140 *United States v. Miller*, 425 U.S. 435, 442 (1976).

141 *Kyllo v. United States*, 523 U.S. 27 (2001).

142 *Riley v. California*, 134 S. Ct. 2473 (2014).

143 *United States v. Jones*, 565 U.S. 400 (2012).

144 *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

145 *Union Pacific Railway Co. v. Botsford*, 141 U.S. 250 (1891).

doctor to determine the extent of her injuries, but the trial court refused to order the examination. The railway appealed. The Supreme Court affirmed, holding that the federal courts lacked authority to compel such an examination. In so ruling the Court stated: "No right is held more sacred, or more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from restraint or interference of others, unless by clear and unquestionable authority of law."[146]

The landmark 1965 decision of *Griswold v. Connecticut* explicitly rested on the right to privacy in striking down a Connecticut law that prohibited the use of contraceptives and prevented anyone from giving information about contraception.[147] The Court reversed Connecticut's conviction of the executive director of the local Planned Parenthood chapter for giving information about contraception to married persons. The lead opinion by Justice William O. Douglas noted that while there is no explicit recognition in the Constitution of a right to privacy, the "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy."[148] Justice Douglas wrote that "zones of privacy" were created by the First Amendment's guarantee of the right to free association, the Third Amendment's prohibition against the quartering of soldiers in homes during peacetime, the Fourth Amendment's right against unreasonable searches and seizures, and the Fifth Amendment's right against self-incrimination. He also noted the Ninth Amendment's statement that the enumeration of rights in the Constitution shall not be interpreted to deny the existence of other rights.[149] The Court said the idea of allowing the police "to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives ... is repulsive to the notions of privacy surrounding the marriage relationship."[150] A concurring opinion by Justice Goldberg argued that the right of privacy was a right that was preserved by the Ninth Amendment as an unenumerated right.[151] Another concurring opinion, by Justice Harlan, argued that the right to privacy was derived from the Due Process Clause of the Fourteenth Amendment.[152]

In 1969, in *Stanley v. Georgia*, the Supreme Court ruled that the right to privacy prevents the government from making it illegal to have obscene materials in the home.[153] Because the materials in question were obscene, their production and distribution were not protected by the First Amendment right to free speech.[154] The Court ruled, however, that possession of obscene materials in one's home was protected by "the right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy."[155] The Court indicated the aspect of the right to privacy at issue in this case — "the right to read or observe what [one] pleases ... in the privacy of [one's] own home"[156] — was derived from the First and Fourteenth Amendments to the Constitution.[157]

In 1972, the Court in *Eisenstadt v. Baird* held that the right to privacy with respect to the use of birth control extended to unmarried persons.[158] The Court stated that "[i]f the right of privacy

146 *Id.* at 484.

147 *Griswold v. Connecticut*, 381 U.S. 479 (1965).

148 *Id.* at 484.

149 *Id.*

150 *Id.* at 485-86.

151 *Id.* at 486-99.

152 *Id.* at 499-502.

153 *Stanley v. Georgia*, 394 U.S. 557 (1969).

154 *Id.* at 560.

155 *Id.* at 564.

156 *Id.* at 565.

157 *Id.* at 568.

158 *Eisenstadt v. Baird*, 405 U.S. 438 (1972).

means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child."[159]

In 1973, the Supreme Court addressed the right of privacy in the context of abortion. In *Roe v. Wade*,[160] the Court ruled that "[t]he right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty [or] in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy."[161] In 1992, in *Planned Parenthood of Southeastern Pennsylvania v. Casey*, the Court affirmed the central holding of *Roe v. Wade* that women had the right to an abortion, while changing the standard of review from "strict scrutiny" to an "undue burden" standard, and altering the analytical framework to give greater emphasis to women's liberty under the Fourteenth Amendment's Due Process Clause rather than the privacy between a woman and her doctor.[162]

In 1986, in the case of *Bowers v. Hardwick*, a gay man was convicted under a Georgia state law criminalizing sodomy; he argued his conviction violated the right to privacy.[163] The Court ruled against him in 5-4 decision; the majority invoked a supposed historical tradition in America of criminalizing homosexual intimacy as the basis for finding that the right to privacy did not extend to it.[164] *Bowers v. Hardwick* was overturned in *Lawrence v. Texas*, in which the Court said that under the Due Process Clause, "[t]he petitioners are entitled to respect for their private lives. The State cannot demean their existence or control their destiny by making their private sexual conduct a crime."[165]

In recent years, the Supreme Court at times has decided cases involving personal autonomy matters without invoking the right to privacy. For example, in *Windsor v. United States*, the Court declared unconstitutional a federal law that outlawed same-sex marriage.[166] The majority opinion was based not on the right to privacy, but rather "a deprivation of the liberty of the person protected by the Fifth Amendment."[167] Similarly, in *Obergefell v. Hodges*, in which the Court ruled there was a federal constitutional right to same-sex marriage, the holding was based on the Due Process and Equal Protection Clauses of the Fourteenth Amendment.[168]

III.1.3. Informational Privacy

The Supreme Court has issued decisions indicating that a constitutional right to informational privacy may exist, but it has never found such a right to have been violated. Only intermediate appellate courts have found violations of the constitutional right to informational privacy. The contours of the right are thus unsettled.[169]

In 1977, the Supreme Court stated in *Whalen v. Roe* that the "zone of privacy" protected by the Constitution includes "the individual interest in avoiding disclosure of personal matters," as

---

[159] *Id.* at 453.

