IMPORTANT NOTICE:
This Publication Has Been Superseded

See the Most Current Publication at

https://thesedonaconference.org/publication/The_Sedona_Conference_Data_Privacy_Primer

The Sedona Conference Working Group Series

wgs

The Sedona Conference

Data Privacy Primer

A Project of The Sedona Conference
Working Group on Data Security and Privacy Liability (WG11)

January 2017
Public Comment Version
Submit comments by April 16, 2017, to
comments@sedonaconference.org.

The Sedona Conference Data Privacy Primer

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

JANUARY 2017 PUBLIC COMMENT VERSION

Author:	The Sedona Conference
Editor-in-Chief:	Corey M. Dennis
Senior Editors:	Elise Houlik
	Peter B. Miller
Contributors:	Jay Edelson
	Jennifer L. Hamilton
	Roy E. Leonard
	Dana L. Post
	Matthew F. Prewitt
	Caroline E. Reynolds
	Joe Sremack

We thank all of our Working Group Series Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, click on the "Sponsors" navigation bar on the homepage of our website.

Preface

Welcome to the public comment version of The Sedona Conference *Data Privacy Primer*, a project of The Sedona Conference Working Group Eleven on Data Security and Privacy Liability (WG11). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The work of WG11, The Sedona Conference's newest Working Group, began in late 2014, with an important mission—identification of and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages. We hope the *Data Privacy Primer* will be of immediate and practical benefit to these organizations and these practitioners.

The Sedona Conference acknowledges the efforts of Editor-in-Chief Corey Dennis, who has moved this project forward through its various stages, and senior editors Elise Houlik and Peter Miller, who were key in bringing this publication to fruition. We also thank contributors Jay Edelson, Jennifer Hamilton, Roy Leonard, Dana Post, Matthew Prewitt, Caroline Reynolds, and Joe Sremack for their efforts and commitments in time and attention to this project.

In addition to the drafters, this non-partisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts of the *Data Privacy Primer* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 annual and midyear meetings where drafts of the *Data Privacy Primer* were the subject of the dialogue. On behalf of The Sedona Conference, I thank all of them for their contributions.

Please note that this version of the *Data Privacy Primer* is open for public comment through April 16, 2017, and suggestions for improvement are very welcome. After the deadline for public comment has passed, the editors will review the public comments and determine what edits are appropriate for the final version. Please submit comments by email to comments@sedonaconference.org.

In addition, we encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, patent litigation best practices, data privacy and security, and other "tipping point" issues in the law. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
January 2017

Foreword

Unquestionably, the law of privacy and data protection has rapidly evolved over the past several years. This complex regulatory framework has become both challenging and esoteric to many, including practitioners, legislators, regulators, and courts alike. Recognizing the need for a useful privacy law guide, we developed the *Data Privacy Primer* ("Primer").

This Primer is intended to provide a practical framework and guide to basic privacy issues in the United States and to identify key considerations and resources, including key privacy concepts in federal and state law, regulations, and guidance. It is not an exhaustive treatment of federal or state privacy law or of any particular privacy-related issue, but instead provides a point of entry to privacy issues. This Primer focuses on privacy laws in the U.S., and as such, global privacy laws are outside the scope of its coverage, as is a comprehensive treatment of criminal laws relating to privacy and surveillance.

Discussions of privacy inevitably lead to discussions of definitions, principles, goals, and underlying intent. It is beyond the scope of a primer to resolve competing definitions of privacy, to harmonize the many policy and practical considerations required to apply privacy principles to day-to-day business activities, or to take a position about the wisdom (or lack thereof) of existing or planned privacy law. Instead, this Primer addresses privacy as it exists and attempts to provide background and context for understanding and interpreting current privacy laws and requirements.

This Primer is the result of extensive efforts and collaboration among the drafting team members, along with the assistance of many others. We would like to extend our sincere gratitude and appreciation to all WG11 members who contributed to the Primer. We particularly acknowledge Indira Cameron-Banks and Colman McCarthy for their outstanding contributions.

Table of Contents

I. INTRODUCTION

This Primer begins with a Background and Overview to provide context for the current privacy issues addressed in the main section. That context is found in the common law development of privacy rights in the United States, the Fair Information Practice Principles and similar privacy-protecting frameworks, and in progressive attempts to determine what constitutes personal information that is entitled to privacy protection. The principal focus of this Primer is on privacy issues arising under civil rather than criminal law. Although criminal law implications are addressed at various points in this Primer, a more systematic treatment of federal criminal law regarding privacy is outside the scope of this Primer.[1]

After laying that groundwork, the Primer is organized into substantive sections by broad privacy categories for ease of reference, with each such category describing key federal and state laws, policies, and considerations from both a compliance and a litigation perspective. Those categories include "Federal and State Governments," "General Consumer Protection," "Health," "Financial," "Workplace Privacy," and "Student Privacy."

[1] Recently, a number of federal criminal laws with privacy implications, including national security laws (such as the USA Patriot Act and the Foreign Intelligence Surveillance Act), the Computer Fraud and Abuse Act, and laws regarding access to personal communications and information about personal activities (such as the Communications Assistance for Law Enforcement Act and the Electronic Communications Privacy Act) have been the subject of extensive public and legislative scrutiny and debate as a result of the Edward Snowden disclosures and follow-on issues relating to transparency, access, and individual rights to privacy.

II. BACKGROUND AND OVERVIEW

This background information provides context for the legal and practical requirements discussed in the substantive privacy categories that follow this section.

A. Common Law of Privacy

No serious written discussion of the concept of privacy begins without a reference to the article by Samuel Warren and Louis Brandeis, published in the Harvard Law Review in 1890, titled "The Right to Privacy."[2] The article stands as the most influential article to advocate for a legal right to privacy.[3]

The article was inspired by a rapidly expanding form of media, the printed newspaper, and by concerns about a revolutionary technology, "instantaneous photograph[y]."[4] Warren and Brandeis were concerned about the lack of "protection of the person," and "for securing to the individual" the right "to be let alone."[5] "Instantaneous photographs and newspaper enterprise," they wrote, "have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[6]

As explained by Dean Prosser, "[p]iecing together old decisions in which relief had been afforded on the basis of defamation, or the invasion of some property right, or a breach of confidence or an implied contract, the article concluded that such cases were in reality based upon a broader principle which was entitled to a separate recognition. This principle they called the right to privacy."[7]

The privacy right conceptualized by Warren and Brandeis did not receive immediate judicial acceptance. It wasn't until fifteen years after publication of "The Right to Privacy" that the first state supreme court adopted the invasion of privacy cause of action. In 1905, the Supreme Court of

---

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

3 Over 100 years after it was published, the article was described as "brilliant" by the United States Court of Appeals for the Ninth Circuit in *Albert D. Seeno Constr. Co. v. Twin City Fire Ins. Co.*, 114 F.3d 1193 (9th Cir. 1997). Judge Richard Posner of the U.S. Court of Appeals for the Seventh Circuit commented in *Anderson v. Romero*, 72 F.3d 518 (7th Cir. 1995), that the "legal concept of privacy . . . originated in a famous article by Warren and Brandeis." *See id.* at 521; *see also* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1342–47.

4 Warren & Brandeis, *supra* note 2, at 195.

5 *Id.*

6 *Id.*

7 *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 384 (1960).

Georgia in *Pavesich v. New England Life Insurance Co.*[8] recognized a cause of action in tort nearly identical to the privacy action articulated by Warren and Brandeis.[9] The court found that the right to privacy is a right derived from natural law[10] and that a violation of the right of privacy is a direct invasion of a legal right of the individual.[11] Emphasizing that the invasion of privacy is a tort, the court described the damages to be recovered for its violation "are those for which the law authorizes a recovery in torts of that character; and if the law authorizes a recovery of damages for wounded feelings in other torts of a similar nature, such damages would be recoverable in an action for a violation of this right."[12]

The right to privacy concept proposed by Warren and Brandeis[13] is almost universally regarded as the origin of the law of privacy, which consists of four distinct kinds of invasion of four different privacy interests, and which is recognized in the vast majority of states today[14] as set forth in the Restatement (Second) of Torts. The privacy torts may be described as:

- intrusion upon seclusion;[15]
- appropriation of name or likeness;[16]

---

8 122 Ga. 190 (Ga. 1905).

9 *See* Benjamin E. Bratman, *Brandeis and Warren's "The Right to Privacy and the Birth of the Right to Privacy*," 69 TENN. L. REV. 623 (2002).

10 *Pavesich*, 122 Ga. at 197.

11 *Id.* at 201–202.

12 *Id.*

13 After becoming a Supreme Court Justice, Brandeis relied on the "right to be let alone—the most comprehensive of rights and the right most valued by civilized man" in arguing that the Fourth Amendment's protection against illegal searches and seizures and the Fifth Amendment's guarantee against self-incrimination implied a right to privacy, in his dissenting opinion in *Olmstead v. U.S.*, 277 U.S. 438, 478 (1928), a government wiretapping case.

14 *See* Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998) ("Today, we join the majority of jurisdictions and recognize the tort of invasion of privacy.").

15 "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).

16 "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasions of his privacy." *Id.* § 652C.

- public disclosure of private facts;[17] and
- false light or "publicity."[18]

Intrusion upon seclusion is the tort claim most often associated with common law privacy liability in the context of data privacy. A privacy violation based on the common law tort of intrusion requires (1) that the defendant intentionally intrude into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy; and (2) the intrusion must occur in a manner highly offensive to a reasonable person.[19] As to the first element of the common law tort, the defendant must have "penetrated some zone of physical or sensory privacy . . . or obtained unwanted access to data" by electronic or other covert means, in violation of the law or social norms.[20] In either case, the expectation of privacy must be objectively reasonable.[21] The second element involves a "policy" determination as to whether the intrusion is highly offensive under the circumstances.[22] "Highly offensive" conduct is not, however, amenable to a precise definition and must be determined on a case-by-case basis.

B. Fair Information Practice Principles and Similar Privacy-Protecting Frameworks

The concept of a framework of privacy principles to protect personal information began to be formalized within the United States government in the early 1970s, as an initiative by the U.S. Department of Health Education and Welfare (now the U.S. Department of Health and Human Services (HHS)) that culminated in the privacy protections built into the Privacy Act of 1974 (5 U.S.C. § 552a). Similar efforts to develop privacy-protecting frameworks were underway outside the United States during that same time frame, including the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).[23]

---

17 "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." *Id.* § 652D.

18 "One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed." *Id.* § 652E.

19 Hernandez v. Hillside, 47 Cal. 4th 272, 286, 211 P.3d 1063, 1072 (Cal. 2009), citing Shulman v. Group W Productions, Inc., 18 Cal. 4th 200, 231 (Cal. 1998) (approving and following RESTATEMENT (SECOND) OF TORTS, § 652B).

20 47 Cal. 4th at 286; *Shulman*, 18 Cal. 4th at 232.

21 *Id.*

22 *Id.*

23 *See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (1980), *available at* www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. The OECD Privacy Guidelines were updated for the first time in 2013. *See 2013 OECD Privacy Guidelines*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (2013), *available at* http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

Different names have been used for privacy-protecting frameworks in the United States, including the "Code of Fair Information Practice,"[24] "Fair Information Practices,"[25] "Fair Information Practice Principles (FIPPs),"[26] and "Generally Accepted Privacy Principles."[27] Although comparing and harmonizing frameworks and privacy-protection principles is beyond the scope of this Primer,[28] the importance of these frameworks and the accompanying principles is that all share the common goal of articulating key privacy protection principles that, when adopted and implemented, assist organizations, whether public sector or private, large or small, to manage the privacy risks associated with collecting, retaining, using, and disclosing personal information.

By way of example, the White House, in announcing its strategy for trusted identities in cyberspace, provided the following articulation of the FIPPs in 2011:

- Transparency: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).

- Individual Participation/Access: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.

---

[24] *See Sec'y's Advisory Comm. on Automated Personal Data Sys., Records, Computers and the Rights of Citizens*, OFFICE OF THE ASSISTANT SECRETARY FOR PLANNING AND EVALUATION, U.S. DEPT. OF HEALTH AND HUMAN SERVICES (1973), *available at* https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

[25] For a thorough history of the evolution, application, and operative principles of Fair Information Practices and related frameworks, *see* ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (2016), *available at* www.bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[26] *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (Dec. 29, 2008), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[27] *See* Am. Inst. of Certified Pub. Accountants, Inc. & Canadian Inst. of Chartered Accountants, *Generally Accepted Privacy Principles*, AMERICAN INSTITUTE OF CPAS (2009), *available at* http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/generallyacceptedprivacyprinciples/Pages/default.aspx.

[28] The American Law Institute is currently working on *Principles of the Law, Data Privacy* (formerly known as RESTATEMENT OF THE LAW, THIRD, INFORMATION PRIVACY PRINCIPLES). As explained in the Reporters' Memorandum regarding this project: "Information privacy law in the United States is currently a bewildering assortment of many types of law that differ from state to state and in federal statutes and regulations . . . . Information privacy law is, therefore, an area of law that requires the type of guidance that the ALI can bring." Paul M. Schwartz & Daniel J. Solove, *Reporters' Memorandum: Restatement Third of Information Privacy Principles*, 2013 *Preliminary Draft No. 1* ix (2013), *available at* http://scholarship.law.berkeley.edu/facpubs/2238.

- Purpose Specification: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose(s) for which the PII is intended to be used.

- Data Minimization: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

- Use Limitation: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purposes for which the PII was collected.

- Data Quality and Integrity: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

- Security: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

- Accountability and Auditing: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.[29]

Over time, these frameworks and their privacy-protecting principles, however articulated, have been incorporated into day-to-day business operations of a significant number of public- and private-sector entities, and they are reflected in much of the federal and state privacy law, enforcement, and guidance discussed in this Primer.

C. Personal Information

One key step in managing privacy risks is to determine what constitutes "personal information" that requires protection. Unfortunately, there is no universal "one size fits all" definition of "personal information" under laws in the U.S. or a single applicable legal rule that applies in all circumstances. Instead, as will be discussed below, this definition depends upon the particular law that applies, the context in which it is used, and each organization's privacy policies and procedures.

---

[29] *See* THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE: ENHANCING ONLINE CHOICE, EFFICIENCY, SECURITY, AND PRIVACY (April 2011), Appendix A, *available at* https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf. The White House also articulated the Fair Information Practice Principles (FIPPs) in its Consumer Privacy Bill of Rights in 2012, along with a comparison between the Consumer Privacy Bill of Rights to other statements of the FIPPs. *See* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), Appendices A and B, *available at* https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

As a general rule, the level of legal protections afforded under the law to the information varies based upon the sensitivity of the information and the risk that unauthorized access to it could cause injury to an individual. Thus, certain U.S. laws define "personal information" to include social security numbers and other government-issued identification numbers, financial account information, medical information, health insurance information, and identifiable information collected from children.

Although U.S. privacy laws typically apply only to individually identifiable personal information, adopting privacy practices solely based upon this narrow definition may be insufficient from the perspective of consumers, for instance where such information is used for data analytics purposes.[30] Moreover, the definition of "personal information" under the laws of other countries, in particular those in the EU, is significantly broader than that under applicable U.S. laws.[31]

Further, in some circumstances, personal information that was thought to have been sufficiently de-identified or anonymized has been re-identified.[32] Opinions vary on the extent to which such re-identification is feasible and cost-effective from a practical perspective, and thus a risk that must be mitigated, but this risk should be considered when using or disclosing such information.[33]

As a result of these considerations, many organizations now take a broader view of what constitutes personal information, including taking into account the potentially identifying effect of combining

---

[30] For example, in 2012, a predictive analytics program used by Target to analyze purchase patterns, identify behaviors, and provide focused advertising to individuals generated media controversy and consumer backlash when consumers discovered that Target sent pregnancy-related advertising materials to the home of a high-school student whose family was unaware of her pregnancy. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), *available at* www.nytimes.com/2012/02/19/magazine/shopping-habits.html; *see also* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J.L. & TECH. 59 (2014), *available at* http://digitalcommons.law.yale.edu/yjolt/vol16/iss1/2.

[31] For example, the EU Data Protection Directive (94/46/EC) defines "personal data" as "any information relating to an identified or identifiable natural person," which includes a broad set of information (e.g., date of birth, address, phone number), as well as identifiable images. *See Opinion of the Article 29 Data Protection Working Party on the "Concept of Personal Data,"* Opinion 4/2007 (June 2007), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

[32] For example, Netflix provided purportedly de-identified datasets of subscriber viewing information to participants in a $1 million contest to improve its algorithm for recommending movies based on movies previously viewed and enjoyed. By combining information from other sources with the datasets, researchers were able to re-identify a number of Netflix subscribers, and, after FTC intervention, Netflix decided not to proceed with a planned second contest. *See* FTC Closing Letter to Netflix (Mar. 12, 2010), *available at* www.ftc.gov/sites/default/files/documents/closing_letters/netflix-inc./100312netflixletter.pdf*; see also* Larry Hardesty, *Privacy Challenges*, MIT NEWS (Jan. 29, 2015), *available at* http://news.mit.edu/2015/identify-from-credit-card-metadata-0129.

[33] *Compare, e.g.,* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010), *available at* http://www.uclalawreview.org/pdf/57-6-3.pdf, *with* NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, DE-IDENTIFICATION OF PERSONAL INFORMATION, NISTIR 8053 (2015), *available at* http://dx.doi.org/10.6028/NIST.IR.8053. For example, HIPAA provides both a Safe Harbor method and an Expert Determination method for sufficiently de-identifying protected health information to permit its use and disclosure.

information from several sources. For example, PII under federal government requirements for federal agencies is defined broadly to include "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."[34] This approach requires a case-by-case assessment of the specific risk of identifying an individual to determine whether the information constitutes PII, recognizing that non-PII can become PII when combined with other available information.[35] Organizations should consider all of the above when developing policies and practices regarding privacy, data security, and the collection, use, and disclosure of personal information.

D. Industry Standards

Industry standards have been cited at both the state[36] and federal[37] levels when determining the reasonableness of an organization's data security practices and potential liability. For example, the U.S. Federal Trade Commission (FTC) has brought a series of high-profile enforcement actions based upon the failure to implement policies and controls consistent with industry standards.[38] Industry standards typically provide guidance on privacy and data security best practices regarding policies, data use and retention, and information security, including encryption.

---

[34] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM M-10-23, GUIDANCE FOR AGENCY USE OF THIRD-PARTY WEBSITES AND APPLICATIONS (2010), at Appendix, *available at* www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

[35] *Id.*; *see also* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM M-07-16, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (2007), at 1 n.1, *available at* www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

[36] *See, e.g.*, Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 MASS. CODE REGS. 17.00 (2010) at 17.01(1), *available at* http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

[37] The FTC has "urge[d] industry to accelerate the pace of its self-regulatory measures" and development of "sector-specific codes of conduct." FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), at v–vi, *available at* https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

[38] *See* PATRICIA BAILIN, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, STUDY: WHAT FTC ENFORCEMENT ACTIONS TEACH US ABOUT THE FEATURES OF REASONABLE PRIVACY AND DATA SECURITY PRACTICES (2014), *available at* https://privacyassociation.org/media/pdf/resource_center/FTC-WhitePaper_V4.pdf.

The applicability of industry standards is based on the size,[39] particular business practices,[40] or specific industry[41] of the subject organization. Although not always legally required, compliance with industry standards is becoming increasingly important to mitigate privacy and security risks.[42]

E. Contract-Based Privacy Rights

In the United States, privacy-related rights of individuals have not generally been seen as enforceable (or waivable) through the application of contract law principles. Accordingly, the trend thus far has not been to determine or limit individual privacy rights based on contract law or the terms of express or implied agreements, such as privacy policies, website terms of use, or end user license agreements.[43] However, companies do impose contractual privacy and data security requirements on service providers with which they do business to ensure that personal information is handled in compliance with applicable laws and best practices.[44]

---

39 *See, e.g.*, *Data Privacy for Small Businesses*, BETTER BUS. BUREAU, *available at* http://www.bbb.org/council/for-businesses/toolkits/data-privacy-for-small-businesses (last visited Jan. 1, 2017).