[160] *Roe v. Wade*, 410 U.S. 113 (1973).

[161] *Id.* at 153.

[162] *Planned Parenthood of Southeastern Pennsylvania v. Casey*, 505 U.S. 833 (1992).

[163] *Bowers v. Hardwick*, 478 U.S. 186 (1986).

[164] *Id.* at 192-94.

[165] *Lawrence v. Texas*, 539 U.S. 558, 579 (2003).

[166] *Windsor v. United States*, 570 U.S. 744 (2013).

[167] *Id.* at 774.

[168] *Obergefell v. Hodges*, 135 S. Ct. 2584, 2604-05 (2015).

[169] *See discussion in* Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U.L. REV. 159, 177-89 (2015), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1226&context=nulr.

well as "the interest in independence in making certain kinds of important decisions."[170] That case involved a challenge to a New York state law that required copies of prescriptions of regulated drugs, including the names and addresses of patients, be provided to the state, but the law forbid disclosure of the information to the public.[171] The Court held that disclosures of personal information pertaining to drug use to representatives of the state having responsibility for the health of the community did not by itself automatically amount to an impermissible invasion of privacy,[172] and the law's statutory scheme and implementing administrative procedures preventing disclosure to the public were sufficient to protect the individual's interest in privacy.[173]

A second Supreme Court case on the constitutional right to informational privacy, *Nixon v. Administrator of General Services*, involved President Richard Nixon's challenge to a law that provided for the National Archives to take possession of and screen the President's papers and tape recordings, archive and make available those of historical interest, and return personal materials to the President.[174] President Nixon filed suit, arguing, among other things, that this violated his right to privacy.[175] The Court ruled that while the President had a legitimate expectation of privacy in his personal communications, the statute was constitutional in light of the limited intrusion of the screening process, the President's status as a public figure, the fact that the vast majority of the materials were governmental rather than personal, and the difficulty of segregating the small quantity of private materials without comprehensive screening.[176]

The third Supreme Court case on the constitutional right to informational privacy, *National Aeronautics and Space Administration v. Nelson,* involved longtime employees of a contractor to a federal agency who objected to the imposition of new background-check requirements as a condition of employment, including questions about recent drug use and counseling or treatment for any such drug use.[177] The Court assumed without deciding that a constitutional informational privacy right existed,[178] but ruled that the background-check requirements did not violate this right, because of the government's strong interest in conducting background checks on employees of contractors,[179] and the presence of legal mechanisms to prevent public disclosure of the information.[180]

While the Supreme Court has never ruled affirmatively in a constitutional right to informational privacy case, several federal appellate courts have affirmed such a right.[181] The US Court of Appeals for the Ninth Circuit recognizes the constitutional right to informational privacy as a conditional right that may be infringed upon a showing of proper governmental interest.

> We balance the following factors to determine whether the governmental interest in obtaining information outweighs the individual's privacy interest: (1) the type of information requested, (2) the potential for harm in any subsequent non-consensual disclosure, (3) the adequacy of safeguards to prevent unauthorized

[170] *Whalen v. Roe,* 429 U.S. 589, 599-600 (1977).

[171] *Id*. at 593-95.

[172] *Id*. at 602.

[173] *Id*. at 605.

[174] *Nixon v. Administrator of General Services*, 433 U.S. 425 (1977).

[175] *Id*. at 455-65.

[176] *Id*. at 465.

[177] *National Aeronautics And Space Administration v. Nelson,* 562 U.S. 134 (2011).

[178] *Id*. at 138.

[179] *Id*. at 151-55.

[180] *Id*. at 155-59.

[181] Scott Skinner-Thompson, *Outing Privacy*, *supra* note 169, at 184-89.

> disclosure, (4) the degree of need for access, and (5) whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.[182]

The Ninth Circuit has thus found, for example, that the constitutional right of informational privacy renders a state law requiring abortion providers to give unredacted patient records to a state agency unconstitutional, where safeguards to prevent unauthorized disclosure were inadequate and there was little need for for the agency to have such unredacted information.[183]

III.1.4. Privacy in Freedom of Association

Another body of constitutional case law involving privacy derives from the right to freedom of association under the First Amendment. In *National Association for the Advancement of Colored People v. Alabama*, the State of Alabama obtain the membership list of the civil rights organization as part of its effort to suppress the group.[184] The Supreme Court stated that "[t]his Court has recognized the vital relationship between freedom to associate and privacy in one's associations ... Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[185]

III.2. Tort Law

During the early years in which photography was emerging as a new technology, legal commentary such as that described in section IV.1 below began considering how tort law might respond to the distribution of photographs that were not authorized by the subject. For example, a New York trial court held that the unauthorized publication of an actor's photograph in a contest implicated the right "to be let alone," and granted an injunction against further publication.[186] However, in 1902, the New York Court of Appeals reversed a judgment awarded a woman whose image had been used in an advertisement, holding that "the so-called "right of privacy' has not as yet found an abiding place in our jurisprudence, and ... cannot now be incorporated without doing violence to settled principles of law by which the profession and the public have long been guided."[187]