40 *See, e.g.*, PCI SEC. STANDARDS COUNCIL, DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES (2010), *available at* https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

41 *See, e.g.*, THE INT'L SOC'Y OF AUTOMATION AM. NAT'L STANDARD, ANSI/ISA—99.00.01—2007, SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS (2007), *available at* http://isa99.isa.org/Public/Documents/ISA-62443-1-1-EX.pdf.

42 *See* Jedidiah Bracy, *Will Industry Self-Regulation Be Privacy's Way Forward?*, THE PRIVACY ADVISOR (June 2014), https://iapp.org/news/a/will-industry-self-regulation-be-privacys-way-forward.

43 *See, e.g.,* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 588–89, 595–97 and cases and materials cited therein (2014), *available at* http://columbialawreview.org/content/the-ftc-and-the-new-common-law-of-privacy/.

44 For example, as discussed below, HIPAA covered entities must enter into business associate agreements with their business associates.

SIDE BAR – BACKGROUND AND OVERVIEW

Privacy laws and industry standards have evolved over the past century. Today, a complex framework exists, which has evolved based upon common law, statutes, and the Fair Information Practice Principles (FIPPs).

Invasion of privacy tort claims are recognized under the vast majority of state laws. There are several theories of liability upon which such claims may be based (which vary by state), including: (1) an "intrusion upon seclusion" where an individual has a reasonable expectation of privacy; (2) an appropriation of one's name or likeness; (3) a public disclosure of private facts; or (4) false light or "publicity."

The FIPPs and related guidelines, which developed in the 1970s and were relied upon as the basis for several U.S. privacy laws, including the Privacy Act of 1974. The FIPPS incorporate a number of key privacy principles, including: access/individual participation, purpose specification, data minimization, use limitation, data quality/integration, security, and accountability/auditing.

Individual privacy rights and organizations' use of personal information today are governed by not only a complex patchwork of state and federal laws, but also industry standards and contractual requirements. Regulators often rely upon industry standards to determine whether an organization maintains reasonable privacy and information security practices.

III. FEDERAL AND STATE GOVERNMENTS

The federal government has a number of statutory, regulatory, and other obligations (including Executive Orders, Office of Management and Budget (OMB) Memoranda, and National Institute of Standards and Technology (NIST) guidance) that impact its collection, handling, use, disclosure, and disposal of personal information.[45] This section of the Primer addresses key privacy obligations that govern federal agency collection, retention, use, and disclosure of personal information.

A. Federal Government

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

Against the backdrop of government surveillance of civil rights activities, the Watergate break-in, and increasing concern about the federal government's ability to compile information about individuals, the Privacy Act of 1974 (5 U.S.C. § 552a) ("Privacy Act")—which incorporated elements of the FIPPs—was enacted to establish requirements for federal agencies' collection, use, sharing, and disclosure of personal information. The Privacy Act generally applies to "any item, collection, or grouping of information about an individual" (i.e., the "record") that is compiled into a system operated by or on behalf of a federal agency (i.e., the "system of records"), but only if the agency actually uses the individual's name or other personal identifier to access and retrieve personal information from the system.[46]

Under the Privacy Act, federal agencies must identify each of their Privacy Act system of records by publishing a System of Records Notice (SORN) in the Federal Register, and by regularly reviewing and updating agency SORNs as needed. In addition, agencies that collect information directly from individuals must provide them with a Privacy Act statement that identifies the legal authority for collecting the information, the purpose for collecting it, the uses of the information, whether provision of the information is voluntary or mandatory, and what, if any, consequences will result from not providing the information.

As a general rule, federal agencies cannot disclose personal information from a Privacy Act system of records unless the agency has written consent from the individual or the disclosure falls within one of twelve statutory exceptions[47]:

---

[45] As noted above, "personally identifiable information" (PII) under federal government requirements for federal agencies is defined broadly to include "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual." OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM M-10-23, GUIDANCE FOR AGENCY USE OF THIRD-PARTY WEBSITES AND APPLICATIONS (2010), at Appendix, *available at* www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

[46] *See* 5 U.S.C. § 552a(a). The Department of Justice oversees federal agency implementation, interpretation, and compliance with the Privacy Act. Its Office of Privacy and Civil Liberties maintains a website that contains resources and guidance and provides a "comprehensive treatise of existing Privacy Act case law." *See* U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974 (2015 ed.), *available at* https://www.justice.gov/opcl/privacy-act-1974.

[47] 5 U.S.C. § 552a(b).

1) "need to know" use by the agency that maintains the record;

2) required disclosure under the Freedom of Information Act (FOIA);[48]

3) "routine uses," i.e., uses that are consistent with the purpose for which the agency collected the information *and* that the agency has identified by publishing in the Federal Register;

4) use by the Bureau of the Census;

5) use for statistical research;

6) transfer to the National Archives and Records Administration;

7) use for civil or criminal law enforcement;

8) compelling health or safety circumstances;

9) official use by Congress;

10) official use by the Government Accountability Office;

11) required disclosure by court order; or

12) reporting bad-debt information to a consumer reporting agency after due process.[49]

The Privacy Act gives individuals, with limited exceptions, the right to request an "accounting" that identifies the name, address, date, nature, and purpose of each disclosure of that person's record to any person or any agency.[50] Individuals also generally have the right to access, review, and request correction of records containing information about them, to have those corrections provided to other individuals and entities who have received copies of the information, and to request agency review of any decision not to amend.[51]

Individuals have the right to bring a civil action in federal district court if a federal agency fails to comply with its Privacy Act obligations, and may be entitled to relief that includes actual damages and recovery of reasonable attorney's fees and litigation costs. No private right of action exists against federal employees who violate the Privacy Act, but federal employees who willfully violate the Privacy Act are subject to criminal prosecution for a misdemeanor, as are individuals who obtain

---

[48] FOIA is discussed further below.

[49] 5 U.S.C. § 552a(b).

[50] *Id.* at § 552a(c).

[51] *Id.* at § 552a(d).

records from federal agencies under false pretenses. For purposes of the Privacy Act, federal contractors who operate a system of records by or on behalf of a federal agency are deemed to be federal employees.[52]

It should be noted that the Privacy Act requires federal and state entities that collect social security numbers (SSNs) directly from individuals to provide them, before collection, with a Privacy Act statement-like disclosure that explains whether their provision of the SSN is mandatory or voluntary, cites the statutory authority for the request, and describes the use of the SSN; and federal and state entities cannot deny benefits solely based on an individual's refusal to provide a SSN.[53] In addition, the Privacy Act limits the circumstances under which federal agencies can engage in "computer matching," in which an agency compares personal information from its systems of records with that from another agency and compiles shared information about individuals.

The Privacy Act has a number of significant carve-outs that limit its applicability. First, it applies only to U.S. citizens and lawfully admitted aliens, although the Judicial Redress Act granting EU citizens the right to legal redress for privacy violations against certain U.S. agencies in U.S. courts was recently passed.[54] Second, there are statutory exceptions that, for example, do the following: prevent individuals from accessing information relating to civil and criminal investigations, law enforcement activities, and national security matters; permit agencies engaged in criminal enforcement or intelligence activities to publicly designate systems of record as exempt from the Privacy Act; and prevent the release of information relating to specified government personnel, promotion, and security activities.[55]

2. E-Government Act of 2002 (Public Law 107-347)

The E-Government Act of 2002 ("E-Gov Act"), applicable to federal government agencies, was enacted to "enhance the management and promotion of electronic Government services and processes" by, among other things, "establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services." This push toward a more modern electronic and digital federal government was accompanied by formal privacy and data security requirements to protect the data, websites, and information systems used by federal government agencies. Although this Primer focuses on the key privacy-re-

---

52 *Id.* at § 552a(m).

53 *Id.* at § 552a note.

54 *Id.* at § 552a(a); European Commission Statement by Commissioner Věra Jourová on the signature of the Judicial Redress Act by President Obama (Feb. 24, 2016), http://europa.eu/rapid/press-release_STATEMENT-16-401_en.htm.

55 *Id.* at § 552a(d)(5), (j), (k).

lated requirements of the E-Gov Act, Title III of the E-Gov Act also created government-wide information security requirements, the Federal Information Security Management Act of 2002 (FISMA).[56]

The OMB provides much of the guidance and interpretation relied on by federal agencies in implementing and complying with the E-Gov Act. OMB maintains a website, https://www.whitehouse.gov/omb/e-gov, with information about E-Gov Act initiatives, as well as links to relevant memoranda, reports, and other materials.

The privacy protections in Title II of the E-Gov Act[57] are intended to "ensur[e] sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government." The following three key privacy requirements imposed on most federal agencies by the E-Gov Act directly impact the public: conduct a "Privacy Impact Assessment" (PIA); post a privacy policy on federal agency web sites; and protect and limit the use of personal information that federal agencies collect for statistical purposes.

- PIA: Federal agencies must conduct a Privacy Impact Assessment before developing or procuring an IT system or initiating a project that collects, maintains, or disseminates information in an identifiable form from or about members of the public. With certain limited exceptions, completed PIAs must be posted on the agency's public-facing website. Each PIA must address what information is to be collected and why, the intended use of the information (including routine agency uses that may be common to multiple PIAs), who the information will be shared with, what notice or opportunities individuals have to decline to provide information, how the information will be secured (including risk mitigation), and whether the collection of information will create a system of records for purposes of the Privacy Act. In addition, agencies must regularly review and update their PIAs as needed to reflect changes in agency practices that impact privacy-related risks.[58]

- Privacy Policy: Federal agency websites must post a privacy policy that, consistent with the Privacy Act, describes what information is being collected (including automatic collection) and why, how the information will be used and who it will be shared with, what notice and opportunity for consent individuals have with regard to collection and sharing of the information, how the information will be secured, and what rights the individuals have under the Privacy

---

[56] *See* 44 U.S.C. § 3541–3549. FISMA interpretation and compliance relies heavily on OMB guidance and NIST publications regarding information security-related practices. FISMA 2002 was amended by the Federal Information Security Modernization Act of 2014 to reflect current thinking about information security, compliance, reporting, and oversight.

[57] Title II of the E-Gov Act is reproduced at 44 U.S.C. § 3501 note.

[58] Other federal laws impact the content of federal agency PIAs, including the Federal Records Act, which imposes obligations to address retention, disposal, and labeling of information.

Act "and other laws relevant to the protection of the privacy of an individual." The privacy policy must be clearly labeled, written in plain language, and easy to access in terms of location, machine readability, and accessibility to persons with disabilities. Like PIAs, privacy policies must be reviewed and updated as needed to reflect changes in practices.

- Confidential Collection of Statistical Information: Title V of the E-Gov Act, enacted as the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA),[59] protects individuals and organizations who provide information to federal agencies for statistical purposes under a pledge of confidentiality by making sure that agencies secure the information, do not disclose it in identifiable form, and do not use it for non-statistical purposes. CIPSEA potentially applies, for example, to online and offline surveys conducted by federal agencies and their contractors if they are represented as being confidential and for statistical purposes. Disclosure of individually identifiable information covered by CIPSEA is a felony.

3. Freedom of Information Act (5 U.S.C. § 552)

The Freedom of Information Act (FOIA) generally requires federal agencies to "make available for public inspection and copying" certain categories of routine agency documents, as well as materials previously released under the FOIA that the agency believes are likely to be subject to multiple requests.[60] In addition, agencies, with certain limitations, must "make records promptly available" to any person who submits a "request for records which reasonably describes such records."[61] Federal agencies can only withhold records or portions of records that fit within one of the nine exemptions at 5 U.S.C. §§ 552(b)(1)–(9). The Department of Justice's (DOJ) Office of Information Policy oversees federal agency compliance with the FOIA and maintains a website that contains current FOIA interpretation and guidance including the comprehensive *Department of Justice Guide to the Freedom of Information Act* ("DOJ Guide").[62]

Although much of the FOIA implicates issues that are beyond the scope of this Primer, two FOIA exemptions specifically protect privacy interests. Exemption 6 protects "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal

---

[59] Reproduced at 44 U.S.C. § 3501 note; *see also* Implementation Guidance for Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), 72 Fed. Reg. 33,362 (June 15, 2007).

[60] 5 U.S.C. § 552(a)(2).

[61] *Id.* at § 552(a)(3)(A).

[62] *See* OFFICE OF INFO. POLICY, U.S. DEP'T OF JUSTICE, OIP GUIDANCE (2016), *available at* www.justice.gov/oip/oip-guidance.

privacy."[63] Exemption 7(C) protects "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy."[64] As stated in the DOJ Guide, "under both personal privacy exemptions of the FOIA, the concept of privacy not only encompasses that which is inherently private, but also includes an 'individual's control of information concerning his or her person.'"[65]

Under Exemption 6, interest balancing is required, but "[s]ubstantial privacy interests cognizable under the FOIA are generally found to exist in such personally identifying information as a person's name, address, image, computer user ID, phone number, date of birth, criminal history, medical history, and social security number."[66] In contrast, the DOJ Guide asserts that:

> Exemption 7(C) can be applied on a categorical basis. In *DOJ v. Reporters Committee for Freedom of the Press*, the Supreme Court found that a third party's request for law enforcement records pertaining to a private citizen categorically invades that citizen's privacy, and that where a request seeks no official information about a government agency, the privacy invasion is unwarranted. Indeed, the Court of Appeals for the District of Columbia Circuit held in *SafeCard Services v. SEC* that, based upon the traditional recognition of the strong privacy interests inherent in law enforcement records, and the logical ramifications of *Reporters Committee*, the categorical withholding of information that identifies third parties in law enforcement records will ordinarily be appropriate under Exemption 7(C).[67]

As a result, notwithstanding that the FOIA is intended to promote openness and transparency and provide ready access to information collected and created by federal agencies, the protections for personal information are relatively strong and well established.

4. The Fourth Amendment

The Fourth Amendment to the U.S. Constitution protects citizens from unreasonable/warrantless searches or seizures by government actors. Evolving technologies make the collection and interpretation of data more readily accessible to federal agencies and law enforcement, placing those parties in the position of justifying their data collection practices over the potential loss of privacy rights of individuals. What constitutes an unreasonable search/seizure of personal information was at the

---

63 5 U.S.C. § 552(b)(6).

64 DOJ Guide, Exemption (7)(C), *available at* www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption7c.pdf.

65 DOJ Guide, Exemption 6 at 1 (citing DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989)), *available at* www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption6.pdf.

66 *Id.* at 10.

67 DOJ Guide, Exemption 7(C) at 1–2 (citations omitted), *available at* www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption7c.pdf.

heart of the recent debate concerning the National Security Agency's (NSA) telephone metadata bulk collection practices, ultimately leading to the shut-down of that aspect of the agency's program.[68]

While traditionally the Fourth Amendment has been most frequently leveraged as a right to suppress evidence in criminal prosecutions, it can also apply in purely civil cases. The use of unreasonably seized information in violation of the Fourth Amendment's privacy protections and causing an injury to a party may give rise to a civil rights claim under 42 U.S.C. § 1983. Further, if a non-government party is acting under color of law with the government, that private party may be subject to the § 1983 claim as well.[69]

These same Fourth Amendment limitations could apply to any other data gathering by the government that is deemed a "search," and what constitutes a reasonable search is an unresolved issue that has evolved over time consistent with technological changes. This has most recently been brought to light when The Federal Bureau of Investigations (FBI) issued a search warrant to Apple compelling the company to assist the FBI in by-passing the encryption technology built into an iPhone device that formerly belonged to terror suspect, Syed Rizwan Farook, who was involved in a mass-shooting in San Bernardino, California. Among the constitutional issues raised by Apple in response to the warrant was the suggestion that while the FBI's search warrant may be technically valid, the method of execution requested to enforce the warrant would be unreasonable under the Fourth Amendment.[70] The FBI later unlocked the phone using a third party tool and the DOJ withdrew the case, but the controversy regarding the balance between individual privacy rights and the government's need to conduct law enforcement investigations and ensure national security persists.[71]

---

[68] Pete Williams, *Massive NSA Phone Data Collection to Cease*, NBCNEWS.COM (Nov. 27, 2015), *available at* http://www.nbcnews.com/news/us-news/massive-nsa-phone-data-collection-cease-n470521; *see also* Charlie Savage, *Judge Deals a Blow to N.S.A. Data Collection Program*, N.Y. TIMES (Nov. 9, 2015), *available at* http://www.nytimes.com/2015/11/10/us/politics/judge-deals-a-blow-to-nsa-phone-surveillance-program.html).

[69] *Cf.* Soldal v. Cook County, 506 U.S. 56 (1992) (holding that a police-assisted seizure of a mobile home for eviction purposes raised a claim under the Fourth Amendment, and was a proper § 1983 claim against both the police and the landlord); *see also* Jack M. Beerman, *Why Do Plaintiffs Sue Private Parties Under Section 1983?*, 26 CARDOZO L. REV. 9 (2004), *available at* http://www.nlg-npap.org/sites/default/files/Beermann.pdf.

[70] *See* Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search and Opposition to Government's Motion to Compel Assistance at 35, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, ED No. CM 16-10 (SP) (E.D. Cal. Feb. 25, 2016), *available at* https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf. Seventeen amicus briefs and four letters to the court were submitted in support of Apple's position. *See Amicus Briefs in Support of Apple*, APPLE INC., http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html (last visited Jan. 5, 2017).

[71] *See* Mark Skilton & Irene Ng, *What the Apple versus FBI Debacle Taught Us*, SCI. AM. GUEST BLOG (May 20, 2016), http://blogs.scientificamerican.com/guest-blog/what-the-apple-versus-fbi-debacle-taught-us.

5. Federal Criminal Law Enforcement

Federal criminal law prohibits, among other conduct, that which constitutes wire fraud, identity theft, unauthorized access of a computer (including through hacking and/or password trafficking), phishing, accessing and/or disclosing stored communications, and cyberstalking.[72] The Federal Bureau of Investigations (FBI) and United States Secret Service (USSS), and other sections of the United States Department of Homeland Security (DHS), have dedicated units that investigate privacy-related conduct that could constitute computer and/or cyber crimes.[73]

FBI accepts computer and cyber complaints via the FBI Internet Crime Complaint Center (IC3), found at http://www.ic3.gov/default.aspx. The DOJ prosecutes criminal conduct that impacts privacy pursuant to federal criminal statutes.[74]

B. State Governments

Like the federal government, of course, state governments collect substantial amounts of data from and about their own citizens as well as non-residents who pass through their borders. States have adopted laws in several key areas to ensure that government entities properly handle that information.

---

[72] *See* 18 U.S.C. §§ 1028–1030, 1343, 2261A, 2511, & 2701. There are additional federal criminal statutes prohibiting conduct that impacts privacy in the context of computer or cyber crimes. The January 2015 DOJ Computer Crime and Intellectual Property Section Criminal Division publication, *Prosecuting Computer Crimes*, discusses some of the statutes referenced herein, as well as others; and can be found at http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf. Additionally, discussion about the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*., and the Stored Communications Act, 18 U.S.C. § 2701 *et seq*., can be found in the United States Attorneys' Manual at sections 9-48.000, 9-7.000, and 9-60.200, and the U.S. Attorneys' Criminal Resource Manual at sections 1021, 1040, and 1061. *See* http://www.justice.gov/usam/usam-9-7000-electronic-surveillance; http://www.justice.gov/usam/usam-9-48000-computer-fraud; https://www.justice.gov/usam/usam-9-60000-protection-individual; http://www.justice.gov/usam/criminal-resource-manual-1021-18-usc-1030-post-october-1996; http://www.justice.gov/usam/criminal-resource-manual-1040-introduction-criminal-sanctions-illegal-electronic-surveillance; http://www.justice.gov/usam/criminal-resource-manual-1061-unlawful-access-stored-communications-18-usc-2701.

[73] *See* https://www.fbi.gov/about-us/investigate/cyber for discussion of the FBI's cyber crime priorities; *see also* http://www.secretservice.gov/investigation/; http://www.dhs.gov/cybersecurity-overview. Federal law enforcement works together as part of a National Cyber Investigative Joint Task Force. *See* https://www.fbi.gov/about-us/investigate/cyber/ncijtf.

[74] Such cases are investigated and brought by the DOJ Criminal Division as well as U.S. Attorney's Offices throughout the country. The Criminal Division has a dedicated Computer Crime and Intellectual Property Section (CCIPS), https://www.justice.gov/criminal-ccips, which includes a cybersecurity unit, http://www.justice.gov/criminal-ccips/cybersecurity-unit. In April 2015, CCIPS provided guidance on *Best Practices for Victim Response and Reporting Cyber Incidents*, which can be found at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

1. State Constitutional Privacy Protections

Ten state constitutions reference a right to privacy: Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington.[75] More than half these provisions enshrine a general right to privacy that, at least in theory, applies in all contexts. The California Constitution, for example, makes "pursuing and obtaining" privacy an inalienable right, on par with "enjoying and defending life and liberty."[76] The Florida Constitution goes almost as far, but leaves room for some governmental invasions of privacy by declaring that "[e]very natural person has the right to be let alone and free from governmental intrusion into the person's private life *except as otherwise provided herein*."[77] Arizona and Washington also allow for at least some governmental intrusions, providing that "[n]o person shall be disturbed in his private affairs . . . without authority of law."[78] Hawaii and Montana are more restrictive, requiring "the showing of a compelling state interest" to justify any infringement of a person's right to privacy.[79] Alaska, on the other hand, does not even include that limited exception; in Alaska, "[t]he right of the people to privacy . . . shall not be infringed."[80]

In several of the state constitutions that address privacy, the state analogue to the Fourth Amendment explicitly provides that invasions of privacy are prohibited as unreasonable searches and seizures. For example, the Illinois Constitution ensures the peoples' right to be secure "against unreasonable searches, seizures, *invasions of privacy or interceptions of communications by eavesdropping devices or other means*."[81] The Florida Constitution, in somewhat more limited fashion, specifies that "[t]he right of the people to be secure . . . against the *unreasonable interception of private communications by any means*, shall not be violated."[82]

---

75 For a hyperlinked list of the state constitutional provisions referenced here, *see* the National Conference of State Legislatures (NCSL) website at http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

76 *See* CAL. CONST. art. I, § 1.

77 FLA. CONST. art. I, § 23 (emphasis added).

78 ARIZ. CONST. art. II, § 8; WASH. CONST. art. I, § 7.

79 HAW. CONST. art. I, § 6; MONT. CONST. art. II, § 10.

80 ALASKA CONST. art. I, § 22.

81 ILL. CONST. art. I, § 6 (emphasis added)*; see also* HAW. CONST. art. I, § 7 ("The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures and *invasions of privacy* shall not be violated[.]") (emphasis added); LA. CONST. art. I, § 5 ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or *invasions of privacy*.") (emphasis added); S.C. CONST. art. I, § 10 ("The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and *unreasonable invasions of privacy* shall not be violated[.]") (emphasis added).

82 FLA. CONST. art. I, § 12 (emphasis added). Although the Missouri Constitution does not explicitly refer to "privacy," a 2014 amendment explicitly protects "electronic communications or data, such as that found on cell phones and other electronic devices" against unreasonable searches and seizures. MO. CONST. art. I, § 15.

2. Public Records Statutes

Every state—including those whose constitutions provide explicit rights to privacy—has enacted a "public records" law that allows members of the public to obtain documents from state and local government agencies.[83] At the same time, many of these states have also passed laws designed to protect certain PII that may be contained in those government records. For example, notwithstanding its public records statute, California law requires the courts in each county, along with the district attorney, to establish procedures to protect victims' confidential personal information that may be contained in various court filings.[84] California also prohibits the disclosure of the names or addresses of victims of certain sex-related crimes in any documents produced in response to requests for records (such as under the Public Records Act).[85] California has also enacted several statutes requiring specified court and other government records to truncate social security numbers in any documents released to the public.[86]

3. Surveillance and Other Data Collection

A number of states have enacted laws designed either to limit the state government's authority to collect certain information about state residents, or to specify whether and how the government can use or disclose that information. This section touches on just a few categories of state-collected information.

(a) Motor Vehicle Records

The federal Drivers Privacy Protection Act (DPPA), 18 U.S. Code § 2721 *et seq*., requires states to provide a minimum baseline of protection to drivers' motor vehicle records, but it does not prohibit states from enacting more stringent provisions. A number of states have done so.[87]

---

83 *See*, *e.g.*, *State Public Record Laws*, FOIADVOCATES, http://www.foiadvocates.com/records.html (hyperlinked list of 50 state laws on access to government records) (last visited Jan. 6, 2017). *See also Privacy/Public Access to Court Records*, NAT'L CENTER FOR STATE COURTS, http://www.ncsc.org/Topics/Access-and-Fairness/Privacy-Public-Access-to-Court-Records/State-Links.aspx?cat=Rules%20on%20Bulk%20Data (hyperlinked list of 38 state laws on access to court records). California even enshrined the right of public access into its constitution. The "Sunshine Amendment," which voters approved in 2004, provides that "[t]he people have the right of access to information concerning the conduct of the people's business, and, therefore, the meetings of public bodies and the writings of public officials and agencies shall be open to public scrutiny." CAL. CONST. art. I, § 3(b)(1).

84 CAL. PENAL CODE § 964.

85 CAL. GOV'T CODE § 6254, CAL. PENAL CODE § 293.

86 *See* CAL. CIV. CODE § 1798.89; CAL. COM. CODE § 9526.5; CAL. EDUC. CODE § 66018.55; CAL. GOV'T CODE § 27300.

87 *See*, *e.g.*, CAL. VEH. CODE §§ 1808–1821.

(b) License Plate Readers

Automated license plate readers (ALPRs) employ specialized image-processing technology to identify vehicles by their license plates. ALPRs may be mounted on police cars or fixed structures, like bridges or signs, and can capture images of hundreds of license plates per minute. The technology can assist law enforcement in locating stolen vehicles or wanted individuals. On the other hand, some have expressed concerns about how the data collected by ALPRs is used, pooled, analyzed, and retained.[88]

A minority of states have enacted statutes limiting the use of data collected by ALPRs.[89] While most of those laws limit the use of ALPR technology to law enforcement or other narrowly prescribed purposes, the other standards embodied in the statutes vary widely. For example, there is little consensus on the length of time the data may be retained. On the shorter end, Maine only permits ALPR data to be stored for a mere 21 days.[90] California permits its highway patrol to retain the data for no more than 60 days (unless the data is being used as evidence in a felony case).[91] The rule in Tennessee is 90 days, unless the data are part of an ongoing investigation.[92] Colorado, on the other hand, allows governmental entities to retain images for up to three years.[93]

The states also vary in the extent to which they afford special privacy protection to ALPR data. The Florida statute specifies that ALPR images and data containing personal information are confidential and exempts them from the state's public records law.[94] Maine contains a similar provision.[95] The California statute prohibits selling the data or making it available to non-law-enforcement agencies.[96]

---

88 *See You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/feature/you-are-being-tracked (last visited Jan. 6, 2017). Additionally, use of data collected by these devices may raise Fourth Amendment concerns under the U.S. Constitution. *See* Jessica Gutierrez-Alm, *The Privacies of Life: Automatic License Plate Recognition is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law*, 38 HAMLINE L. REV. 127 (2015), *available at* http://digitalcommons.hamline.edu/hlr/vol38/iss1/5.

89 *See Automated Plate Readers: State Statutes Regulating Their Use*, NAT'L CONFERENCE OF STATE LEGIS. (April 13, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plade-readers-alpr-or-alpr-data.aspx.

90 ME. REV. STAT. ANN. tit. 29-A, § 2117-A(2).

91 CAL. VEH. CODE § 2413.

92 S.B. 1664, 108th Gen. Assemb. (Tenn. 2014) (enacted at TENN. CODE ANN. § 55-10-302 (West)).

93 COLO. REV. STAT. § 24-72-113. After the first year, the custodian of the data may only access it if there has been a claim or a specific incident that may cause the record to become evidence in a civil, labor, administrative, or felony criminal proceeding. *Id.*

94 FLA. STAT. § 316.0777.

95 ME. REV. STAT. ANN. tit. 29-A, § 2117-A(2) (providing that ALPR data is confidential and may be used only for law enforcement purposes).

96 *Id.*

(c) Event Data Recorders

An event data recorder (EDR), sometimes called a "black box," is a device stored in some motor vehicles that records information specifically related to crashes, including "pre-crash vehicle dynamics and system status" and whether or not the vehicle's occupants were wearing seatbelts.[97] About 17 states have passed statutes covering EDRs.[98] Those states uniformly prohibit data collected by the EDR from being downloaded without the owner's consent, except in limited circumstances.[99] The statutes also generally require disclosure to the consumer that the motor vehicle contains an EDR, often in or along with the owner's manual.[100]

(d) 911 Call Recordings

Some states have statutes that specifically address whether recordings or transcripts of 911 calls are confidential.[101] More often, those recordings and transcripts fall under the state's public records law.

States that expressly address 911 calls often provide strong protection for the audio recording of the call. For example, in Alabama, audio recordings of 911 calls may not be released (other than to law enforcement) without a court order explicitly finding that the "right of the public to the release of the recording outweighs the privacy interests of the individual who made the 911 call or any person involved."[102] That rule is subject to only a narrow exception providing access for the caller or his or her estate.[103] Pennsylvania, likewise, exempts recordings of 911 calls from public disclosure unless "the agency or a court determines that the public disclosure outweighs the interest in nondisclosure."[104] Mississippi also generally protects the confidentiality of recordings of calls.[105]

---

97 *See Welcome to the NHTSA Event Data Recorder Research Web Site*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., http://nhthqnlas187.nhtsa.dot.gov/Research/Event+Data+Recorder+%28EDR%29/Welcome+to+the+NHTSA+Event+Data+Recorder+Research+Web+site.

98 *See Privacy of Data From Event Data Records: State Statutes*, NAT'L CONFERENCE OF STATE LEGIS. (Dec. 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

99 *See*, *e.g.*, CAL. VEH. CODE § 9951 (data may also be downloaded by court order, for vehicle safety research, or for servicing of the vehicle).

100 *See*, *e.g.*, CAL. VEH. CODE § 9951; COLO. REV. STAT. § 12-6-401; ME. REV. STAT. ANN. tit. 29-A, § 1971; NEV. REV. STAT. § 484D.485; N.H. REV. STAT. § 357-G:1; N.Y. VEH. & TRAF. § 416-b.

101 *See State 9-1-1 Legislation Tracking Database*, NAT'L CONFERENCE OF STATE LEGIS. (Jan. 3, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-9-1-1-legislation-tracking-database.aspx.

102 ALA. CODE § 11-98-12.

103 *Id.*

104 65 PA. CONS. STAT. § 67.708.

105 MISS. CODE ANN. § 19-5-319(2).

Several states distinguish between the audio recording and a written transcript, providing different protection to each form of record. Maine makes *audio recordings* of 911 calls confidential and prohibits their disclosure except in limited circumstances.[106] On the other hand, *transcripts* of the calls are public and must be disclosed in most cases.[107] Minnesota, North Carolina, and North Dakota take essentially the same approach.[108] North Carolina, however, also permits the release of an "altered voice reproduction" of the call.[109]

Other states err on the side of disclosure. In Georgia, for example, 911 calls are public records, and the caller's PII may only be redacted from the records "if necessary to prevent the disclosure of the identity of a confidential source, to prevent disclosure of material which would endanger the life or physical safety of any person or persons, or to prevent the disclosure of the existence of a confidential surveillance or investigation."[110] In Wyoming, the custodian of any information obtained through a 911 call "shall allow any person the right of inspection" of the records unless contrary to law, prohibited by court order, or contrary to the public interest.[111] Similarly, 911 records are presumed open under Virginia law, although personal, medical, or financial information in those records may be withheld if the safety or privacy of any person is jeopardized.[112]

4. Privacy Policies

About one-third of states have passed laws requiring government agencies to maintain and publicize a privacy policy.[113] California, for example, requires state agencies to adopt a privacy policy and to appoint an employee to be responsible for the policy.[114] A Connecticut statute requires anyone who collects social security numbers in the course of business to create a privacy policy, which must be

---

106 ME. REV. STAT. ANN. tit 25, § 2929(4).

107 *Id.*

108 *See* MINN. STAT. § 13.82, subd. 4; N.C. GEN. STAT. § 132-1.4(c), N.D. CENT. CODE § 57-40.6-07.

109 N.C. GEN. STAT. § 132-1.4(c)(4). In North Carolina and North Dakota, the caller's PII is exempt from the public records laws and may always be redacted. *See* N.C. GEN. STAT. § 132-1.4(c); N.D. CENT. CODE § 57-40.6-07 (3).

110 GA. CODE ANN. § 50-18-72(a)(26). In keeping with states' tendency to give more protection to audio recordings, Georgia does exempt from disclosure audio recordings that capture the voices of minors or the cries "in extremis" of any person who died during the call. GA. CODE ANN. § 50-18-72 (26.1). Other audio recordings, however, are not protected by the Georgia statute.

111 WYO. STAT. ANN. § 16-4-203.

112 VA. CODE ANN. § 2.2-3706g.

113 DEL. CODE ANN. tit. 6, § 1206C. For a hyperlinked list of 17 such state laws, see *State Laws Related to Internet Privacy*, NAT'L CONFERENCE OF STATE LEGIS. (Jan. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

114 CAL. GOV'T CODE § 11019.9; *see also* CAL. STS. & HY. CODE § 31490 (explicitly requiring transportation agency that uses electronic toll collection systems to establish and conspicuously post a privacy policy).

posted on a publicly-available web page.[115] The policy must limit access to the numbers and prohibit their unlawful disclosures.[116]

States are increasingly adopting legislation to criminalize a wide variety of conduct relating to privacy. The most important categories of state laws relate to computer crimes of various forms, identity theft, and online threats and harassment.

5. State Criminal Statutes

(a) Computer Crimes

State laws criminalize a wide variety of conduct concerning computers, computer systems, networks, and the like.[117] Nearly every state makes it a crime to obtain unauthorized access to a computer or system, whether that conduct is described generally as any access obtained without consent[118] or more specifically as hacking,[119] trespass,[120] or tampering.[121] Unauthorized access is often a misdemeanor, but many states provide that aggravating factors, such as accessing a computer in order to further a scheme to defraud or to steal intellectual property, may make the crime a felony. For example, in Oregon, unauthorized access is a misdemeanor, but the crime becomes a felony if the access or attempted access was for the purpose of:

a) devising or executing any scheme or artifice to defraud;

b) obtaining money, property or services by means of false or fraudulent pretenses, representations or promises; or

c) committing theft, including, but not limited to, theft of proprietary information.[122]

---

115 CONN. GEN. STAT. ANN. § 42-471.

116 *Id.*

117 *See, e.g.*, *Computer Crime Statutes*, NAT'L CONFERENCE OF STATE LEGIS. (Dec. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx; *State Hacking/Computer Security Laws*, IRONGEEK.COM, http://www.irongeek.com/i.php?page=computerlaws/state-hacking-laws (last visited Jan. 6, 2017).

118 *See generally* IRONGEEK.COM, *supra* note 117.

119 Only a small handful of states expressly outlaw "hacking." *See, e.g.*, OHIO REV. CODE ANN. § 2909.07(A)(6)(a); S.C. CODE ANN. §§ 16-16-10(j), 16-16-20(4).

120 A number of states have criminalized "trespass" into a computer or computer system. *See, e.g.*, ARK. CODE ANN. § 5-41-104; N.Y. PENAL LAW § 156.10; VA. CODE ANN. § 18.2-152.4.

121 *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-2316; 720 ILL. COMP. STAT. ANN. 5/17-51, 5/17-52; MO. ANN. STAT. § 569.095.

122 OR. REV. STAT. § 164.377(2)–(5).

In at least twelve states, it is a crime to introduce a virus or other "contaminant" into a computer.[123] Just under half the states have outlawed "spyware" or "adware," which is software that performs certain behaviors on a person's computer without first obtaining their consent, such as advertising and collecting personal information.[124] Similarly, about half of the states have passed statutes specifically criminalizing "phishing," which refers to internet schemes in which a fraudster poses as a legitimate sender in order to dupe the recipient into providing personal information.[125]

State penalties for computer crimes range widely from small fines for misdemeanor offenses to lengthy prison sentences and substantial fines for felonies.[126] Some states also provide for civil remedies for certain computer crimes.[127]

(b) Identity Theft

All 50 states and the District of Columbia criminalize identity theft or impersonation.[128] A slight majority of those statutes include restitution provisions.[129] In some states, stealing the identity of an elderly person is an aggravating factor leading to stiffer penalties.[130]

One possible method of collecting information for identity theft purposes—scanning or "skimming" of radio frequency identification (RFID) tags—has received particular scrutiny and is the subject of specific legislation in many states. As the National Conference of State Legislatures explains, an RFID tag "consists of a microchip and antenna that, when stimulated by a remote reader, sends

---

123 *See*, *e.g.*, FLA. STAT. § 815.04(1); *id.* at § 815.03(3) (defining "computer contaminant" to include viruses and worms).

124 *See State Spyware Laws*, NAT'L. CONFERENCE OF STATE LEGIS. (Dec. 3, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/state-spyware-laws.aspx.

125 *See*, *e.g.*, *Phishing*, FED. TRADE COMM'N (Sep. 2011), http://www.consumer.ftc.gov/articles/0003-phishing.

126 For example, in Missouri, "computer tampering" is a Class A misdemeanor subject to a fine not to exceed $1,000. MO. ANN. STAT. §§ 560.016, 569.095. If the tampering was for the purpose of any scheme to defraud, however, the crime is a Class D felony punishable by imprisonment for up to four years, as well as a fine of up to $5,000. MO. ANN. STAT. §§ 558.011, 560.011. In Connecticut, the offense of "computer crime in the first degree" is a class B felony, which could be punished by imprisonment up to twenty years. *See* CONN. GEN. STAT. ANN. §§ 53a-35a, 53a-252.

127 *See, e.g.*, MO. ANN. STAT. § 537.525 (providing for civil action for compensatory damages against anyone who commits computer tampering).

128 *Identify Theft*, NAT'L. CONFERENCE OF STATE LEGIS., http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx (last visited Jan. 6, 2017).