The first state supreme court to recognize a tort for violation of privacy was the Georgia Supreme Court, which upheld a claim by a plaintiff against an insurance company for the unauthorized use of a photograph of him in an advertisement.[188] The court said that "the law recognizes within proper limits, as a legal right, the right of privacy, and ... the publication of one's picture without his consent by another as an advertisement, for the mere purpose of increasing the profits and gains of the advertiser, is an invasion of that right."[189]

The privacy tort gradually spread to other states around the country in cases like *Edison v. Edison Polyform and Manufacturing Co*., a New Jersey case in which the inventor was granted an injunction against a business using his image and name;[190] *Foster-Milburn Co. v. Chin*, a Kentucky case in which a drug manufacturer published an advertisement falsely indicating the

---

182 *Tuscon Woman's Clinic v. Eden*, 379 F.2d 531, 551 (9th Cir. 2004).

183 *Id*. at 552-53.

184 *National Association for the Advancement of Colored People v. Alabama*, 357 U.S. 449 (1958).

185 *Id*. at 462.

186 *Marks v. Jaffa*, 26 N.Y.S. 908, 909 (N.Y. Spec. Term 1893)

187 *Roberson v. Rochester Folding Box*, 171 N.Y. 538, 556; 64 N.E. 442 (1902).

188 *Pavesich v. New England Life Insurance Co*., 122 GA. 190, 50 S.E. 68 (Ga. 1905).

189 122 GA. at 220.

190 *Edison v. Edison Polyform and Manufacturing Co*., 73 N.J. EQ. 136 (1907).

plaintiff endorsed a product;[191] and *Munden v. Harris*, a Missouri case in which a man's picture was used in an advertisement without authorization.[192]

Over time the tort gained sufficient traction across the country so that in 1939, the American Law Institute deemed it a general principle of tort law that "[a] person who unreasonably and seriously interferes with another's interest in not having his affairs known to others or his likeness exhibited to the public is liable to the other."[193]

Following academic commentary by William Prosser discussed in section IV below, courts began conceptualizing the privacy tort as four distinct torts: intrusion upon seclusion,[194] false-light publicity,[195] disclosure of private facts,[196] and unauthorized appropriation of the name or likeness of another.[197] An overwhelming majority of the states of the US have recognized some or all of these torts.[198]

[191] *Foster-Milburn Co. v. Chin*, 134 KY. 424 (1909).

[192] *Munden v. Harris*, 134 S.W. 1076 (Mo. Ct. App. 1911).

[193] RESTATEMENT OF TORTS § 867 (Am. Law Inst. 1939).

[194] *See, e.g.*, *Housh v. Peth*, 165 Ohio St. 35, 133 N.E.2d 340 (1956) (Ohio Supreme Court decision recognizing cause of action for intrusion upon seclusion).

[195] *Rinsley v. Frydman*, 221 Kan. 297, 559 P.2d 334 (1977) (Kansas Supreme Court decision recognizing false light form of invasion of privacy).

[196] *See, e.g.*, *Robert C. Ozer, P.C. v. Borquez*, 940 P.2d 371 (Colo. 1997) (Colorado Supreme Court decision recognizing an invasion of privacy tort claim based on unreasonable publicity given to one's private life).

[197] *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231 (Minn. 1998) (Minnesota Supreme Court decision recognizing tort of unauthorized appropriation of name or likeness of another)

[198] Of the fifty states and the District of Columbia, 46 jurisdictions recognize the tort of intrusion upon seclusion, 42 recognize the tort of publicity given to private life; 33 recognize the tort of false light publicity; and 46 recognize the tort of appropriation of name or likeness. Joshua M. Greenberg, *The Privacy-Proof Plaintiff: But First, Let Me Share Your #Selfie*, 23 J.L. & POL'Y 689, 716 n. 141 (2015) (*citing* MEDIA LAW RESOURCE CENTER, MLRC 50-STATE SURVEY: MEDIA PRIVACY & RELATED LAW 1589-92 (2013-14 ed.)), https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1038&context=jlp.

IV. The nature of the right to respect for private life

IV.1. The Concept of the Right to Privacy in US Law

As the foregoing demonstrates, in US law, many different legal interests are encompassed within the right to privacy.

> Americans have chosen to label so many categories of legal interest as 'privacy' interests ... Americans and American law apply the term 'privacy' to mean: limited access to information, confidentiality, secrecy, anonymity, and data protection ('informational' privacy); limited access to persons, possessions, and personal property ('physical' privacy); decision-making about sex, families, religion, and health-care ('decisional' privacy); and control over the attributes of personal identity ('proprietary' privacy).[199]

As a result, scholars have struggled to define the essential attributes of the right to privacy.[200] Attempts by US scholars to define privacy include:

- "The condition of being protected from unwanted access by others — either physical access, personal information, or attention."[201]
- The right of persons "to conceal information about themselves that others might use to their disadvantage."[202]
- "[T]he realm in which an actor (either a person or a group, such as a couple) can legitimately act without disclosure and accountability to others."[203]
- "[T]he claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[204]
- The right that "protects the individual's interest in becoming, being, and remaining a person."[205]
- "[T]he fundamental freedom not to have one's life too totally determined by a progressively more normalizing state."[206]
- "[T]he state of the agent having control over decisions concerning matters that draw their meaning and value from the agent's love, caring or liking ... cover[ing] choices on the agent's part about access to herself, the dissemination of information about herself, and her actions."[207]

A leading US privacy law scholar, Daniel Solove, notes in US law, "privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."[208] As a result, Solove

---

[199] Anita L. Allen, *Privacy in American Law, in* PRIVACIES: PHILOSOPHICAL EVALUATIONS 19, 26 (Beate Rossler ed., 2004).