129 *Id.*

130 *See*, *e.g.*, CONN. GEN. STAT. ANN. § 53a-129b (lower dollar value threshold for class B felony if victim is over sixty years of age).

back information via radio waves."[131] RFID technology may be used in a number of consumer contexts, from race time trackers to public transit passes to no-swipe tickets at amusement parks—and most notably, in credit cards and even drivers' licenses or ID cards. Although it is not clear whether remote "skimming" of RFID chips is a serious or frequent threat, some states have enacted criminal laws addressing particular RFID applications.[132] In California, for example, it is a crime to remotely read another person's RFID identification document without that person's knowledge or consent.[133]

(c) Threats and Harassment

(1) Cyber-Stalking

All 50 states and the District of Columbia have enacted laws criminalizing stalking. A substantial majority of them have now amended their statutes to include language that expressly applies to cyber-stalking, or stalking that occurs online or uses electronic communications.[134] As one cyber-stalking expert has explained,

> cyber-stalking can include threats of violence (often sexual), spreading lies asserted as facts (like a person has herpes, a criminal record, or is a sexual predator), posting sensitive information online (whether that's nude or compromising photos or social security numbers), and technological attacks (falsely shutting down a person's social-media account).[135]

The specific conduct these statutes outlaw varies from state to state. For example, in Alaska, "non-consensual contact" for purposes of criminal stalking may include "sending mail or electronic communications" to the victim or a family member.[136] In Arizona, on the other hand, felony stalking does not include sending emails, but does cover, "[u]sing any electronic, digital or global positioning system device to surveil a specific person" for twelve hours or on two or more occasions.[137]

---

131 *Radio Frequency Identification (RFID) Privacy Laws*, NAT'L. CONFERENCE OF STATE LEGIS. (Oct. 29, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/radio-frequency-identification-rfid-privacy-laws.aspx.

132 *Id.*

133 *See, e.g.*, CAL. CIV. CODE § 1798.79 (conduct is a misdemeanor, punishable by up to a year in jail and/or a find up to $1,500).

134 WORKING TO HALT ONLINE ABUSE, http://www.haltabuse.org/resources/laws/ (last visited Jan. 13, 2017).

135 Marlisse Silver Sweeney, *What the Law Can (and Can't) Do About Online Harassment*, THE ATLANTIC (Nov. 12, 2014), http://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/ (quoting Danielle Citron, a professor at the University of Maryland's Francis King Carey School of Law).

136 ALASKA STAT. § 11.41.270(b)(3)(F).

137 ARIZ. REV. STAT. § 13-2923(C)(1)(a)(ii).

(2) Revenge Porn

Following a few high-profile cases that made clear there were gaps in the law, states have recently begun criminalizing "revenge porn," which refers to the publication (usually online) of sexually explicit photographs or videos of a person without their consent. In many cases, the victim's name and address is included along with the images. The practice became known as "[r]evenge porn" because images may be posted by the victim's former partner after a romantic relationship has ended, but in a large number of cases (such as hacking incidents), the perpetrator does not even know the victim. About sixteen states now outlaw revenge porn.[138]

The Illinois statute, passed at the end of 2014, is a particularly powerful example.[139] Unlike some other state laws, the Illinois ban applies to unauthorized publication of "selfies," or photos taken by the victim, as well as photos taken by someone else.[140] The Illinois law is not limited to nude photos, and it also applies to individuals who received the photos secondhand.[141] In Illinois, publishing revenge porn is a Class 4 felony punishable by one to three years in prison, a possible $25,000 fine, and restitution to victims for costs incurred.

Some states have law enforcement authorities that specifically investigate privacy-related criminal conduct.[142] Oftentimes the state law enforcement agency refers complainants to the FBI's IC3 at http://www.ic3.gov/default.aspx or the FTC's Complaint Assistant at https://www.ftccomplaintassistant.gov/#crnt&panel1-1.

---

138 Barbara Herman, *Illinois Passes Revenge Porn Law with Teeth*, INT'L BUS. TIMES (Jan. 6, 2015), http://www.ibtimes.com/illinois-passes-revenge-porn-law-teeth-other-states-should-copy-says-privacy-lawyer-1774974.

139 *See* 720 ILL. COMP. STAT. ANN. 5/11-23.5.

140 *Id.*

141 *Id.*

142 State law enforcement efforts vary between states. In order to identify whether a specific state has dedicated law enforcement addressing privacy-related criminal conduct, one should contact the state attorney general's office. For example, California has an "eCrime Unit" that is "tasked with investigating and prosecuting large scale identity theft and technology crimes with actual losses in excess of $50,000." *See Ecrime Unit*, STATE OF CAL. DEP'T OF JUSTICE, https://oag.ca.gov/ecrime (last visited Jan. 6, 2017). Kentucky has a "Cyber Crimes Unit" to "concentrate . . . efforts on cases of online solicitation, scams and identity theft." *See Cyber Crimes Unit*, KY.GOV, http://ag.ky.gov/criminal/dci/cybercrimes/Pages/default.aspx (last visited Jan. 6, 2017).

SIDE BAR – FEDERAL AND STATE GOVERNMENTS

The existing privacy laws governing the collection, use, and safeguards applied to personal information by state and federal governments, as well as the privacy rights of individuals with respect to such governments, are complex and varied.

The Privacy Act of 1974 imposes significant compliance obligations upon federal agencies that maintain a "system of records" that is used to access personal information, as well as government contractors that maintain such a system on behalf of federal agencies. The Privacy Act restricts disclosure of personal information by such agencies, grants individuals a right to access and seek amendment to such information, and generally requires agencies to comply with the FIPPs.

The Fourth Amendment protects citizens from unreasonable/warrantless searches or seizures by government actors, and has been interpreted to provide a right to privacy, including regarding access to electronic data and communications by government actors. Government agencies should consider these restrictions where personal information is accessed without fully transparent consent by the individual.

Many state laws exist that govern the collection, use, disclosure, and access to personal information by state governments and agencies, including laws applicable to motor vehicle records, 911 recordings, and license plate readers. In addition, many state constitutions include a general right to privacy that applies in a wide variety of contexts.

IV. GENERAL CONSUMER PROTECTION

A. Federal Privacy Statutes of General Applicability

1. Federal Trade Commission Act (FTC) Act

In its annual privacy and data security update, the FTC reported that, since inception, its privacy and data security enforcement program had been responsible for "over 130 spam and spyware cases and more than 50 general privacy lawsuits" as well as "almost 60 cases against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk."[143] A large number of those matters were brought under Section 5 of the FTC Act, 15 U.S.C. § 45(a), which generally authorizes FTC consumer protection activities to prevent "persons, partnerships, or corporations" subject to FTC jurisdiction from engaging in "unfair or deceptive acts and practices" (UDAP) "in and affecting commerce."[144] The FTC uses its Section 5 authority to bring enforcement actions against entities that fail to protect consumer privacy and fail to properly secure personal information, as well as to engage in a wide variety of policy, educational, and other activities relating to consumer privacy and data security.[145]

From the FTC's perspective, using Section 5 as a basis for privacy and data security activities is consistent with well-established FTC consumer protection and UDAP principles. As Bureau of Consumer Protection Director Jessica Rich made clear in 2014,

> [T]his is the same Section 5 that we have used for decades to challenge practices involving deceptive advertising and fraud; and the same Section 5 that has been litigated and developed in the courts. There is no separate privacy and data security jurisprudence, but simply application of a tried and true Section 5 standard . . . just as

---

[143] *Privacy & Data Security Update*, FED. TRADE COMM'N (2015), *available at* https://www.ftc.gov/reports/privacy-data-security-update-2015.

[144] The FTC lacks jurisdiction over a number of categories of entities, including non-profit organizations, insurance and financial institutions, and providers of federally regulated transportation and telecommunication services. *See* 15 U.S.C. § 45(a)(2). Other federal agencies have general statutory authority to protect consumers with regard to privacy and data security in areas where the FTC lacks jurisdiction, including, as discussed below, the Federal Communications Commission for issues relating to telecommunications and telemarketing, and the Consumer Financial Protection Bureau with regard to financial institutions. In addition, as discussed in the subject matter sections below, specific privacy and data security statutes vest regulatory and enforcement authority in the FTC and other federal agencies.

[145] Information about the FTC's privacy and data security activities, including cases and educational materials, are available on the FTC website, including at www.consumer.ftc.gov/topics/privacy-identity (consumers), www.ftc.gov/tips-advice/business-center/privacy-and-security (businesses), and www.ftc.gov/datasecurity. In addition, the International Association of Privacy Professionals (IAPP) maintains an online "FTC Casebook," a "full-text searchable, tagged, indexed and annotated" collection of FTC privacy and data security cases, https://iapp.org/resources/ftc-casebook (IAPP membership required).

> the law has been applied to pyramid schemes, business opportunity scams, weight loss products, cramming, and many other areas of consumer protection.[146]

Businesses and other entities have questioned the FTC's authority to apply Section 5 UDAP standards to privacy and data security matters, particularly given the existence of other more specific statutes that authorize the FTC to regulate and enforce privacy and data security issues for specific categories of activities. Until 2015, however, the FTC's authority to bring privacy and data security enforcement actions under Section 5 of the FTC Act had not been challenged in and substantively reviewed by a federal court of appeals, because the administrative and federal court complaints filed by the FTC in privacy and data security enforcement actions had, with two exceptions, been resolved by settlement agreements. Through what Professors Daniel Solove and Woodrow Hartzog describe as an FTC-developed "common law of privacy":

> the FTC has risen to act as a kind of data protection authority in the United States. Despite having limited jurisdiction and limited resources, the FTC has created a body of common law doctrines through complaints, consent decrees, and various reports and other materials. The FTC's jurisprudence has developed in some classic common law patterns, evolving from general to more specific standards, gradually incorporating more qualitative judgments, imposing certain default standards, and broadening liability by recognizing contributory liability.[147]

In the only two privacy and data security cases to be litigated rather than resolved by settlements, the FTC's use of Section 5 authority and its failure to provide concrete guidance about specific privacy and data security practices have been hotly contested. In its administrative complaint against LabMD, the FTC alleged that the medical testing laboratory had unfairly failed to secure personal information.[148] That matter is still underway. In its complaint in federal court against a number of Wyndham hotel entities,[149] the FTC alleged that the hotels had deceptively asserted that they protected personal information and unfairly failed to secure that personal information. In August 2015, the United States Court of Appeals for the Third Circuit upheld the FTC's authority to "regulate cybersecurity under the unfairness prong of [15 U.S.C.] § 45(a)" in the FTC's action against Wyndham Worldwide.[150]

---

146 Jessica Rich, *The FTC's Privacy and Data Security Program: Where It Came From, Where It's Going*, Remarks to the International Association of Privacy Professionals Global Privacy Summit (Mar. 6, 2014), *available at* www.ftc.gov/system/files/documents/public_statements/293641/140306iappremarks.pdf.

147 Solove & Hartzog, *supra* note 43, at 676.

148 *In re* abMD, FTC Matter No. 102 3099, Docket No. 9357, *available at* www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

149 FTC v. Wyndham Worldwide Corp. et al., Case No. 2:13-cv-01887-ES-JAD (D.N.J.), some documents *available at* https://www.ftc.gov/enforcement/cases-proceedings/1023142-x120032/wyndham-worldwide-corporation.

150 FTC v. Wyndham Worldwide Corp. et al., Case No. 14-3514 (3rd Cir. Aug. 24, 2015), opinion *available at* www.ftc.gov/system/files/documents/cases/150824wyndhamopinion.pdf.

Under Section 5, the FTC defines deceptive conduct to be "a misrepresentation, omission, or other practice, that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment."[151] In its privacy and data security enforcement actions, typical FTC deception counts focus on an entity's failure to "do what it says and say what it does" with regard to its privacy and data security practices. For example, in August 2015, the FTC announced settlements with 13 companies that claimed to be current participants in the now defunct EU-US Safe Harbor Framework but whose certifications had either lapsed or never been submitted.[152] Similarly, in March 2015, the FTC announced a settlement with TRUSTe, a company that provided "Certified Privacy Seals" to client websites and mobile applications that complied with privacy program requirements that TRUSTe administered, including the Children's Online Privacy Protection Act and the EU-US Safe Harbor Framework. The FTC complaint alleged that TRUSTe's claim that it recertified its clients annually was deceptive because "from 2006 until January 2013, Respondent did not conduct annual recertifications for all companies holding TRUSTe Certified Privacy Seals. In over 1,000 instances, TRUSTe conducted no annual review of the company's compliance with applicable Program Requirements."[153]

An unfair practice under Section 5 is conduct that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[154] In privacy and data security enforcement actions, typical FTC unfairness counts involve an entity that fails to properly handle and safeguard personal information. For example, the FTC announced settlements with two debt brokers who were trying to sell debt portfolios in an online marketplace and posted information in an unencrypted spreadsheet. The FTC's complaint contained an unfairness count alleging that the would-be sellers:

> publicly disclosed consumers' sensitive personal information without the consumers' knowledge or consent, including, consumers' first or last names, addresses, telephone numbers, email addresses, dates of birth, driver's license numbers, credit card num-

---

151 *See also FTC Policy Statement on Deception*, FED. TRADE COMM'N (Oct. 10, 1983), *available at* www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

152 *See* case materials linked to *Thirteen Companies Agree to Settle FTC Charges They Falsely Claimed To Comply With International Safe Harbor Framework*, FED. TRADE COMM'N (Aug. 17, 2015), *available at* www.ftc.gov/news-events/press-releases/2015/08/thirteen-companies-agree-settle-ftc-charges-they-falsely-claimed.

153 *See* case materials linked to *TRUSTe Settles FTC Charges It Deceived Consumers Through Its Privacy Seal Program*, FED. TRADE COMM'N (Nov. 17, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its.

154 15 U.S.C. § 45(n). *See also* Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science and Transportation, United States Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (December 17, 1980), reprinted in *In re* Int'l Harvester Co., 104 F.T.C. 949, 1070, 1074 n.3 (1984) ("Unfairness Policy Statement").

> bers, full bank account and bank routing numbers, employers' names and contact information, the consumers' status as purported debtors, and the amount of each consumer's purported debt.[155]

Similarly, the FTC entered a settlement with a medical transcription company that primarily worked online with contract transcribers. The FTC complaint included an unfairness count alleging that the defendants "failed to employ reasonable and appropriate measures to prevent unauthorized access to personal information in audio and transcript files" and that, as a result of that failure, the defendants did not know that the contractor they worked with:

> used a File Transfer Protocol ("FTP") application to both store medical audio and transcript files on its computer network and transmit the files between the network and its typists. The application stored and transmitted files in clear readable text and was configured so that the files could be accessed online by anyone without authentication. A major search engine therefore was able to reach . . . and index thousands of medical transcript files . . . .[156]

The FTC has the same range of equitable remedies available to it in privacy and data security enforcement actions that it has for its other Section 5 consumer protection actions. Thus, among other forms of relief, the FTC may seek an ex parte temporary restraining order (including asset freezes and appointment of a receiver, in appropriate cases, to preserve assets and information), temporary and permanent injunctions to stop the unlawful UDAP conduct, and to impose additional "fencing-in" obligations on future conduct. FTC settlements in privacy and data security cases under Section 5 also typically include provisions requiring entities to implement effective privacy and/or data security programs, obtain regular third-party audits of the program(s), and comply with records-retention, compliance, and reporting requirements, usually for a 20-year period. The FTC retains enforcement authority over resolved cases and can bring contempt actions for violation of privacy and data protection orders.

2. Children's Online Privacy Protection Act (COPPA; 15 U.S.C. §§ 6501–6505)

In 1998, Congress enacted the Children's Online Privacy Protection Act (COPPA), which protects personal information of individuals under the age of 13.[157] In general, COPPA prohibits operators

---

[155] Fed. Trade Comm'n v. Cornerstone and Co., et al., Case No. 1:14-cv-1479-RC, Dkt. No. 3 at 6–7 (D.D.C. Aug. 27, 2014); *see also Debt Brokers Settle FTC Charges They Exposed Consumers' Information Online*, FED. TRADE COMM'N (April 13, 2015), *available at* www.ftc.gov/news-events/press-releases/2015/04/debt-brokers-settle-ftc-charges-they-exposed-consumers.

[156] *See* case materials linked to *Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information*, FED. TRADE COMM'N (Jan. 31, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

[157] 15 U.S.C. § 6501(1).

of commercial[158] websites and online services (including mobile apps) from collecting, using, or disclosing personal information from children except in compliance with COPPA implementing regulations issued by the FTC,[159] or in compliance with a self-regulatory "safe harbor" program that has been reviewed and approved by the FTC.[160] COPPA applies not only to operators of sites and services that are specifically "directed to children," but also to any operator "who has actual knowledge that it is collecting personal information from a child."[161]

As regulator and primary enforcer of COPPA, the FTC maintains COPPA-related information online for businesses and consumers, including educational materials for businesses and consumers, agency guidance and recommendations, FTC policy and enforcement activities, and information about approved safe harbor programs and approved methods for verifying parental consent.[162]

The FTC's COPPA Rule, 16 C.F.R. Part 312, took effect in April 2000, and was last amended effective July 2013. As amended, the COPPA Rule defines personal information to be "individually identifiable information about an individual" that is "collected online," including:

a) a first and last name;

b) a home or other physical address including street name and name of a city or town;

c) an e-mail address or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's e-mail address, that permits direct contact with a person online;

d) a telephone number;

e) a social security number;

f) a persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of

---

158 COPPA does not alter the FTC's lack of jurisdiction over non-profit entities.

159 15 U.S.C. § 6502(a).

160 *Id.* at § 6503.

161 *Id.*

162 *See Children's Online Privacy Protection Rule ("COPPA")*, FED. TRADE COMM'N, www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule; *Children's Privacy*, FED. TRADE COMM'N, www.ftc.gov/tips-advice/business-center/privacy-and-security/children's-privacy (businesses); *Protecting Your Child's Privacy Online*, FED. TRADE COMM'N, www.consumer.ftc.gov/articles/0031-protecting-your-childs-privacy-online (consumers). The FTC also maintains a "COPPA Hotline" for questions not covered by its existing materials, *available at* COPPAHotLine@ftc.gov.

the individual with other information such that the combination permits physical or online contacting; or

g) information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.[163]

The FTC defines "collection" broadly to include not only directly asking children to submit personal information online, but also providing services that allow children to make their personal information publicly available online (for example, through instant messaging, chat rooms, or bulletin boards), and passively tracking children while they are online (for example, by using cookies or other unique online identifiers).[164]

The COPPA Rule identifies a number of factors to be considered when determining whether a website or online service is "directed to children," and thus subject to COPPA, including:

- specific characteristics of the site or service, including subject matter, visual or audio content, age of models, language or other characteristics or online service, and use of animated characters and/or child-oriented activities and incentives;
- extent to which advertising "promoting or appearing" on the website or online service is directed to children; and
- evidence about the intended and actual audience.[165]

To comply with COPPA, operators of websites and online services that collect, use, or disclose personal information from children must:

- provide a privacy notice that is "clearly and understandably written," complete, and contains "no unrelated, confusing, or contradictory materials";[166]
- with limited exceptions, obtain "verifiable parental consent," to the collection of personal information from children;[167]

---

[163] 16 C.F.R. § 312.2.

[164] *Id.*

[165] *Id.* at § 312.2.

[166] *Id.* at §§ 312.3(a), 312.4(a)–(b).

[167] *Id.* at §§ 312.3(b), 312.5.

- provide parents with the ability to review personal information collected from their child and prevent further use or maintenance of that collected information;[168]

- limit the personal information that children must disclose to participate in a game, prize offering, or other activity to the information than is reasonably necessary to that activity;[169] and

- use "reasonable procedures" to protect the confidentiality, security, and integrity of personal information collected from children.[170]

The requirements for entities that wish to operate self-regulatory programs under COPPA's safe harbor program, and for COPPA-covered operators who wish to use the COPPA safe harbor to be "deemed to be in compliance with" the COPPA Rule, are set forth at 16 C.F.R. § 312.10.

The FTC has primary COPPA enforcement authority to the extent that an entity is subject to FTC Act jurisdiction, and COPPA violations are subject to civil penalties as well as the equitable relief and remedies that are available under the FTC Act.[171] In addition, to the extent the FTC lacks jurisdiction over certain entities (e.g., common carriers, insurance, and financial institutions), the federal agencies with jurisdiction over those entities have COPPA enforcement authority.[172] State attorneys general also have COPPA enforcement authority with regard to conduct affecting their state residents, but that authority must be exercised in consultation with the FTC.[173]

3. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act; 15 U.S.C. §§ 7701–13)

The CAN-SPAM Act addresses concerns about "commercial electronic mail messages," which are defined as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service."[174] Congress noted "the extremely rapid growth in the volume of unsolicited commercial electronic mail," most of which "is fraudulent or deceptive in one or more respects."[175] In general, CAN-SPAM prohibits marketers from using deceptive header information that conceals the identity of the sender and deceptive subject lines that

---

168 *Id.* at §§ 312.3(c), 312.6.

169 *Id.* at §§ 312.3(d), 312.7.

170 *Id.* at §§ 312.3(e), 312.8.

171 15 U.S.C. §§ 6505(a), (d); 16 C.F.R. § 312.9.

172 15 U.S.C. § 6505(b).

173 *Id.* at § 6504.

174 *Id.* at § 7702(2)(a).

175 *Id.* at § 7701(a)(2).

conceal the nature of the communication.[176] It also requires all marketing emails to include a return email address or similar method to opt out of future messages, and requires marketers to honor all such requests.[177]

The CAN-SPAM Act prohibits "aggravated" commercial email activity, which includes automated collection of email addresses from online locations, automated generation of possible email addresses from patterns, automated creation of multiple accounts to send commercial email from, and unauthorized access to and use of a network to send commercial email messages.[178] The FTC implemented the CAN-SPAM Act in its CAN-SPAM Rule, 16 C.F.R. Part 316.

As regulator and primary enforcer of the CAN-SPAM Act and Rule, the FTC maintains CAN-SPAM-related information online, including educational materials, agency guidance and recommendations, and policy and enforcement activities.[179]

The Rule specifies that the CAN-SPAM Act applies when the "primary purpose" of an email message is commercial.[180] For email messages that contain commercial advertising or promotion blended with other content, the CAN-SPAM Rule provides that the primary purpose will be determined based on the nature of the other content and the manner in which it is presented:

- If the blended content is "transactional or relationship content" that relates to a prior or current business transaction or that provides information about the recipient's ongoing relationship with the business (e.g., warranties, recalls, changes in policies and features), the primary purpose of the email message is commercial if a recipient would reasonably interpret the subject line as relating to advertising or promotion, or if the bulk of the transactional or relationship content does not appear at the beginning of the message.[181]

- If the blended content is something other than transactional or relationship content, the primary purpose of the email message is commercial if a recipient would reasonably interpret the subject line as relating to advertising or promotion or would reasonably interpret the primary purpose of the body of the message—

---

176 *Id.* at §§ 7704(a)(1), (2).

177 *Id.* at §§ 7704(a)(3)–(5).

178 *Id.* at § 7704(b).

179 *See CAN-SPAM Rule*, FED. TRADE COMM'N, www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/can-spam-rule; *CAN-SPAM Act: A Compliance Guide for Business*, FED. TRADE COMM'N, www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

180 16 C.F.R. § 316.3.

181 *Id.* at §§ 316.3(a)(2), (c).

based on factors such as appearance, emphasis, and location of the content in the message—to be advertising or promotion.[182]

For email messages containing sexually oriented material, the first 19 characters on the subject line must be, in all caps and as depicted "SEXUALLY-EXPLICIT:" and that same phrase must also appear when the email is opened, along with the other required CAN-SPAM elements.[183] Finally, the CAN-SPAM Rule prohibits marketers from charging a fee, collecting information other than email address and opt-out preferences, or otherwise complicating a recipient's ability to opt out of future marketing messages.[184]

The CAN-SPAM Act applies not only to those who directly engage in prohibited conduct, but also to businesses that knowingly allow themselves to be marketed in ways that violate the act (unless they take steps to prevent the violation or notify the FTC), and, under certain circumstances, to third parties working with those businesses.[185]

The FTC has primary CAN-SPAM enforcement authority to the extent an entity is subject to FTC Act jurisdiction, and CAN-SPAM violations are subject to civil penalties, and to the other relief and remedies available under the FTC Act.[186] In addition, to the extent the FTC lacks jurisdiction over certain entities (e.g., common carriers, insurance, and financial institutions), the federal agencies with jurisdiction over those entities have CAN-SPAM enforcement authority.[187] State attorneys general also have CAN-SPAM enforcement authority with regard to conduct affecting their state residents, but that authority must be exercised in consultation with the FTC.[188] Finally, internet service providers who have been adversely affected by CAN-SPAM Act violations can seek injunctive relief and damages in federal district court.[189]

In addition to actual damages, treble damages are available in certain instances for "knowing and willful violations" of the CAN-SPAM Act and for the aggravated violations defined in § 7704(b). Note that, when seeking cease-and-desist orders and other forms of injunctive relief, the FTC, the Federal Communications Commission, and state enforcement entities are exempt from CAN-SPAM Act requirements to allege and prove a particular state of mind.[190]

---

182 *Id.* at § 316.3(a)(3).

183 *Id.* at §§ 316.4(a)(1), (2), unless the email recipient has previously provided affirmative consent, as defined in 15 U.S.C. § 7702.

184 16 C.F.R. § 316.5.

185 15 U.S.C. §§ 7705(a), (b).

186 *Id.* at §§ 7706(a), (d).

187 *Id.* at § 7706(b).

188 *Id.* at § 7706(f).

189 *Id.* at § 7706(g).

190 *Id.* at §§ 7706(e), (f)(2).

Although the primary relief and remedies under the CAN-SPAM Act are civil, the act provides for criminal liability in certain circumstances. Congress noted that "[s]ome commercial electronic mail contains material that many recipients may consider vulgar or pornographic in nature."[191] As a result, failure to comply with the requirement that messages containing sexually oriented material be identified in the subject line and that the explicit material not be displayed upon opening but instead provide a link or similar mechanism,[192] can give rise to criminal liability.[193] Similarly, because "spam has become the method of choice for those who distribute pornography, perpetrate fraudulent schemes, and introduce viruses, worms, and Trojan horses into personal and business computer systems," Congress instructed the U.S. Sentencing Commission to "review and, as appropriate, amend the sentencing guidelines and policy statements to provide appropriate penalties for . . . offenses that may be facilitated by the sending of large quantities of unsolicited electronic mail."[194]

4. Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"; 15 U.S.C. §§ 6101–6108)

The Telemarketing Act is the FTC equivalent of the Federal Communication Commission's (FCC) Telephone Consumer Protection Act of 1991 (TCPA; 47 U.S.C. § 227), although the FCC's TCPA jurisdiction is broader than the FTC's Telemarketing Act jurisdiction. Given the overlapping authority over telemarketing activity and the joint coordination regarding the National Do Not Call Registry, the FTC and the FCC coordinate many of their telemarketing policy and enforcement activities.

The Telemarketing Act addresses widespread concerns about, among other things, the dramatic increase in telemarketing fraud "and other forms of telemarketing deception and abuse," and the difficulties of bringing law enforcement actions against highly mobile and often out-of-state telemarketers.[195] Accordingly, Congress instructed the FTC to promulgate regulations to:

- define and prohibit deceptive telemarketing acts or practices, including "fraudulent charitable solicitations";
- prohibit "a pattern of unsolicited telephone calls" that "the reasonable consumer would consider coercive or abusive of such consumer's right to privacy";
- restrict "the hours of the day and night when unsolicited telephone calls may be made to consumers"; and
- require telemarketers to "promptly and clearly disclose" that "the purpose of the call is to sell goods or services" or "to solicit charitable contributions, donations,

---

191 *Id.* at § 7701(a)(5).

192 *Id.* at § 7704(d).

193 *Id.* at § 7704(d)(5).

194 *Id.* at §§ 7703(b)(1), (c)(3).

195 *Id.* at § 6101.

or gifts or money of any other thing of value" and to make "other disclosures as the [FTC] deems appropriate."[196]

Congress also authorized the FTC, at its discretion, to address conduct by entities that "assist or facilitate" deceptive telemarketing practices, "including credit card laundering."[197] The FTC implemented the act in its Telemarketing Sales Rule (TSR), 16 C.F.R. Part 310.

As regulator and primary enforcer of the Telemarketing Act and the TSR, the FTC maintains telemarketing-related information online, including educational materials, agency guidance and recommendations, and enforcement activities.[198]

The TSR, like the Telemarketing Act, defines, with limited exceptions, telemarketing as "a plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call."[199] The portion of the TSR prohibiting deceptive conduct, 16 C.F.R. § 310.3, is focused on conduct involving disclosures, billing practices, and misrepresentations that are generally beyond the scope of this Primer.

The portion of the TSR addressing abusive telemarketing practices, however, protects consumer privacy interests by, among other things, prohibiting the following telemarketing conduct:

- "threats, intimidation, or the use of profane or obscene language";
- calls intended to "annoy, abuse, or harass";
- calling persons who have previously indicated that they do not wish to be contacted by telemarketers;
- failing to connect the person who answers a telemarketing call with a live telemarketer within 2 seconds ("abandoned" call);
- use of prerecorded messages, including "robocalls," with very limited exceptions; or

196 *Id.* at § 6102.

197 *Id.*

198 *See Telemarketing*, FED. TRADE COMM'N, www.ftc.gov/tips-advice/business-center/advertising-and-marketing/telemarketing (last visited Jan. 6, 2017) (businesses); *Limiting Unwanted Calls & Emails*, FED. TRADE COMM'N, www.consumer.ftc.gov/topics/limiting-unwanted-calls-emails (last visited Jan. 6, 2017) (consumers).

199 15 U.S.C § 6106; 16 C.F.R. § 310.2.

- calling persons before 8:00 a.m. or after 9:00 p.m. at their local time without prior consent.[200]

When promulgating the TSR, the FTC also implemented company-specific and national "do not call" (DNC) lists for individuals who did not wish to be contacted by telemarketers. The FTC maintains, in collaboration with the FCC, a national DNC Registry for consumers who wish to avoid telemarketing calls, www.donotcall.gov. With certain exceptions, the TSR prohibits telemarketers from:

- calling numbers on the company-specific and national DNC list;[201]
- "denying or interfering" with an individual's right to be placed on a company-specific or national DNC list;[202] and
- "sell[ing], rent[ing], leas[ing], purchas[ing], or us[ing]" a company-specific or national DNC list for any purpose other than preventing phone calls to listed numbers.[203]

Shortly after the FTC promulgated the TSR, Congress authorized the FTC's National DNC Registry, ratified the TSR concept of DNC lists, and authorized the FTC to "assess and collect an annual fee . . . to implement and enforce" the National DNC Registry.[204]

The FTC has primary Telemarketing Act and TSR enforcement authority over entities within its FTC Act jurisdiction, and can use all powers and obtain all remedies and relief available to it under the FTC Act.[205] With regard to entities beyond the FTC's jurisdiction, Congress instructed the Securities and Exchange Commission (SEC) to review and, as appropriate, promulgate "rules substantially similar to" the TSR.[206] A later Telemarketing Act amendment provides that a violation of the TSR by an entity subject to the jurisdiction of the Consumer Financial Protection Bureau (CFPB) is deemed to be a violation of the CFPB's rules prohibiting unfair, deceptive, or abusive acts or practices.[207] Finally, Congress directed the FCC to "issue a final [DNC] rule pursuant to the rulemaking proceeding that it began on September 18, 2002, under the Telephone Consumer Protection Act (47 U.S.C. 227 *et seq*.)."[208]

---

200 16 C.F.R. § 310.4.

201 *Id.* at § 310.4(b)(iii).

202 *Id.* at § 310.4(b)(ii).

203 *Id.* at § 310.4(b)(iii).

204 15 U.S.C. §§ 6151–6152.

205 *Id.* at § 6105.

206 *Id.* at § 6102(d).

207 *Id.* at § 6102(c)(2).

208 *Id.* at § 6153.

State attorneys general have enforcement authority with regard to conduct that violates the TSR and affects their state residents, but that authority must be exercised with notification to the FTC, and states cannot bring enforcement actions in federal court if either the FTC or the CFPB have pending enforcement actions.[209] Similarly, private individuals have enforcement authority for conduct that violates the TSR "if the amount in controversy exceeds the sum or value of $50,000 in actual damages for each person adversely affected by such telemarketing," but they must also notify the FTC of any such action and defer to any pending FTC and CFPB enforcement actions.[210]

5. Communications Act of 1934 (47 U.S.C. §§ 151 *et seq.*)

The FCC's authorizing statute, the Communications Act of 1934 (47 U.S.C. §§ 151 *et seq.*), imposes affirmative privacy and data security obligations on telecommunications carriers in the form of the "duty to protect the confidentiality of proprietary information of, and relating to other telecommunication carriers, equipment manufacturers, and customers."[211] The Communications Act defines the personal information that carriers must protect as "Consumer Proprietary Network Information" (CPNI), which consists of:

- information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

- information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier,

but not "subscriber list information," which is information about the names, numbers, and addresses of subscribers if that information has or will be published by the carrier.[212] In a Declaratory Ruling, the FCC also determined that the definition of CPNI and the related obligations also applied "to information that telecommunications carriers cause to be stored on their customers' [mobile] devices when carriers or their designees have access to or control over that information."[213]

---

[209] *Id.*

[210] 15 U.S.C. § 6154.

[211] 47 U.S.C. § 222(a). This statutory requirement for entities subject to FCC jurisdiction to protect proprietary information, including the personal information of customers, provides the FCC with a direct statutory hook for its privacy and data security enforcement activities, unlike the FTC's use of its broader and more general "unfair or deceptive acts or practices" authority for privacy and data security activities under Section 5 of the FTC Act.

[212] 47 U.S.C. §§ 222(h)(1), (3).

[213] *In re* Implementation of the Telecommc'ns Act of 1996: Telecommc'ns Carriers' Use of Customer Proprietary Network Info. and Other Customer Info., FCC 13-89, CC Docket No. 96-115, Declaratory Ruling (June 27, 2013), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-89A1.pdf.

In February 2015, as part of its hotly contested "Open Internet" initiative, a divided FCC issued an Order that reclassified "broadband Internet access service"—internet services provided by cable, phone, and wireless internet service providers (ISPs)—as telecommunications services and thus made ISPs "common carriers."[214] That Order, which is currently on appeal before the United States Court of Appeals for the District of Columbia Circuit,[215] shifts jurisdiction over ISPs from the FTC to the FCC, and imposes on ISPs the statutory privacy and data security protections discussed in this section.

With limited exceptions, carriers can only use or disclose CPNI to the extent necessary to provide telecommunications services; carriers may also disclose CPNI in response to an "affirmative written request by the customer, to any person designated by the customer."[216] The FCC implemented 47 U.S.C. § 222 in its regulations at 47 C.F.R. §§ 64.2001–.2011.

The FCC maintains Communications Act-related information online, including educational materials, agency guidance, and enforcement activities.[217] The FCC regulations provide additional detail about the limited circumstances in which CPNI can be used without customer approval,[218] and place the burden on the carrier to demonstrate that customer approval has been obtained.[219]

Even more important in terms of the FCC's privacy and data security enforcement activities, the FCC regulations impose obligations on carriers with regard to obtaining customer approval, using and securing CPNI, and verifying compliance. When soliciting approval, carriers must first notify customers of "their right to restrict use of, disclosure of, and access to" CPNI, and do so in a way that permits the customer to make an informed decision, including the carrier's identification of what CPNI is, who will receive it and why, and the customer's right to revoke approval.[220] Carriers must maintain safeguards to make sure that CPNI is used appropriately, including training, a supervisory review process, retention of compliance records, and annual certification of the carrier's compliance with the CPNI rules.[221] The FCC also requires carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI," including "properly

---

214 *In re* Protecting and Promoting the Open Internet, Order, FCC 15-24, Report and Order on Remand, Declaratory Ruling, and Order (Feb. 26, 2015), 30 FCC Rcd. 5601 (2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf.

215 United States Telecom Ass'n, et al. v. FCC and U.S.A, No. 15-1063 (D.C. Cir. 2015).

216 *See* 47 U.S.C. § 222(c).

217 *See, e.g.*, *Protecting Proprietary Information Including Customer Proprietary Network Information (CPNI)*, FED. COMMC'NS COMM'N, http://transition.fcc.gov/eb/CPNI/; *Enforcement Primer*, FED. COMMC'NS COMM'N, https://www.fcc.gov/encyclopedia/enforcement-primer; *Consumer Guides*, FED. COMMC'NS COMM'N, www.fcc.gov/encyclopedia/consumer-publications-library#Privacy; *Protecting Your Telephone Calling Records*, FED. COMMC'NS COMM'N, www.fcc.gov/guides/protecting-your-telephone-calling-records.

218 47 C.F.R. § 64.2005.

219 *Id.* at § 64.2007.

220 *Id.* at § 64.2008.

221 *Id.* at § 64.2009.

authenticat[ing]" customers who request disclosure of their CPNI, using methods other than "readily available biographical or account information" to authenticate customers with "lost or forgotten passwords," and "notify[ing] customers immediately" about account changes.[222]

Finally, the regulations impose specific incident notification and response requirements in addition to any requirements that might be imposed by states. The regulations define a breach as a circumstance in which "a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."[223] Carriers must notify the USSS and the FBI "as soon as practicable" but "no later than seven (7) business days" after "reasonable determination of a breach," and then wait another 7 days before notifying its customers or the public about the breach, unless earlier notification is necessary to avoid "irreparable harm" or delayed notification is required to avoid "imped[ing] or compromis[ing] a criminal investigation or national security."[224] The carrier has no discretion in terms of breach notification: it "shall notify its customers" about a breach of their CPNI.[225]

From the FCC's perspective, the failure to reasonably secure customers' personal information violates a carrier's statutory duty under 47 U.S.C. § 222 and constitutes an "unjust and unreasonable practice" that is unlawful under 47 U.S.C. § 201 and subject to civil penalties and injunctive relief. In April 2015, the FCC obtained a $25 million civil penalty from AT&T Services, Inc. to resolve an FCC investigation into AT&T's failure "to properly protect the confidentiality of almost 280,000 customers' proprietary information, including sensitive personal information such as customers' names and at least the last four digits of their Social Security numbers, as well as account-related data known as customer proprietary network information (CPNI), in connection with data breaches at AT&T call centers in Mexico, Columbia, and the Philippines."[226] The breaches involved unauthorized access to and sales of CPNI to third parties, and the consent decree required AT&T to:

> develop and implement a compliance plan to ensure appropriate processes and procedures are incorporated into AT&T's business practices to protect consumers against similar data breaches in the future. In particular, AT&T will be required to improve its privacy and data security practices by appointing a senior compliance manager who is privacy certified, conducting a privacy risk assessment, implementing an information security program, preparing an appropriate compliance manual, and regularly training employees on the company's privacy policies and the applicable privacy legal authorities.[227]

---

[222] *Id.* at § 64.2010.

[223] *Id.* at § 64.2011(e).

[224] *Id.* at §§ 64.2011(a), (b).

[225] *Id.* at § 64.2011(c).

[226] *In re* AT&T Servs., Inc., DA 15-399, File No.: EB-TCD-14-00016243, Order (April 8, 2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-15-399A1.pdf.