[200] DANIEL SOLOVE, UNDERSTANDING PRIVACY 12-38 (2008) (citing *inter alia* the definitions of privacy listed below).

[201] SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 10-11 (1983).

[202] RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 271 (1981).

[203] AMITAI ETZIONI, THE LIMITS OF PRIVACY 196 (1999).

[204] ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).

[205] Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 300, 314 (Ferdinand David Schoeman ed., 1984)

[206] Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 784 (1989), https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2568&context=fss_papers.

[207] JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 91 (1992).

[208] Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1088 (2002),

argues that efforts at locating a common core encompassing all ways in which privacy is used are likely to fail. Invoking Ludwig Wittgenstein's insight that not all concepts have a "core" or "essence,"[209] Solove argues persuasively that privacy is best conceptualized in terms of the different practices — activities, customs, norms, and traditions — that draw from a common pool of similar characteristics.[210]

One area of US privacy law that is well-theorized is the area of privacy tort law, discussed in section III.2 *supra*. The origin of this body of law is commonly attributed to a scholarly work that has often been called the most influential law review article in US legal history — *The Right to Privacy*, by Samuel Warren and Louis Brandeis, published in 1890.[211] Solove observes that this article "inspired significant interest in and attention to privacy; it spawned at least four common law tort actions to protect privacy; and it framed the discussion of privacy in the United States throughout the twentieth century."[212] The article, written two years after George Eastman introduced the first mass-produced Kodak camera, argued that it was necessary for the common law to address the fact that new technologies like photography and mass-produced newspapers threatened "the sacred precincts of private and domestic life," the invasions of which "subjected [individuals] to mental pain and distress far greater than could be inflicted by mere bodily injury."[213] They called for common law tort liability to protect an individual's "inviolate personality" from publication of information on the "private life, habits, acts, and relations of an individual [that] have no legitimate relation to or bearing upon any act done by him in a public or quasi public capacity."[214]

The work of the American Law Institute, an organization established to promote the clarification and simplification of the law and its better adaptation to social needs, played a significant role in the development of privacy law by recognizing the tort of privacy in 1939 in its RESTATEMENT OF TORTS, stating the principle that "[a] person who unreasonably and seriously interferes with another's interest in not having his affairs known to others or his likeness exhibited to the public is liable to the other."[215]

William Prosser, in a 1960 article, sought to bring analytical clarity to the tort law on privacy.[216] He argued that rather than a single tort protecting the right to privacy, there were four separate torts, "four distinct kinds of invasions of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff ... 'to be let alone.'"[217] The four separate torts identified by Prosser were:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.

---

https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview.

209 *Id.* at 1097-99 (*citing* LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS 66-71 (G.E.M. Anscombe trans., 1958)).

210 *Id.* at 1097-99.

211 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). It is the second most-frequently cited American law review article of all time. Fred R. Shapiro & Michelle Pearse, *The Most-Cited Law Review Articles of All Time*, 110 MICH. L. REV. 1483, 1489 (2012), https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1084&context=mlr.

212 Solove, *Conceptualizing Privacy*, *supra* note 208, at 1100.

213 4 HARV. L. REV. at 195.

214 *Id.* at 216.

215 RESTATEMENT OF TORTS § 867 (1939).

216 William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview.

217 *Id.* at 389.

4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[218]

The American Law Institute's RESTATEMENT (SECOND) OF TORTS in 1977 incorporated Prof. Prosser's identification of the four separate privacy-related torts, and set forth the standard elements of each.[219] State courts often rely on the Restatements in considering whether to recognize causes of action, and most states have now adopted the four forms of the privacy tort as outlined in the RESTATEMENT (SECOND) OF TORTS.

The privacy tort thus had a well-delineated path to conceptual development. Other aspects of the right to privacy in US law developed within their own conceptual spheres, albeit overlapping and borrowing from other privacy law concepts.[220]

IV.2. The status of the right to privacy in US law

Because there are many different interests embodied in the right to privacy in the US, there can be different answers to the question whether the right to privacy is fundamental. Fundamental rights in the US are those set forth either explicitly or impliedly in the US Constitution (or in a state constitution). The phrase "fundamental right" usually means a right recognized by the Supreme Court as subject to requiring a high level of judicial protection from government encroachment, such as rights subject to the "strict scrutiny" standard or other relatively stringent level of judicial review.[221] Rights based in tort such as those discussed in section III.2 and the statutory privacy rights discussed in section II.2 are not fundamental and their boundaries are provided for in the respective bodies of law governing them.

As discussed in section II.1, while the word "privacy" does not appear in the US Constitution, there are four senses in which it has been recognized as a constitutional right.