[227] *Id.*

Similarly, in September 2014, the FCC obtained a $7,400,000 civil penalty from Verizon to resolve an FCC investigation into Verizon's "failure to generate the required opt-out notices to approximately two million of the company's customers. These failures deprived those customers of information about Verizon's marketing practices and its customers' right to deny Verizon permission to access or use their personal data to market new Verizon services to those customers."[228] The consent decree required Verizon to:

> (i) implement a process to place an opt-out notice on every invoice (whether electronic or paper) to every customer for whom Verizon relies on opt-out consent; (ii) designate a senior corporate manager as a compliance officer; (iii) implement a process for immediately reporting to the Compliance Officer any problems detected with opt-out notices, regardless of size; and (iv) develop and implement a three-year compliance plan.[229]

6. Telephone Consumer Protection Act of 1991 (TCPA; 47 U.S.C. § 227)

As noted above, the TCPA is the FCC equivalent of the FTC's Telemarketing Act, although the FCC's TCPA jurisdiction is broader than the FTC's Telemarketing Act jurisdiction. As also noted above, given the overlapping authority over telemarketing activity and the joint coordination regarding the National DNC Registry, the FTC and the FCC coordinate many of their telemarketing policy and enforcement activities.

In its findings supporting the TCPA, Congress found, among other things, that "[m]ore than 300,000 solicitors call more than 18,000,000 Americans every day" and that "[t]otal United States sales generated through telemarketing amounted to $435,000,000,000 in 1990, a more than four-fold increase since 1984."[230] Accordingly, Congress instructed the FCC to balance "[i]ndividuals' privacy rights, public safety interests, and commercial freedoms of speech and trade . . . in a way that protects the privacy of individuals and permits legitimate telemarketing practices" and to "consider adopting reasonable restrictions on automated or prerecorded calls to businesses as well as to the home, consistent with the constitutional protections of free speech."[231] The FCC implemented the TCPA in its regulations at 47 C.F.R. § 64.1200.

The TCPA and its implementing rule, with limited exceptions for emergencies and prior express consent, prohibit any "person or entity" from:

---

[228] *In re* Verizon Compliance with the Comm'n's Rules and Regulations Governing Customer Proprietary Network Info., DA 14-1251, File No.: EB-TCD-13-00007027, Adopting Order (Sept. 2, 2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1251A1.pdf.

[229] *Id.*

[230] 47 U.S.C. § 227 note.

[231] *Id.*

- using an automatic telephone dialing system or an artificial or prerecorded voice to call emergency telephone lines; rooms in hospitals, health care facilities, and retirement facilities; paging services; or mobile phones;[232]

- making or causing someone else to make a telemarketing call to any of the above facilities using an artificial or prerecorded voice;[233]

- using an artificial or prerecorded voice to make a telemarketing call to a residential line;[234]

- sending unsolicited advertisements to a telephone facsimile machine;[235]

- using an automatic telephone dialing system in a way that ties up two or more telephone lines of a multi-line business;[236]

- causing any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value;[237]

- disconnecting an unanswered telemarketing call before at least 15 seconds or 4 rings;[238]

- abandoning more than three percent of all telemarketing calls in a 30-day period by failing to connect a person who answers with a live sales representative within two seconds;[239]

- using any technology to dial any telephone number to determine whether the line is a facsimile or voice line;[240]

---

[232] *Id.* at § 227 (b)(1)(A).

[233] *Id.* at § 227 (b)(1)(B).

[234] *Id.* at § 227 (b)(1)(C).

[235] *Id.* at § 227 (b)(1)(D).

[236] *Id.* at § 227 (b)(4).

[237] *Id.* at § 227 (e)(1).

[238] 47 C.F.R. § 64.1200(a)(6).

[239] *Id.* at § 64.1200(a)(7).

[240] *Id.* at § 64.1200(a)(8).

- initiating any telephone solicitations before 8:00 a.m. or after 9:00 p.m. local time at the called party's location;[241] or

- initiating any telephone solicitations to numbers listed in the National DNC Registry, although the caller can escape liability for the violation if it can demonstrate that the call was in error and that its routine business practices meet the regulatory standard for DNC compliance.[242]

In addition, any person or entity who makes telemarketing calls to residential lines must have procedures in place to create and maintain an entity-specific DNC list in accordance with the standards set forth at 47 C.F.R. § 64.1200(d), including the requirement to provide the called party with the name of the individual caller, the name of the person or entity on whose behalf the call is being made, and the telephone number or address at which the person or entity may be contacted.

In June 2015, the FCC issued a Declaratory Ruling and Order to resolve "21 separate requests for clarification or other action regarding the TCPA or the Commission's rules and orders."[243] Among other things, the Order confirmed that:

- callers who are not "currently" or "presently" dialing random or sequential phone numbers still must obtain consumer consent for calls using artificial or prerecorded voices ("robocalls");

- internet-to-phone text messages require consumer consent;

- text messages are "calls" subject to the TCPA;

- the Communications Act and FCC rules do not prevent consumers and their carriers and Voice over Internet Protocol (VoIP) providers from using call-blocking technology to avoid unwanted robocalls; and

- certain free, pro-consumer financial- and healthcare-related messages are exempt from the consumer-consent requirement, subject to strict conditions and limitations to protect consumer privacy.[244]

The FCC's enforcement activities under the TCPA primarily involve marketers who send unsolicited junk faxes. For example, in January 2015, the FCC entered an $87,500 forfeiture order against

---

[241] *Id.* at § 64.1200(b)(c)(1).

[242] *Id.* at § 64.1200(b)(c)(2).

[243] *In Re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, FCC 15-72, CG Docket No. 02-278, Declaratory Ruling and Order (June 18, 2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1.pdf.

[244] *Id.*

Worldwide Industrial Enterprises, Inc., which "faxed 17 advertisements to consumers who did not request them, did not want them, and had no established business relationship with the Company."[245] However, the TCPA includes a private right of action for individuals, businesses, and states to recover "actual monetary loss or $500 per violation, whichever is greater," and, for willful or knowing violations, three times those amounts.[246]

B. State Statutes of General Applicability

The states have enacted statutes aimed at privacy and consumer protection in a particularly wide variety of areas. The summary below touches on a few of the most prominent subjects of legislation, as well as some interesting outliers.

1. Disclosure of PII by Certain Non-Governmental Entities

(a) Consumer Credit Reporting Agencies

Some states have adopted laws analogous to the federal Fair Credit Reporting Act. For example, California's law requires the consumer credit reporting agencies, among other things, to block information that appears on a report as a result of identity theft, to place security alerts or freezes on a report when a consumer requests it, and to provide free copies of credit reports to victims of identity theft.[247] On the other hand, the statute expressly permits the consumer credit agencies to disclose public record information that they lawfully obtained from an open public record.[248]

(b) Financial Institutions

California's Financial Information Privacy Act prohibits financial institutions from selling or otherwise sharing nonpublic PII without the consumers' consent.[249] The law requires consumers to "opt in" to having their information shared with unaffiliated third parties, but requires them to "opt out" of sharing with the institution's affiliates, subject to a few exceptions.

(c) Insurance Companies

California's Insurance Information and Privacy Protection Act governs insurance companies' collection, use, and disclosure of PII in connection with insurance transactions. The law prohibits compa-

---

[245] *In Re* Worldwide Indus. Enters., Inc., FCC 15-6, File No. EB-TCD-12-00000254, Forfeiture Order (Jan. 26, 2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-6A1.pdf.

[246] 47 U.S.C. §§ 227(b)(3), (c)(5).

[247] CAL. CIV. CODE §§ 1785.1–36.

[248] *See Id.* at § 1785.11.2.

[249] CAL. FIN. CODE §§ 4050–4060.

nies from disclosing the information without written authorization from the individual, unless disclosure is "necessary for conducting business." The law requires the insurance company to give the individual the opportunity to opt out of disclosures made for marketing purposes.[250]

2. Use of Consumer PII for Marketing Purposes

California's "Shine the Light" statute gives consumers the right to know how their personal information is shared by companies (other than financial institutions, which are subject to the state's Financial Information Privacy Act) for marketing purposes.[251] The law "encourages"—but does not require—businesses to allow consumers to opt out of such sharing. California's Right of Publicity Statute prohibits the misappropriation of a person's name, photograph, likeness, and identity for use in paid advertisements without obtaining that person's consent.[252]

3. Data Disposal Requirements

A majority of states have passed laws requiring businesses (and, in some cases, government agencies) to ensure that consumers' PII is undecipherable when the entity disposes of both hard-copy and digital records.[253] California's law, for example, requires businesses to shred, erase, or modify the PII when disposing of consumer records under their control.[254]

4. Digital Assets After Death

A small number of states now have laws that cover what happens to a person's digital assets—from email and social media accounts to blogs and other websites—upon the person's death.[255] Most of those states provide for a representative of the decedent's estate to obtain access to the online accounts, subject to varying requirements.[256] In Nevada, however, the executor of the person's estate is only granted authority to terminate the accounts.[257]

---

250 *Privacy Laws*, OFFICE OF THE ATTORNEY GEN., STATE OF CAL. DEP'T OF JUSTICE, https://oag.ca.gov/privacy/privacy-laws.

251 CAL. CIV. CODE §§ 1798.83–1798.84.

252 *Id.* at § 3344.

253 *See Data Disposal Laws*, NAT'L CONFERENCE OF STATE LEGIS. (Jan. 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

254 CAL. CIV. CODE §§ 1798.80–81, 1798.84.

255 *Access to Digital Assets of Decedents*, NAT'L CONFERENCE OF STATE LEGIS. (Mar. 31, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/access-to-digital-assets-of-decedents.aspx.

256 *Id.*

257 NEV. REV. STAT. § 143.18.

5. Children's Online Privacy

Some states have enacted specialized statutes designed to protect the privacy of minors online. For example, California's Privacy Rights for California Minors in the Digital World Act allows minors to request and obtain the removal of content about them posted on a website or other online application.[258] The law also prohibits marketing products based on personal information specific to a minor.

6. Breach Notification and Data Security Laws

The vast majority of states (currently 47) have breach notification laws requiring notification to individuals (and in some cases, state regulators) where there is an unauthorized access or acquisition of the individual's PII.[259] In addition, a minority of states have also enacted state data security laws requiring companies to maintain data security safeguards to protect state residents' personal information from being compromised, which typically require companies to implement and maintain reasonable security measures.[260]

---

[258] *See* CAL. BUS. & PROF. CODE §§ 22580–22582.

[259] *See Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGIS. (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. The statutes typically define personal information triggering notification obligations as an individual's name in combination with: social security number; credit/debit card number; financial account number; driver's license or state-issued identification number; or, in some cases, medical/health insurance information.

[260] *See* Corey M. Dennis & David A. Goldman, *Data Security Laws and the Cybersecurity Debate*, 17 J. OF INTERNET LAW 1 (Aug. 2013), http://www.governo.com/News/News_News725_1.pdf. For a state-by-state breakdown of the requirements of these statutes, *see* Mintz Levin P.C., *State Data Security Breach Notification Laws* (April 16, 2016), https://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf.

SIDE BAR – GENERAL CONSUMER PROTECTION

There are many general consumer-related privacy laws (state and federal) that govern the collection, use, and disclosure of personal information, as well as marketing and communications to individuals. These include Section 5 of the FTC Act, COPPA, CAN-SPAM, the TCPA, and state laws.

Section 5 of the FTC Act prohibits "unfair and deceptive acts in or affecting commerce." This has been interpreted to include privacy-related misrepresentations (e.g., uses of personal information inconsistent with an organization's privacy policy) and security-related deficiencies (e.g., weak information security practices leading to a security breach).

The Telephone Consumer Protection Act (TCPA) and the Children's Online Privacy Protection Act (COPPA) are key federal privacy laws that organizations should be aware of. The TCPA generally requires prior express consent (and, in many cases, written consent) when calling landlines or cell phones (including text messages) for marketing purposes using an automatic telephone dialing system (or artificial/prerecorded voice); consent is also generally required for non-marketing calls/texts to cell phones. COPPA imposes restrictions and consent/notice requirements regarding the collection of personal information from children under the age of 13.

There are numerous state general consumer-related privacy laws. Chief among these laws are the state breach notification laws, which typically require notification to individuals (and, in some cases, regulators) in the event of an unauthorized access or acquisition of personal information.

V. HEALTH

A. HIPAA

1. Overview of HIPAA Privacy and Security Rules

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is one of the most prescriptive and comprehensive data privacy laws in the world. The HIPAA Privacy Rule ("Privacy Rule"), promulgated in 2000, generally prohibits the unauthorized disclosure of protected health information (PHI) by "covered entities," including health care providers, pharmacies, health insurers, HMOs, and health care clearinghouses.[261]

Covered entities must also require by contract any "business associates" (BA) to whom they disclose protected health information (e.g., third party administrators of health plans, medical billing and transcript companies, accounting firms providing services to health care providers, cloud service providers) to appropriately safeguard the information.[262] Such "business associate agreements" (BAAs) must include certain provisions, including a description of the permitted and impermissible uses of PHI, and a requirement that the BA use appropriate safeguards to prevent impermissible uses and disclosures of PHI.[263]

The HIPAA Security Rule ("Security Rule"), promulgated in 2003, requires covered entities to maintain certain safeguards for the protection of electronic health information, which must be documented in written policies and procedures.[264] The Security Rule also imposes other obligations, including training employees and conducting a thorough "risk analysis" to prevent security violations.[265] HIPAA generally preempts contrary state laws, with few exceptions, such as where the requirements of the state law are more stringent than those under HIPAA.[266]

---

261 *See* 45 C.F.R. § 164.500 *et seq*. "Hybrid entities"—i.e., those that conduct both covered and non-covered functions, such as companies with fully self-insured health plans—may designate the covered components of their organizations to segregate covered from non-covered functions. *See id.* at § 164.103.

262 *See id.* at §§ 160.103, 164.502(e). A "business associate" is defined as a "person" who: (1) on behalf of a covered entity, "creates, receives, maintains, or transmits" PHI for a "function or activity" regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, certain patient safety activities, billing, benefit management, practice management, and repricing; or (2) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity where the services provided involve the disclosure of PHI from such covered entity, or from another BA of such covered entity. *See id.* at § 160.103.

263 *See id.* at § 164.504.

264 *See id.* at §§ 164.302 *et seq*.

265 *See id.* at § 164.308(a).

266 *See id.* at § 160.203.

2. Protected Health Information and the De-Identification Standard

PHI under HIPAA is broadly defined to include "individually identifiable information," including demographic information: (1) that is "created or received" by a HIPAA Covered Entity; and (2) relates to the past, present, or future physical or mental health or condition of an individual, or the provision or payment for such health care; and (3) that identifies the individual, or for which there is a reasonable basis to belief can be used to identify the individual.[267] However, the Privacy Rule does not restrict the use or disclosure of "de-identified health information," which neither identifies, nor provides a reasonable basis to identify, an individual.[268]

There are two methods for de-identification under HIPAA:

1) *The Safe Harbor Method*—removal of all 18 HIPAA identifiers, including: (a) names/initials; (b) all dates directly related to the individual (e.g., DOB, admission date); (c) medical record numbers; (d) ages over 89 (must be grouped into 90+); (d) telephone numbers and email addresses; or (e) any unique identifying number (e.g., hospital number), characteristic (e.g., "CEO"), or code (if derived from PHI)

2) *The Expert Determination Method*—based upon a statistical analysis by a recognized expert, to ensure there is a "very small" risk of re-identification[269]

3. Uses and Disclosures of PHI

The basic principle of the Privacy Rule is that a covered entity may not use or disclose PHI, except either (1) as the Privacy Rule permits or requires, or (2) as the individual or the individual's personal representative permits pursuant to a written authorization. Under the Privacy Rule, a valid authorization must contain:

1) a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

2) the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

3) the name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;

4) a description of each purpose of the requested use or disclosure;

---

[267] *See id.* at § 160.103.

[268] *See id.* at §§ 164.502(d), 164.514.

[269] *See id.* at § 164.514.

5) an expiration date/event ("none" or similar language is sufficient if the disclosure is for research);

6) signature of the individual (or personal representative) and date; and

7) statements regarding: (a) the individual's right to revoke the authorization (including to revoke the authorization and exceptions to the right to revoke); (b) the potential for information disclosed to be subject to re-disclosure and no longer subject to the Privacy Rule; and (c) the ability or inability to condition treatment, payment, enrollment, or eligibility for benefits (i.e., stating that the covered entity may not do so, or the consequences if the individual refuses to sign when the covered entity may do so).

The authorization must also be written in plain language, and a copy must be provided to the individual. The authorization requirements under HIPAA differ from the elements of informed consent under the FDA regulations governing clinical trials, which include additional requirements (e.g., a statement that the study involves research, and an explanation of the research purpose, procedures to be followed, risks and benefits of the study, the extent confidentiality of records will be maintained).

A covered entity is required to disclose PHI in only two situations: (1) to individuals or their representatives when they request access to PHI or an accounting of disclosures of PHI; and (2) to HHS when it is undertaking a compliance investigation, review, or enforcement action.

The "minimum necessary" requirement is a key principle of the Privacy Rule. Under this principle, a covered entity must implement policies and procedures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. This includes implementing policies and procedures that restrict access to PHI based on specific roles of members of their workforce (i.e., access should be limited only to those who need access to fulfill their job duties), as well as policies and procedures limiting PHI disclosed for routine/recurring disclosures.

(a) Permitted Uses and Disclosures

The Privacy Rule sets forth a number of exceptions to the general rule requiring an authorization for disclosures of PHI, which are described below. A covered entity is permitted to use and disclose PHI, without an individual's authorization:

1) to the individual;

2) for treatment, payment, or health care operations;

3) for certain uses and disclosures where the individual has an opportunity to agree or object (e.g., for healthcare facility directors or to an individual's family or friends);

4) for incidental uses or disclosures that are otherwise permitted by the Privacy Rule (e.g., a hospital visitor overhears a provider's confidential conversation with another provider or patient), provided that the covered entity has complied with the "minimum necessary rule";

5) for public health activities;

6) in certain circumstances (e.g., victims of abuse, neglect, or domestic violence);

7) for health oversight activities (e.g., audits and investigations necessary for oversight of healthcare systems and government benefit programs);

8) in judicial and administrative proceedings (if ordered by a court or administrative tribunal);

9) for law enforcement purposes;

10) to decedents (e.g., to funeral directors, coroners, medical examiners in certain circumstances);

11) to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue;

12) where necessary to prevent a serious threat to health or safety;

13) for essential government functions (e.g., assuring proper execution of military mission, conducting authorized intelligence and national security activities, protecting the health and safety of inmates or employees of correctional institutions, determining eligibility for certain government benefit programs); and

14) as authorized by, and to comply with, workers' compensation laws and similar programs.

(b) Research

The rules regarding disclosure of PHI for research purposes under HIPAA seek to balance the rights of privacy and confidentiality in research subjects' personal information with the public policy in favor of public health and developing life-saving treatments. Clinical research is not only vital to achieving these goals, but is also required for the development of pharmaceutical drugs and devices.

Research under the Privacy Rule is defined as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." In general, the Privacy Rule requires that a covered entity obtain an individual's authorization before using and disclosing PHI for research purposes. However, there are several exceptions to this rule:

1) Institutional Review Board (IRB) waiver—An IRB or Privacy Board may grant a waiver of authorization where research cannot practicably be conducted without the disclosure of PHI and there is minimal privacy risk.

2) Preparatory to Research—PHI may be disclosed if the researcher represents that the use of PHI is necessary (and solely) for purposes preparatory to research (e.g., research study/protocol design or feasibility), and that the PHI will not be "removed" from the covered entity.

3) Limited Data Set—A researcher may access a "limited data set," which includes indirect identifiers (e.g., DOB, dates of treatment, city), but excludes direct identifiers (e.g., name, address, phone number) where the researcher and covered entity execute a "data use agreement."

4) Research on Decedents—PHI of decedents may be disclosed where the researcher represents (written or orally) that the use is necessary (and solely) for the research and provides documentation of the subject's death.