For example, the Fourth Amendment right to be free of unreasonable searches and seizures protects privacy in the sense of freedom from government surveillance, as discussed in section III.1.1. The right to be free from unreasonable searches and seizures is sometimes described as "fundamental," but the right falls far short of being absolute. Fourth Amendment doctrine rests largely on what constitutes a "reasonable expectation of privacy," which subjects the right to a context-dependent reasonableness inquiry that depends on circumstances and may evolve as new technologies develop.[222] Scholars have criticized the "reasonable expectation" test as circular: the government could prominently announce a massive surveillance program so that everyone had knowledge, which would render it unreasonable to expect privacy, even if such a program would clearly violate the purpose of the Fourth Amendment.[223] One strategy to avoid this circularity is to deny Fourth Amendment rights when information has been shared with third parties (as in the *United States v. Miller* decision discussed in section III.1.1 *supra*), but the third-party doctrine could enable the government to surveil massive amounts of

---

218 *Id.*

219 RESTATEMENT (SECOND) OF TORTS §§ 652B-652E (Am. Law Inst. 1977).

220 For a taxonomy of other recognized privacy violations, *see* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006), https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf.

221 *Fundamental Right*, LEGAL INFORMATION INSTITUTE: WEX LEGAL DICTIONARY, https://www.law.cornell.edu/wex/fundamental_right (last visited Sept. 4, 2018).

222 *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 804-05 (2004) https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1722&context=mlr.

223 *See* Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 106 (2008), https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2551&context=fss_papers ("Suppose the President announces that all telephone conversations will henceforth be monitored. Arguably, no one thereafter can reasonably expect privacy in his phone calls, and the announced eavesdropping will have constitutionalized itself.").

information about individuals in a digital information environment.[224] In short, while the right against unreasonable search and seizures is a foundational principle of US constitutionalism, the right is a limited one.

As discussed in section III.1.2 *supra*, the Supreme Court has determined there is an implied fundamental right to privacy that protects the right to make autonomous decisions on matters like contraception, abortion, etc. The line of cases finding an implied fundamental right to privacy have been controversial. In particular, *Roe v. Wade*, which struck down state laws limiting abortion by making access to abortion a federal constitutional right, is among the most controversial of Supreme Court cases. Its reasoning has been criticized by many legal scholars, including by some who approved of the result.[225] *Roe v. Wade*'s strict scrutiny standard for evaluating abortion restrictions was changed to an intermediate "undue burden" standard in *Planned Parenthood of Southeastern Pennsylvania v. Casey*. Impending changes to the personnel on the Supreme Court may soon lead to the right to abortion being overturned, or slowly chipped away as state restrictions on abortion are found to survive the undue burden standard.[226] If that happens, a right that was once called fundamental would no longer exist.

As noted in section III.1.3, while the Supreme Court has suggested, but never held, that there is a constitutional right to informational privacy, several federal appellate courts have affirmed such a right. Without Supreme Court guidance, the intermediate appellate courts have been split as to the extent of such a right, with courts typically finding it subject to countervailing considerations.[227]

Lastly, as discussed in section III.1.4 *supra*, there is a constitutional right to privacy in association, which, for example, protects organizations' membership lists from compelled disclosure. This right is not absolute; the Supreme Court has stated that where there is "a substantial relation between the information sought and a subject of overriding and compelling state interest," the right to associational privacy can be overcome.[228]

In sum, the constitutional right to privacy is considered "fundamental" in US law only in narrow contexts.

---

[224] *Id.* at 109-15; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1089-1117 (2002), http://www-bcf.usc.edu/~usclrev/pdf/075502.pdf.

[225] *See, e.g.*, Anita L. Allen, *The Proposed Equal Protection Fix for Abortion Law: Reflections on Citizenship, Gender, and the Constitution*, 18 HARV. J.L. & PUB. POLICY 419 (1994-1995), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1792&context=faculty_scholarship; Ruth Bader Ginsburg, *Some Thoughts on Autonomy and Equality in Relation to Roe v. Wade*, 63 N.C. L. REV. 375 (1985), https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=2961&context=nclr.

[226] For one legal journalist's speculation on this point, see Mark Joseph Stern, *How Brett Kavanaugh Will Gut Roe v. Wade*, SLATE (July 9, 2018), https://slate.com/news-and-politics/2018/07/how-brett-kavanaugh-will-gut-roe-v-wade.html.

[227] *See* Scott Skinner-Thompson, *Outing Privacy*, *supra* note 169, 110 NW. U. L. REV. at 184-89 (describing various intermediate appellate court approaches to evaluating claims to an informational privacy right).

[228] *See Gibson v. Florida Legislative Investigation Committee*, 372 U.S. 539, 546-48 (1963) (distinguishing cases where overriding state interest was present from case involving government demand for civil rights organization's membership list); *see generally* Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1 (1991), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2410&context=faculty_scholarship.

V. Conclusions

As shown above, the US approach to privacy regulation is sectoral in nature: instead of having a single omnibus law, separate laws regulate privacy matters in particular industries like health, financial services, and education. While the FTC has generalized enforcement authority under the FTC Act, there is no single entity with overall regulatory responsibility for privacy in the US.

Some have advocated that the US adopt an omnibus framework.[229] Daniel Solove, for instance, argues that the sectoral approach is characterized by complexity, inconsistency, and uncertainty, and the US should adopt at least a baseline omnibus privacy and data security law in order to "avoid needless complexity, close gaps, avoid overlap when it is not needed, and strive to eliminate inconsistency."[230]

Not all observers believe that a federal omnibus right would be optimal for regulating privacy. Paul Schwartz has argued that an omnibus federal statute that preempts state law and federal sectoral experimentation would be an unfortunate development.[231] He notes that state privacy law has been more innovative and responsive than federal law in various ways, for example in areas such as data breach notification requirements and providing relief for victims of identity theft.[232] He argues that states should be allowed to enact more protective privacy legislation, and speaks favorably of sectoral federal laws that set a "floor" for privacy, but which allow for more stringent state regulation. Sometimes federal sectoral legislation preempts state regulation and thus forestalls experimentation, however.[233] Schwartz argues as a fallback position that if a federal privacy law with preemptive effect were to be enacted, it should at least follow a preemption "plus one" strategy, which would allow one state to regulate at a more stringent level than the federal requirements, and allow other states to adopt the standard of that state. This would be modeled after the Clean Air Act's regulation of mobile source air pollution, which allows California to exceed federal emission standards.[234]

An omnibus privacy framework was proposed by the Obama Administration in 2012.[235] The Administration proposed draft legislation,[236] but Congress did not take action.[237]

A feature of the US privacy landscape is intermittent scandals that receive sustained media coverage, which sometimes lead to piecemeal legislative responses, but not a sustained rethinking of the sectoral framework.[238] Recently, however, a major privacy scandal served as

---

[229] Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 29 CONN. J. INT'L L. 257, 289-99 (2014); Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, PRIVACY + SECURITY BLOG (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/.

[230] Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, *supra* note 229.

[231] Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1071&context=facpubs.

[232] *Id*. at 919-20.

[233] *Id*. at 920-21.

[234] *Id*. at 945.

[235] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (Feb. 23, 2012), http://cdm266901.cdmhost.com/cdm/ref/collection/p266901coll4/id/3950.

[236] The WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT (2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[237] Natasha Singer, *Why a Push for Online Privacy Is Bogged Down in Washington*, N.Y. TIMES (Feb. 28, 2016), https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html. In its last week of office the Obama Administration published a report summarizing its efforts. THE WHITE HOUSE, PRIVACY IN OUR DIGITAL LIVES: PROTECTING INDIVIDUALS AND PROMOTING INNOVATION (Jan. 2017), https://iapp.org/media/pdf/resource_center/Privacy_in_Our_Digital_Lives.pdf.

[238] *See* Sandra Byrd Petersen, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?*, 48 FED. COMM. L.J. 163, 180-83 (1995), www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1096&context=fclj (noting how the Privacy Act of

the backdrop for California succeeding in passing an omnibus bill. In March 2018 it was reported that Cambridge Analytica, a British political consulting firm that worked on the presidential campaign of Donald Trump, obtained the data of tens of millions of Facebook users from an outside researcher who had bought the data from Facebook but shared the data with Cambridge Analytica in violation of his agreement with Facebook.[239] This scandal was one factor in the enactment of the most comprehensive privacy statute ever passed in the US, the California Consumer Privacy Act of 2018, described in section II.3.2 above.[240] Facebook had joined other companies in opposing the California legislation, but when the Cambridge Analytica news broke, Facebook stopped opposing the legislation.[241]

Now that California has enacted comprehensive privacy legislation, tech industry lobbyists reportedly are working on proposals for a federal privacy law that would nullify the California law.[242] An omnibus federal law that preempts state law is what Paul Schwartz has warned would stifle state regulatory experimentation in protecting privacy.[243]

1974, the Video Privacy Protection Act, and the Driver's Privacy Protection Act of 1994 were legislative reactions to well-publicized events highlighting regulatory shortfalls).

239 Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (March 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html; Andrew Prokop, *Cambridge Analytica Shutting Down: The Firm's Many Scandals, Explained*, VOX (May 2, 2018), https://www.vox.com/policy-and-politics/2018/3/21/17141428/cambridge-analytica-trump-russia-mueller.

240 Dana Simberkoff, *How Facebook's Cambridge Analytica Scandal Impacted the Intersection of Privacy and Regulation*, CMSWIRE (Aug. 30, 2018), https://www.cmswire.com/information-management/how-facebooks-cambridge-analytica-scandal-impacted-the-intersection-of-privacy-and-regulation/.

241 Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/.

242 Cecelia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html.

243 Schwartz, *Preemption and Privacy*, *supra* note 231.

List of statutes consulted

Act of February 20, 1792, 1 Stat. 232

Bank Secrecy Act of 1970, 12 U.S.C. §§ 1951 et seq. (2012)

Cable Communications Policy Act of 1984, 47 U.S.C. §§ 521-573 (2012)

California Consumer Privacy Act of 2018, Assemb. Bill 375, 2017-2018 Reg. Sess., Ch. 55, Sec. 2 (Cal. 2018), adding California Civil Code §§ 1798.100-.198

California Civil Code § 1798.93 (2018)

California Penal Law § 530.6 (2018)

Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2012)

Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (1934)

Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a(a)(8)-(13), (e)(12), (o), (p), (q), (r), (u) (2012)

Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (2012)

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), 18 U.S.C §§ 2510–22, 2701–11, 3121–27 (2012)