5) Limited Data Set with a Data Use Agreement—A covered entity may disclose a limited data set to the researcher for research, public health, or health care operations pursuant to a data use agreement.

The Privacy Rule generally requires an individual's written authorization before a use or disclosure of protected health information can be made for "marketing," which is defined as making "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." However, there are several exceptions to this rule:

1) Communications made to describe a health-related product or service that is provided by a covered entity or its plan of benefits (e.g., the entities participating in a healthcare provider network, enhancements to a health plan)

2) Communications made for the treatment of the individual (e.g., pharmacy prescription refill reminders or primary care physician referrals to a specialist)

3) Communications made for case management or care coordination (e.g., recommending alternative treatments or healthcare providers)

In addition, face-to-face-marketing communications or communications regarding a promotional gift of nominal value from the covered entity do not require an authorization.

4. Notice of Privacy Practices

Covered health plans and healthcare providers must generally provide a notice of privacy practices (NPP) to all individuals of the use or disclosure of their PHI, which must describe the ways in which the PHI may be used and disclosed, state the covered entity's duties to protect privacy and abide by

the NPP, describe the individuals' rights (e.g., to the covered entity or to HHS), and include a point of contact for further information and for making complaints.[270]

The NPP must be made available to any individual who requests it and prominently posted on any website providing information about its customer services or benefits. Health plans must also provide the notice to all new enrollees at the time of enrollment and provide a revised notice to individuals within 60 days of a material revision, while healthcare providers must generally provide the notice to the individual on the first date of service and obtain a written acknowledgement from patients of receipt of the NPP.[271]

5. Rights of Access, Amendment, and Disclosure Accounting

Individuals generally have a right to access and obtain a copy of their PHI in a covered entity's designated record set.[272] Excluded from the right to access are psychotherapy notes and information compiled for legal proceedings.[273] Individuals also have a right to have their PHI amended if it is inaccurate or incomplete.[274]

In addition, individuals have a right to an accounting of the disclosure of their PHI to a covered entity's business associates made in the preceding six years. However, no accounting is required:

a) for treatment, payment, or health care operations;

b) to the individual or the individual's personal representative;

c) for notification to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories;

d) pursuant to an authorization;

e) of a limited data set;

f) for national security or intelligence purposes;

g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or

---

[270] *See id.* at § 164.520.

[271] *See id.* at § 164.520.

[272] *See id.* at § 164.524(a). "Designated record set" is defined as the group of records maintained by the covered entity that is: (1) medical records and billing records about the individuals; (2) used (in whole or in part) to make decisions about individuals; or (3) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by a health plan. *See id.* at § 164.520.

[273] *See id.* at § 164.524(a).

[274] *See id.* at § 164.526.

h) incident to otherwise permitted or required uses or disclosures.[275]

6. Administrative Requirements

The Privacy Rule sets forth a number of administrative requirements, including:

1) developing and implementing written policies and procedures in compliance with the requirements of the Privacy Rule;

2) designating a "privacy official" (Privacy Officer) who is responsible for developing and implementing policies and procedures, and a contact person/office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices;

3) applying sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule;

4) mitigating any harmful effect that may be caused by an improper use or disclosure of PHI;

5) maintaining reasonable and appropriate administrative, technical, and physical safeguards to prevent improper uses and disclosures of PHI (e.g., shredding documents with PHI before discarding them);

6) maintaining procedures for individuals to complain about its compliance with policies and procedures or the Privacy Rule;

7) banning retaliation against any person who exercises rights provided by the Privacy Rule, and prohibiting a waiver of an individual's rights under the Privacy Rule as a condition of obtaining treatment, payment, and enrollment or benefits eligibility;

8) maintaining, until the later of six years after its creation or last effective date, its privacy policies and procedures, NPP, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.[276]

---

[275] *See id.* at § 164.528.

[276] *See id.* at § 164.530. Fully-insured group health plans that do not create or receive PHI, with the exception of enrollment data and "summary health information" (as defined under 45 C.F.R. §164.504(a)) are only subject to the following administrative requirements: (1) ban on retaliatory acts and waiver of individual rights; and (2) health plan documentation requirements if plan documents are amended to allow disclosure of PHI by an insurance company to the plan sponsor. *See id.* at § 164.530(k).

The Security Rule also sets forth numerous administrative, technical, and physical safeguards with which covered entities and business associates must comply.[277] However, those requirements are beyond the scope of this primer, which focuses on privacy, rather than security laws.

7. Breach Notification Under the Health Information Technology for Economic and Clinical Health (HITECH) Act

In January 2013, HHS issued the final omnibus HIPAA/HITECH rule, which makes important changes to the privacy and security requirements under HIPAA and the HITECH Act. Some of the more significant changes include:

1) HIPAA violation liability is extended to business associates to whom protected health information is disclosed;

2) "business associate" is now more broadly defined to include subcontractors of business associates (thus, business associates themselves must obtain business associate agreements from their subcontractors);

3) the threshold for reporting breaches has been reduced such that more breaches may be reported—an impermissible use/disclosure is now presumed to be a breach unless it is shown, based upon a risk assessment, that there is a low probability of PHI being compromised; and

4) non-compliance penalties are increased based on the level of negligence, with a maximum penalty of $1.5 million per violation (for cases involving willful negligence).[278]

The HITECH Act's breach notification regulations require HIPAA covered entities to report data breaches affecting 500 or more individuals to the affected individuals, to HHS, and to "prominent media outlets serving a State or jurisdiction." Breaches affecting fewer than 500 individuals must be reported to HHS annually. In addition, business associates must notify covered entities of any breaches.[279]

8. Audits

In 2011, HHS began an audit program to evaluate organizations' HIPAA compliance with the HIPAA Privacy, Security, and Breach Notification Rules. The results of Phase 1 of the audits re-

---

[277] *See id.* at § 164.302.

[278] *See id.* at §§ 164.400 *et seq.*; 42 U.S.C. §§ 17931 *et seq.*; 42 U.S.C. § 1320d-5.

[279] *See id.* at §§ 164.404 *et seq.*

vealed that the vast majority of covered entities failed to comply with mandatory HIPAA requirements, and that the most common cause of non-compliance was a fundamental lack of awareness of those requirements.[280]

HHS Office of Civil Rights (OCR) Senior Adviser Linda Sanches explained that "security was overwhelmingly an area of concern," noting that most of the healthcare providers had not done a complete and accurate risk assessment.[281] The negative findings were forwarded to OCR investigators for consideration. The OCR has now begun Phase 2 of the audits, which focuses on both covered entities and business associates.

9. Enforcement

Since the HITECH Act became effective, HHS has substantially increased its enforcement efforts relating to HIPAA. In 2013, former OCR Director Leon Rodriguez noted that the OCR would "vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates."[282] And in February 2015, the OCR noted that it will continue to "aggressively enforce" these rules.[283] Examples of recent investigations and fines include the following:

- In March 2016, the Feinstein Institute for Medical Research agreed to pay $3.9 million to settle potential HIPAA violations following an incident in which an unencrypted laptop containing PHI of 13,000 patients and research participants was stolen from an employee's car; the OCR found that Feinstein's HIPAA policies, procedures, and processes were non-compliant and insufficient to address privacy and security risks relating to that information.[284]

- In March 2016, North Memorial Health Care of Minnesota settled potential HIPAA violations for $1.55 million based on allegations that it failed to enter

---

[280] *See* Linda Sanches, *HIPAA Privacy, Security and Breach Notification Audits: Program Overview & Initial Analysis*, HCCA 2013 COMPLIANCE INSTITUTE (Apr. 23, 2013), http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/Tuesday/500/504print1.pdf.

[281] Joe Carlson, *Audits find organizations unaware of new data, privacy rules*, MODERN HEALTHCARE (April 23, 2013), http://www.modernhealthcare.com/article/20130423/NEWS/304239958.

[282] *See New Rule Protects Patient Privacy, Secures Health Information*, DEP'T OF HEALTH & HUMAN SERVS. (Jan. 17, 2013), http://www.hhs.gov/news/press/2013pres/01/20130117b.html.

[283] *See* OFFICE FOR CIV. RIGHTS, DEP'T OF HEALTH & HUMAN SERVS., OCR FISCAL YEAR 2016 CONGRESSIONAL JUSTIFICATION (Feb. 2, 2015), http://www.hhs.gov/sites/default/files/budget/office-of-civil-rights-budget-justification-2016.pdf.

[284] *See Improper disclosure of research participants' protected health information results in $3.9 million HIPAA settlement*, DEP'T OF HEALTH & HUMAN SERVS. (Mar. 17, 2016), http://www.hhs.gov/about/news/2016/03/17/improper-disclosure-research-participants-protected-health-information-results-in-hipaa-settlement.html.

into a BAA with a major contractor and failed to conduct an organization-wide risk analysis and management plan as required by HIPAA.[285]

- In November 2015, Triple-S Management Corporation (an insurance company, formerly known as American Health Medicare Inc.) agreed to a $3.5 million HIPAA settlement. Following multiple breach notifications involving PHI, the OCR found widespread non-compliance with the Privacy and Security Rules, including failure to develop appropriate policies and procedures, implement necessary technical safeguards, conduct a risk analysis, and implement required training.[286]

Other recent breaches include the following:

- In August 2015, an oncology practice agreed to pay $750,000 following a breach involving the theft of unencrypted backup media where the OCR's investigation revealed widespread non-compliance with the Security Rule, including failure to conduct a risk analysis or to have a policy in place regarding removal of electronic media containing PHI.[287]

- In February 2015, health insurer Anthem suffered a breach involving 80 million current and former members, the largest ever disclosed by a healthcare company, which affected customers of all products lines, including Anthem Blue Cross, and Anthem Blue Cross and Blue Shield. The breach prompted a multi-state insurance regulator investigation and more than 50 putative class action lawsuits.[288]

- In May 2014, New York and Presbyterian Hospital and Columbia University agreed to pay $4.8 million to settle potential HIPAA violations following a breach resulting in the disclosure of the electronic personal health information of

---

285 *See $1.55 million settlement underscores the importance of executing HIPAA business associate agreements*, DEP'T OF HEALTH & HUMAN SERVS. (Mar. 16, 2016), http://www.hhs.gov/about/news/2016/03/16/155-million-settlement-underscores-importance-executing-hipaa-business-associate-agreements.html.

286 *See Triple-S Management Corporation Settles HHS Charges by Agreeing to $3.5 Million HIPAA Settlement*, DEP'T OF HEALTH & HUMAN SERVS. (Nov. 30, 2015), http://www.hhs.gov/about/news/2015/11/30/triple-s-management-corporation-settles-hhs-charges.html#.

287 *See $750,000 HIPAA settlement emphasizes the importance of risk analysis and device and media control policies*, DEP'T OF HEALTH & HUMAN SERVS. (Sept. 2, 2015), http://www.hhs.gov/news/press/2015pres/09/20150902a.html.

288 *See* Joseph Conn, *Legal liabilities in recent data breach extend far beyond Anthem*, MODERN HEALTHCARE (Feb. 23, 2015), http://www.modernhealthcare.com/article/20150223/NEWS/302239977/legal-liabilities-in-recent-data-breach-extend-far-beyond-anthem; Anna Wilde Mathews, *Insurance Regulators to Investigate Recent Data Breach at Anthem*, WALL ST. J. (Feb. 6, 2015), http://www.wsj.com/articles/insurance-regulators-to-investigate-recent-data-breach-at-anthem-1423268574.

6,800 individuals, including patient status, vital signs, medications, and laboratory results.[289]

In addition, it should be noted that although most private lawsuits based upon data breaches have been dismissed in the past, recent decisions ruling in favor of plaintiffs—including a Connecticut Supreme Court decision that could give rise to negligence liability based upon HIPAA violations[290]—may lead to an increase in litigation and more difficulty for defendants facing such cases.[291]

B. State Laws on Privacy of Health Information

While a review of all 50 states' health privacy laws is beyond the scope of this Primer, the following discussion highlights a handful of state statutes that build on the federal framework, whether by permitting private enforcement or by broadening the scope of statutory protections.

1. Alaska's Genetic Privacy Act

Alaska's Genetic Privacy Act ("Alaska law"), Alaska Stat. §§ 18.13.010–100, treats genetic information, including DNA samples, as the private property of the individual. As such, the statute provides that DNA samples cannot be collected, analyzed, or disclosed without an individual's informed consent. The statute was enacted to "curtain exploitation of [citizens'] valuable genetic information" and to afford Alaskans "the right to keep their genetic information private."[292]

(a) Specific Provisions

The Alaska law makes it illegal for anyone to "collect a DNA sample from a person, perform a DNA analysis on a sample, retain a DNA sample or the results of a DNA analysis, or disclose the results of a DNA analysis" without first obtaining that person's informed consent.[293] The Alaska law

---

289 *See Data breach results in $4.8 million HIPAA settlements*, DEP'T OF HEALTH & HUMAN SERVS. (May 7, 2014), http://www.hhs.gov/news/press/2014pres/05/20140507b.html.

290 *See* Byrne v. Avery Ctr. for Obstetrics and Gynecology, P.C., 314 Conn. 433, 436, 102 A.3d 32, 36 (Conn. 2014) (holding "HIPAA may inform the applicable standard of care" in negligence case against physician involving improper disclosure of records).

291 *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 694–96 (7th Cir. 2015) (holding plaintiff's lost time and money resolving fraudulent charges and protecting themselves against future identity theft by purchasing credit monetary conferred adequate Article III standing); Resnick v. AvMed, Inc., 693 F.3d 1317, 1330 (11th Cir. 2012) (holding plaintiffs' allegations of injury and causation were sufficient to withstand a motion to dismiss where they suffered identity theft due to a data breach affecting their health insurer; case later settled for $3M); *cf.* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. Aug. 24, 2015) (upholding FTC's authority to regulate and enforce in the area of data security following data security breach affecting Wyndham hotels' customers).

292 SB 217, 2004 Alaska Legis. Comm. Minutes 1539.

293 ALASKA STAT. § 18.13.010(a)(1).

specifies that both the DNA sample and the results of any analysis of the sample are the exclusive property of the "person sampled or analyzed."[294]

The Alaska law defines "DNA analysis" to mean "DNA or genetic typing and testing to determine the presence or absence of genetic characteristics in an individual," and further defines "genetic characteristics" to include "a gene, chromosome, or alteration of a gene or chromosome that may be tested to determine the risk of a disease, disorder, trait, propensity, or syndrome, or to identify an individual or a blood relative."[295]

The Alaska law contains a number of exclusions that narrow its otherwise sweeping scope. The statute expressly defines "DNA analysis" to exclude "routine physical measurement, a test for drugs, alcohol, cholesterol, or [HIV], a chemical, blood or urine analysis, or *any other diagnostic test that is widely accepted and in use in clinical practice*."[296] Thus, the law arguably has no application to routine tests a person could obtain at most doctors' offices. The statute also exempts five categories of activities, specifying that its prohibitions do not apply to genetic testing for purposes of:

- criminal identifications pursuant to any jurisdiction's DNA registration system;
- law enforcement, including the identification of both victims and perpetrators;
- paternity testing;
- screening of newborns as required by law; or
- emergency medical treatment.[297]

The Alaska law makes clear that a "general authorization for the release of medical records or medical information" does not count as the necessary informed consent to release the genetic information the law protects.[298] The law also expressly permits a person, at any time, to revoke or amend their informed consent to analysis or disclosure of genetic information.[299]

---

294 *Id.* at § 18.13.010(a)(2).

295 *Id.* at §§ 18.13.100(2)–(3).

296 *Id.* at § 18.13.100(2) (emphasis added).

297 *Id.* at § 18.13.10(b).

298 The law contemplates that the Alaska Department of Health and Social Services may adopt a uniform informed and written consent form, the use of which would immunize a person from civil or criminal liability under the statute. ALASKA STAT. § 18.13.10(c). However, as of the date of this publication, no such regulation has been adopted.

299 *Id.* at § 18.13.10(c).

(b) Enforcement

In Alaska, unlawful DNA collection, analysis, retention or disclosure is a class A misdemeanor punishable by up to one year in jail and a fine of up to $10,000.[300] The statute specifies that a person is criminally liable only if he or she acts "knowingly," which need not include any intention to violate the law. Rather, under Alaska law, a person acts "knowingly" if he or she is aware that the circumstance making the conduct unlawful exists, or if she or she is aware of a substantial probability that the circumstance exists.[301]

The Alaska law also creates a private right of action for anyone whose genetic information is collected, analyzed, retained, or disclosed in violation of the statute. The statute provides for statutory damages of $5,000, in addition to any actual damages suffered by the person whose genetic information was misused. If the violator profited from the violation, the statutory damages increase to $100,000.

Although the statute has been on the books for more than a decade, it appears to have been invoked only rarely. In 2014, a plaintiff named Michael Cole filed a putative class action lawsuit in Alaska against Gene by Gene, Ltd., a Texas company doing business as "Family Tree DNA."[302] According to the complaint, Family Tree DNA is a commercial genetic testing company that sells DNA tests to consumers for the purpose of helping them to research and identify their ancestry.[303] Cole alleges that Family Tree ships DNA collection kits to consumers, who collect cotton swab samples and return them to the company for analysis. When the analysis is complete, Family Tree invites the customer to sign in to the Family Tree database to search for "matches" based on the customer's DNA sequence, and, if a match is found, Family Tree encourages the customer to "join" a "project," or a forum for individuals conducting ancestral research.[304] According to Cole, even though Family Tree never seeks or obtains the customer's consent to disclose the results of his or her DNA analysis with third persons, "when customers join certain 'projects,' Family Tree automatically publishes the full results of their DNA tests to its publicly available websites."[305] Cole alleges that his DNA test results were made publicly available on the Internet and that his full name, email address, and unique DNA kit number were also disclosed to a separate ancestry research company, RootsWeb.[306] On his own

---

[300] *Id.* at § 18.13.030(c); *see also id.* at §§ 12.55.035, 12.55.135.

[301] *Id.* at § 11.81.900(a)(2).

[302] Cole v. Gene by Gene, Ltd., Case No. 14-cv-00004, Dkt. No. 1 (D. Alaska May 13, 2014). One of the lawyers representing Cole, Jay Edelson, is the immediate past Co-Chair of Working Group 11 and a contributor to this publication.

[303] *Id.* at ¶ 1.

[304] *Id.* ¶¶ 1–2, 20–23.

[305] *Id.* ¶¶ 24–26, 32.

[306] *Id.* ¶ 32. In its Answer, Family Tree DNA states that the "projects" are administered by non-employee volunteers who are "genealogy enthusiasts." *See Cole*, Case No. 14-cv-00004, Dkt. No. 20 at 6, 8. Family Tree DNA asserts that such a volunteer was responsible for posting Cole's information on RootsWeb. *Id.* at 8. Family Tree DNA also states

behalf and on behalf of a class of similarly situated individuals, Cole seeks injunctive relief, actual and statutory damages, and an award of attorneys' fees. The complaint alleges that the total damages exceed $5,000,000.[307]

As of the date of this publication, the *Cole* case is still in the discovery phase. Because Family Tree did not move to dismiss the complaint, the court's first opportunity to evaluate the viability of the claim will be when Cole moves for class certification.

2. California Confidentiality of Medical Information Act

The California Confidentiality of Medical Information Act (CMIA), California Civil Code § 56 *et seq.,* includes extensive provisions governing how and when medical information may be disclosed by health care providers and certain other entities in California.