Employee Polygraph Protection Act of 1988, 29 U.S.C. §§ 2001-2009 (2012)

Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. §§ 1681c-1, 1681c-2 (2012)

Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 et seq. (2012)

Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2012)

Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2012)

Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1885c (2012)

Freedom of Information Act of 1966, 5 U.S.C. § 552 (2012)

Gramm-Leach-Bliley Act of 1999, Public Law No. 106-102, 113 Stat. 2338 (1999), 15 U.S.C. §§ 6801-6809 (2012)

Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191, 110 Stat. 1936 (1996)

Law of May 9, 1867, ch. 871, 1867 N.Y. LAWS 2186

Massachusetts General Laws ch. 167B (2018)

New York General Business Law § 899-aa (2018)

New York Penal Law §§ 190.77-.84 (2018)

Omnibus Crime Control and Safe Streets Act of 1968, Public Law No. 90-351, title III, 82 Stat. 212

Post Office Act of 1710, 9 Anne ch. 11

Privacy Act of 1974, 5 U.S.C. § 552a (2012)

Privacy Protection Act of 1980, 42 U.S.C. §§ 2000aa-2000aa12 (2012)

Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (2012)

Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2012)

Townshend Act of 1767, 7 Geo. III, ch. 46

Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710-2711 (2012)

Wisconsin Statutes § 995.50 (2018)

List of cases

Supreme Court of the United States

Berger v. New York, 388 U.S. 41 (1967)

Bowers v. Hardwick, 478 U.S. 186 (1986)

Boyd v. United States, 116 U.S. 616 (1886)

Carpenter v. United States, 138 S. Ct. 2206 (2018)

Gibson v. Florida Legislative Investigation Committee, 372 U.S. 539 (1963)

Griswold v. Connecticut, 381 U.S. 479 (1965)

Eisenstadt v. Baird, 405 U.S. 438 (1972)

Ex parte Jackson, 96 U.S. 727 (1878)

Katz v. United States, 389 U.S. 347 (1967)

Kyllo v. United States, 523 U.S. 27 (2001)

Lawrence v. Texas, 539 U.S. 558 (2003)

Mapp v. Ohio, 367 U.S. 643 (1961)

National Aeronautics And Space Administration v. Nelson, 562 U.S. 134 (2011)

National Association for the Advancement of Colored People v. Alabama, 357 U.S. 449 (1958)

Nixon v. Administrator of General Services, 433 U.S. 425 (1977)

Obergefell v. Hodges, 135 S. Ct. 2584 (2015)

Olmstead v. United States, 277 U.S. 438 (1928)

Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833 (1992)

Riley v. California, 134 S. Ct. 2473 (2014)

Roe v. Wade, 410 U.S. 113 (1973)

Silverman v. United States, 365 U.S. 505 (1961)

Stanley v. Georgia, 394 U.S. 557 (1969)

Union Pacific Railway Co. v. Botsford, 141 U.S. 250 (1891)

United States v. Jones, 565 U.S. 400 (2012)

United States v. Miller, 425 U.S. 435 (1976)

Weeks v. United States, 232 U.S. 383 (1914)

Whalen v. Roe, 429 U.S. 589 (1977)

Windsor v. United States, 570 U.S. 744 (2013)

Zurcher v. Stanford Daily, 436 U.S. 547 (1978)

Other Courts

Edison v. Edison Polyform and Manufacturing Co., 73 N.J. Eq. 136 (1907)

Foster-Milburn Co. v. Chin, 134 Ky. 424 (1909)

Housh v. Peth, 165 Ohio St. 35, 133 N.E.2d 340 (1956)

Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231 (Minn. 1998)

Marks v. Jaffa, 26 N.Y.S. 908 (N.Y. Spec. Term 1893)

Munden v. Harris, 134 S.W. 1076 (Mo. Ct. App. 1911)

Pavesich v. New England Life Insurance Co., 122 GA. 190, 50 S.E. 68 (Ga. 1905)

Rinsley v. Frydman, 221 KAN. 297, 559 P.2d 334 (1977)

Roberson v. Rochester Folding Box, 171 N.Y. 538; 64 N.E. 442 (1902)

Robert C. Ozer, P.C. v. Borquez, 940 P.2d 371 (Colo. 1997)

Tuscon Woman's Clinic v. Eden, 379 F.2d 531 (9th Cir. 2004)

Bibliography

Anita L. Allen, *Privacy in American Law, in* PRIVACIES: PHILOSOPHICAL EVALUATIONS (Beate Rossler ed., 2004).

Anita L. Allen, *The Proposed Equal Protection Fix for Abortion Law: Reflections on Citizenship, Gender, and the Constitution*, 18 HARV. J.L. & PUB. POLICY 419 (1994-1995), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1792&context=faculty_scholarship.

SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION (1983).

CONG. RESEARCH SERV., THE CONSTITUTION OF THE UNITED STATES OF AMERICA: ANALYSIS AND INTERPRETATION (cases decided through August 26, 2017), https://www.congress.gov/content/conan/pdf/GPO-CONAN-2017-10-5.pdf.

Anuj C. Desai, *Wiretapping before the Wires: The Post Office and the Rebirth of Communications Privacy*, 60 Stan. L. Rev. 553 (2007), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1079958.

Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181(2016), https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=5941&context=uclrev.

AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999).

Ruth Bader Ginsburg, *Some Thoughts on Autonomy and Equality in Relation to Roe v. Wade*, 63 N.C. L. REV. 375 (1985), https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=2961&context=nclr.

Joshua M. Greenberg, *The Privacy-Proof Plaintiff: But First, Let Me Share Your #Selfie*, 23 J.L. & POL'Y 689, (2015), https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1038&context=jlp.

William C. Heffernan, *Privacy Rights*, 29 SUFFOLK U. L. REV. 737 (1995).

JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION (1992).

Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 29 CONN. J. INT'L L. 257 (2014).

Cecelia Kang, Tech Industry Pursues a Federal Privacy Law, on Its Own Terms, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html.

Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1722&context=mlr.

Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1 (1991), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2410&context=faculty_scholarship.

FREDERICK S. LANE, AMERICAN PRIVACY: THE 400-YEAR HISTORY OF OUR MOST CONTESTED RIGHT (2009).

Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/.

Sandra Byrd Petersen, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?*, 48 FED. COMM. L.J. 163 (1995), www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1096&context=fclj.

RICHARD A. POSNER, THE ECONOMICS OF JUSTICE (1981).

Andrew Prokop, *Cambridge Analytica Shutting Down: The Firm's Many Scandals, Explained*, VOX (May 2, 2018), https://www.vox.com/policy-and-politics/2018/3/21/17141428/cambridge-analytica-trump-russia-mueller.

William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview.

Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY (Ferdinand David Schoeman ed., 1984).

RESTATEMENT OF TORTS (Am. Law Inst. 1939).

RESTATEMENT (SECOND) OF TORTS (Am. Law Inst. 1977).

Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (March 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101 (2008), https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2551&context=fss_papers.

Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737 (1989), https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2568&context=fss_papers.

Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1071&context=facpubs.

Fred R. Shapiro & Michelle Pearse, *The Most-Cited Law Review Articles of All Time*, 110 MICH. L. REV. 1483 (2012), https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1084&context=mlr.

Dana Simberkoff, *How Facebook's Cambridge Analytica Scandal Impacted the Intersection of Privacy and Regulation*, CMSWIRE (Aug. 30, 2018), https://www.cmswire.com/information-management/how-facebooks-cambridge-analytica-scandal-impacted-the-intersection-of-privacy-and-regulation/.

Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U.L. REV. 159 (2015), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1226&context=nulr.

Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview.

Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002), http://www-bcf.usc.edu/~usclrev/pdf/075502.pdf. Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, PRIVACY + SECURITY BLOG (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/.

Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006), https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf.

DANIEL SOLOVE, UNDERSTANDING PRIVACY (2008).

Mark Joseph Stern, *How Brett Kavanaugh Will Gut Roe v. Wade*, SLATE (July 9, 2018), https://slate.com/news-and-politics/2018/07/how-brett-kavanaugh-will-gut-roe-v-wade.html.

Athan Theoharis, *FBI Wiretapping: A Case Study of Bureaucratic Autonomy*, 107 POL. SCI. Q. 102 (1992).

Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. L. REV. 139 (2016), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1264&context=nulr.

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

ALAN WESTIN, PRIVACY AND FREEDOM (1967).

The WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT (2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (Feb. 23, 2012), http://cdm266901.cdmhost.com/cdm/ref/collection/p266901coll4/id/3950.

THE WHITE HOUSE, PRIVACY IN OUR DIGITAL LIVES: PROTECTING INDIVIDUALS AND PROMOTING INNOVATION (Jan. 2017), https://iapp.org/media/pdf/resource_center/Privacy_in_Our_Digital_Lives.pdf.

Consulted websites

FEDERAL TRADE COMMISSION, PRIVACY AND SECURITY ENFORCEMENT, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

Privacy Legislation Related to Internet Service Providers – 2018, NATIONAL CONFERENCE OF STATE LEGISLATURES (May 8, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx.

Privacy Provisions in State Constitutions, NATIONAL CONFERENCE OF STATE LEGISLATURES (May 5, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

State Social Media Privacy Laws, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 2, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx.

State Spyware Laws, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 25, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-spyware-laws.aspx.

This study forms part of a wider-ranging project which seeks to lay the groundwork for comparisons between legal frameworks governing the right to respect for private life in different legal systems, and between the ways in which the systems address the challenges that the 'digital age' poses to the exercise of that right.

It analyses, with reference to the United States and the subject at hand, the legislation in force, the most relevant case law and the nature of the right to respect for private life, ending with some conclusions on the challenges discussed.

Unlike jurisdictions that have adopted an omnibus approach to privacy protection, the US takes a sectoral approach to regulating privacy, with different regulatory regimes for different contexts and sectors of the economy. This report provides an overview of the different areas of law addressing privacy, including constitutional, statutory, and common law, as well as of relevant scholarly commentary. The report concludes with a summary of the current legislative outlook.

QA-04-18-838-EN-N

This is a publication of the Comparative Law Library Unit
EPRS | European Parliamentary Research Service

Print ISBN 978-92-846-3910-6 | doi:10.2861/66217 | QA-04-18-838-EN-C
PDF ISBN 978-92-846-3903-8 | doi:10.2861/096079 | QA-04-18-838-EN-N