(a) Specific Provisions

The CMIA broadly defines "Medical Information" to include any "individually identifiable information" about "a patient's medical history, mental or physical condition, or treatment," in any format that is possessed by or "derived from" certain health-related entities.[308] "Individually identifiable" is defined equally broadly, to mean that the information includes "any element of personal identifying information" that would make it possible to identify the individual. In addition to PII like name, address, electronic mail address, telephone number, and social security number, the statute expressly includes "other information that, alone *or in combination with other publicly available information*, reveals the individual's identity."[309]

The CMIA prohibits health care providers from disclosing their patients' medical information without prior authorization, except as provided by statute.[310] The latter caveat is fairly broad, however. The statute expressly *requires* disclosure in a number of situations, including when compelled by a court order, subpoena, or search warrant, or pursuant to a patient's request for inspection pursuant to California's Patient Access to Health Records statute.[311] The CMIA also permits disclosure in a wide variety of circumstances, including, among other things:

- to other health care professionals for purposes of diagnosis or treatment of the patient, including via radio transmissions in emergency situations;

---

that Cole signed a release, which directed him to the company's privacy policy, which notified him that his information would be made available to the "volunteer project administrator." *Id.*

307 *Cole*, Case No. 14-cv-00004, Dkt. No. 1 at ¶¶ 7, 34, 49.

308 CAL. CIV. CODE § 56.05(j). The statute applies to information possessed by or derived from "a provider of health care, health care service plan, pharmaceutical company, or contractor."

309 *Id.* (emphasis added).

310 *Id.* at §§ 56.10(a), (d), (e).

311 *Id.* at §§ 56.10(b)(1)–(9).

- to an insurer, employee benefit plan, governmental authority, or other entity responsible for paying for health care services rendered to the patient, as needed to establish responsibility for payment;
- to a person or entity that provides billing, claims management, medical data processing, or other administrative services for health care providers;
- to agents of professional societies, professional standards review organizations and the like, if they are reviewing the competence or qualifications of the health care provider;
- to a private or public body responsible for licensing or accrediting the health care provider or service plan;
- to public agencies, clinical investigators, and accredited educational institutions for bona fide research purposes;
- to an organ procurement organization or tissue bank for the purpose of aiding in the transplantation of tissue into the body of another person;
- to a third party "for purposes of encoding, encrypting, or otherwise anonymizing data"; and
- to a local health department for the purpose of preventing or controlling disease, injury, or disability.[312]

The CMIA also expressly permits a psychotherapist to disclose information if he or she believes, in good faith, that "disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a reasonably foreseeable victim or victims, and the disclosure is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat."[313] The CMIA specifies that the recipient of a permitted disclosure may not further disclose the information in violation of the statute.[314] The CMIA also requires health care providers and other covered entities that create, maintain, preserve, store, abandon, destroy, or dispose of medical records to do so in a manner that preserves the confidentiality of the information contained within those records.[315]

The CMIA spells out exactly what is necessary for an authorization of disclosure to be valid, including that the signature executing the authorization must serve no other purpose than to execute the

---

[312] *Id.* at §§ 56.10(c)(1)–(22).

[313] *Id.* at § 56.10(c)(19).

[314] *Id.* at § 56.13.

[315] *Id.* at § 56.101(a).

authorization, and that the authorization must include an expiration date.[316] The CMIA also gives patients the right to cancel or revoke their authorization at any time, so long as the provider actually receives the written revocation.[317]

(b) Enforcement

A violation of the CMIA constitutes a misdemeanor if it causes economic loss or personal injury to a patient.[318] In California, misdemeanors are punishable by probation, jail time, fines, community service, or a combination. The CMIA also creates a private right of action against any person or entity that violates the statute by negligently releasing the plaintiff's confidential information or records.[319] If the plaintiff suffered economic loss or personal injury, he or she can recover actual damages, if any, and punitive damages up to $3,000; attorneys' fees up to $1,000; and the costs of litigation.[320] The CMIA also provides for statutory damages of $1,000, which do not require proof that the plaintiff suffered actual damages[321] unless the defendant establishes the affirmative defense added to the act effective January 1, 2013.[322]

The affirmative defense applies if a covered entity or business associate released confidential information solely to another covered entity or business associate, and all of the following are true:

- the defendant complied with any obligation to notify affected individuals;
- the disclosure was not in connection with medical identity theft;
- the defendant took appropriate preventive actions to protect the information and records under both HIPAA and applicable state laws, including, among other things, using encryption;
- the defendant took appropriate corrective action after the disclosure, including measures to prevent similar occurrences in the future; and
- the recipient did not use or release the information or records and returned or destroyed the material promptly.[323]

---

316 *Id.* at § 56.11.

317 *Id.* at § 56.15.

318 *Id.* at § 56.36(a).

319 *Id.* at § 56.36(b).

320 *Id.* at § 56.35; *see also id.* at §§ 56.36(b), (e).

321 *Id.* at § 56.36(b)(1).

322 *Id.* at § 56.36(e).

323 *Id.* at §§ 56.36(e)(2)(A)–(H).

In general, a defendant may only take advantage of the affirmative defense once, unless the court determines that the justification for the defense is "compelling" and applying it would promote reasonable conduct consistent with the CMIA.[324] The CMIA also explicitly instructs courts to consider the equities of the situation when deciding whether to apply the affirmative defense.[325]

The CMIA also provides for administrative fines and civil penalties in varying amounts for certain violations,[326] which may be imposed by the State Department of Public Health, a licensing agency, a certifying board, or a court.[327] Only specified public officials, including the state attorney general, any district attorney, and certain city attorneys, may bring a civil action, in the name of the people of the State of California, seeking civil penalties.[328]

A person who negligently discloses information in violation of the statute faces a fine or penalty of up to $2,500 per violation, irrespective of whether the violation caused any actual damages.[329] Anyone other than a licensed health care professional who knowingly or willfully obtains, discloses, or uses medical information in violation of the statute is liable for up to $25,000 per violation.[330] If the violation was for the purpose of financial gain, the fine or penalty may be up to $250,000 per violation, as well as disgorgement of the ill-gotten gains.[331]

A licensed health care professional who knowingly and willfully obtains, discloses, or uses medical information in violation of the law is subject to fines or penalties of up to $2,500 for the first violation, $10,000 for the second violation, and $25,000 for a third or subsequent violation. If the violation was for the purpose of financial gain, the fines or penalties grow to $5,000 for a first violation, $25,000 for the second one, and $250,000 for a third or subsequent violation, as well as disgorgement.[332]

A handful of recent cases applying and interpreting the CMIA have emphasized the statute's focus on preserving the confidentiality of information. For example, in *Regents of the Univ. of Cal. v. Super. Ct.*,[333] the California Court of Appeals concluded that negligently maintaining or storing medical in-

---

[324] *Id.* at § 56.36(e)(2)(I).

[325] *Id.* at § 56.36(e)(3).

[326] *Id.* at §§ 56.36(c)–(d).

[327] *Id.* at § 56.36(d).

[328] *Id.* at § 56.36(f).

[329] *Id.* at § 56.36(c).

[330] *Id.*

[331] *Id.* at § 56.36(c)(3)(A). The penalty similarly rises to $250,000 per violation if the person was not permitted under the statute to receive medical information.

[332] *Id.* at § 56.36(c)(3)(B).

[333] 220 Cal. App. 4th 549 (2013).

formation, by itself, did not give rise to a cause of action under the CMIA. The court held that plaintiffs must plead that their information was in fact improperly viewed or accessed by an unauthorized person, and not just lost, in order to support a claim under the CMIA.

Similarly, *Sutter Health v. Super. Ct.*,[334] arose from the theft of a health care provider's computer, which contained the medical records of some four million patients. The plaintiffs brought the case on behalf of themselves and a putative class of all of the affected individuals, and sought an award of as much as $4 billion. After the trial court refused to dismiss the complaint, the defendant appealed. A unanimous panel of the court of appeals held that the plaintiffs had failed to state a claim under the CMIA because they did not allege that any unauthorized person actually viewed the stolen medical information. In so ruling, the court reasoned that the focus of the CMIA is on "preserving the confidentiality of the medical information, not necessarily preventing others from gaining possession of the paper-based or electronic information itself." Therefore, the court held, a breach of confidentiality is a necessary element of a claim under the CMIA. Since no breach of confidentiality takes place "until an unauthorized person views the medical information," the failure to plead such unauthorized access was fatal to the plaintiffs' claim.

3. Texas Medical Records Privacy Act

The Texas Medical Records Privacy Act ("Texas law"), Tex. Health & Safety Code Ann. § 181.001 *et seq.*, which became effective on September 1, 2012, builds on HIPAA to provide even more comprehensive protection of medical information.

(a) Specific Requirements

The Texas law broadens HIPAA's definition of "covered entity" to include *any* person who "comes into possession" of PHI.[335] The statute expressly includes anyone who assembles, collects, analyzes, uses, evaluates, obtains, stores, or transmits PHI, whether that person is a health care provider, business associate, governmental unit, or other entity.[336] The statute also makes explicit that employees, agents, or contractors of anyone falling within the definition of a "covered entity" are also "covered."[337] However, the Texas law exempts employee benefit plans, workers' compensation programs, and the American Red Cross, among other entities, from the statute's reach.[338]

---

334 Case No. C072591 (Cal. Ct. App. July 21, 2014).

335 TEX. HEALTH & SAFETY CODE ANN. § 181.001(b)(2)(B).

336 *Id.* at § 181.001(b)(2).

337 *Id.* at § 181.001(b)(2)(D).

338 *See generally id.* at §§ 181.052–059. The act exempts insurers and employers from some provisions, but not from the statute's prohibitions on re-identification; disclosure or use of PHI for marketing purposes without prior authorization; and sale of PHI. *Id.* at § 181.051. Insurers and employers are also subject to the notice requirement in § 181.154 of the Act.

Among other affirmative requirements, the Texas law mandates training for a covered entity's employees as to state and federal law concerning PHI, as necessary and appropriate for the employee to perform his or her job.[339] Such training must be provided within 90 days of the employee's date of hire. The statute further requires employees to stay current: if the employee's job duties are affected by a material change in the law regarding PHI, the employee must have additional training within one year after the material change in law takes effect. Employers must also obtain a signed statement verifying the employee's completion of the training and retain it for six years.

The Texas law also provides for consumers' right to access their own medical records upon request. With limited exceptions, if a health care provider is using an electronic system capable of fulfilling the request, the provider must provide requested records to the patient, in electronic form, within 15 days of receiving the request.[340]

The statute charges the state attorney general with the duty of monitoring compliance with the law and reporting annually to the legislature about consumer complaints under the Texas law. The Texas law expressly prohibits the re-identification (or attempted re-identification), without prior consent, of an individual who is the subject of any PHI.[341]

In general, before PHI may be disclosed or used for marketing purposes, a covered entity must first obtain "clear and unambiguous permission" from the individual.[342] This requirement does not apply if the marketing communication is (1) in a face-to-face conversation, (2) a promotional gift of nominal value provided by the covered entity, (3) necessary for administration of a patient assistance program or other prescription drug savings or discount program, or (4) made at the clear and unambiguous oral request of the individual.[343] Marketing communications sent through the mail (1) must be placed in an envelope showing only the names and addresses of the sender and recipient, (2) must state the name and toll-free number of the entity sending the materials, (3) must explain the recipient's right to be removed from the mailing list, and (4) if the recipient so requests, the entity must remove the person's name within 45 days of receiving the request.[344]

The Texas law broadly prohibits the sale of PHI. The only exceptions to the prohibition on receiving direct or indirect remuneration in exchange of a disclosure of PHI are that a covered entity may disclosed PHI to another covered entity for the purposes of treatment, payment, health care operations, certain insurance functions defined by statute, or as otherwise authorized or required by state or federal law.[345] A covered entity that discloses information pursuant to these exceptions may not

---

339 *Id.* at § 181.101.

340 *Id.* at § 181.102.

341 *Id.* at § 181.151.

342 *Id.* at § 181.152.

343 *Id.* at §§ 181.152(a), (d).

344 *Id.* at §§ 181.152(b), (c).

345 *Id.* at § 181.153.

make a profit; however, its direct and indirect compensation must be limited to its reasonable costs of preparing or transmitting the protected health information.[346]

Finally, the Texas law prohibits any individual disclosure of PHI from being made without prior notice to the individual, which may be done through a notice posted at the covered entity's place of business or on its website.[347] In many cases, the statute also requires the covered entity to obtain written authorization from the individual or his or her representative prior to disclosure.[348] Prior authorization is not required, however, if the disclosure is to another covered entity for the purposes of treatment, payment, health care operations, certain insurance functions defined by statute, or as otherwise authorized or required by state or federal law.[349]

(b) Enforcement

The Texas law permits the state attorney general to bring an action for injunctive relief to enjoin any violation of the statute or for civil penalties.[350] Under the statute, civil penalties may not exceed $5,000 for each negligent violation; $25,000 for each knowing or intentional violation; and $250,000 for each violation in which the covered entity knowingly or intentionally used PHI for financial gain.[351] Total penalties are capped at $250,000 per year if the disclosure was only to another covered entity for the purposes of treatment, payment, health care operations, or certain statutorily-defined insurance functions *and* the disclosed PHI was encrypted; the recipient of the PHI did not use or release it; and, as of the time of the disclosure, the covered entity had developed, implemented, and maintained security policies, including training.[352] On the other hand, if a court finds that violations have occurred frequently enough to constitute a "pattern or practice," the court may assess a civil penalty as large as $1.5 million per year[353] and the entity may be precluded from participating in any state-funded health care program.[354]

Covered entities may be subject to disciplinary action by appropriate Texas licensing authorities, including possible revocation of the entity's license if the violation is sufficiently egregious,[355] and

---

346 *Id.*

347 *Id.* at § 181.154(a).

348 *Id.* at § 181.154(b). The Texas attorney general has developed a standard authorization form for this purpose. *See* https://texasattorneygeneral.gov/files/agency/hb300_auth_form.pdf.

349 TEX. HEALTH & SAFETY CODE ANN. § 181.154(c).

350 *Id.* at § 181.201.

351 *Id.*

352 *Id.* at § 181.201(b-1).

353 *Id.* at § 181.201(c).

354 *Id.* at § 181.203.

355 *Id.* at § 181.202.

compliance audits under both HIPAA and the Texas law.[356] The statute, however, does not include any private right of action through which individuals could seek to remedy an improper disclosure of their own information, nor has it been the subject of any reported decisions.

[356] *Id.* at § 181.206.

SIDE BAR – HEALTH PRIVACY

Companies handling health information must understand the complex framework of laws and regulations comprising the healthcare privacy legal landscape.

Organizations processing or storing health information should understand whether this might subject them to the regulatory obligations of "covered entities" or "business associates" under HIPAA. Such organizations must comply with the HIPAA Privacy and Security Rules, which impose comprehensive requirements regarding the privacy and information security of protected health information.

Entities that are subject to HIPAA face the risk of potential regulatory audits, enforcement actions, and liability. Following the enactment of the final omnibus HIPAA/HITECH rule in January 2013, the Office of Civil Rights (OCR) of the U.S. Department of Health and Human Services has aggressively enforced HIPAA violations. Since that time, there have been numerous multimillion dollar OCR settlements based upon HIPAA non-compliance, often subsequent to large security breaches and OCR investigations.

Organizations processing or storing health information should understand that even if they are not subject to the regulatory obligations of "covered entities" or "business associates" under HIPAA, they may nevertheless be subject to certain state privacy laws imposing restrictions on the uses and disclosures of such information. Some of these laws apply more broadly than HIPAA, and even provide individuals with a private right of action to seek redress based on non-compliance with the law.

VI. FINANCIAL

Records containing the personal financial data of individuals have long been a focus in the ongoing privacy debate. Exposure of the records for over 100,000 U.S. taxpayers during a 2015 data breach at the Internal Revenue Service provided a clear reminder that both financial institutions and government agencies collect and retain a great deal of this data.[357] For that reason, a number of regulations have been created over the years to attempt to address the confidentiality of personally identifiable financial information, while permitting financial institutions to conduct business in a safe and secure manner.

A. The Gramm-Leach-Bliley Act

1. Overview of The GLBA

Enacted in 1999, the Financial Services Modernization Act, more commonly known as the Gramm-Leach-Bliley Act (GLBA)[358] was designed to provide financial institutions with requirements for protecting the personal information of customers and consumers. This was accomplished through a set of Safeguard Rules and Privacy Rules, the latter of which will be discussed in detail here.

At the time the GLBA was enacted, the financial services sector had long been moving toward consolidation.[359] In response to the stock market crash of 1929 and the subsequent Great Depression, regulations[360] had been put into place to create separations between financial services entities such as banks and securities firms.[361] In amending these regulations, the GLBA broke down the barriers between these entities so as to allow them to function in a more integrated fashion, thereby permitting financial institutions to serve a customer's needs across the banking spectrum. Acknowledging that one of the natural results of this integration would be that these financial institutions would have increased access to higher volumes of customer information, the GLBA set out to establish boundaries on how those institutions could handle that data in a safe and secure way.[362]

---

357 *Data Thieves Gain Access to 100,000 U.S. Taxpayers' Information: IRS*, REUTERS (May 26, 2015), *available at* http://www.reuters.com/article/us-usa-tax-cybersecurity-idUSKBN0OB2H520150526.

358 15 U.S.C. §§ 6801–6809 (1999), *available at* https://www.law.cornell.edu/uscode/text/15/chapter-94/subchapter-I.

359 *See* Joe Mahon, Fed. Reserve Bank of Minneapolis, *Financial Services Modernization Act of 1999, Commonly Called Gramm-Leach-Bliley*, FED. RESERVE HISTORY (Nov. 22, 2013), *available at* http://www.federalreservehistory.org/Events/DetailView/53.

360 *See, e.g.*, *Federal Reserve Bank of New York Circulars: 1248. Banking Act of 1933*, FED. RESERVE ARCHIVE, *available at* https://fraser.stlouisfed.org/scribd/?item_id=15952&filepath=/docs/historical/ny%20circulars/1933_01248.pdf#scribd-open.

361 *See id.*

362 For additional background on the Congressional debate, see Financial Services Modernization Act of 1999, 145 CONG. REC. S13871-S13881, S13883-S13917 (Nov. 4, 1999), and Conference Report on S. 900, Gramm-Leach-Bliley Act, 145 CONG. REC. H11513-H11551 (Nov. 4, 1999).

The terms of the GLBA apply to "financial institutions" that are required to implement technical safeguards around the personal data of their customers. The term is defined broadly to account for essentially all U.S. companies that, "the business of which is engaging in financial activities [that are financial in nature]."[363] Examples of such entities include, "companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance."[364]

The GLBA takes care to distinguish between "consumers" of financial institutions and "customers." Under the GLBA, a consumer is an "individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual."[365] This can be a one-time or infrequent touch point. A customer, by contrast, is an entity that is in a longer term, more continual relationship with the financial institution.[366] As more fully described below, this distinction is significant in that the notification requirements of the GLBA vary for customers and consumers.

2. Information Protected by the GLBA

The GLBA is designed to provide requirements for the handling and protection of "nonpublic personal information" provided by a consumer to a financial institution. Such information includes "personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."[367] This would exclude any information that is otherwise already publicly available, but does account for any combination of information (e.g., grouping, list, description) that is derived from nonpublic personal information.[368] Examples can include information provided in connection with a loan application packet, bank account data, and other personal financial data submitted in connection with a request for services from a financial institution.

3. Obligations of the GLBA

The GLBA has requirements for both the internal management and handling of nonpublic personal information by a financial institution ("The Safeguard Rules") and restrictions on the use and sharing of that data ("The Privacy Rules"). The Safeguard Rules are designed to serve as "standards for the financial institutions subject to" the jurisdiction of agencies with regulatory authority over such institutions as identified by § 6805 of the GLBA:

---

363 15 U.S.C. § 6809(3).

364 *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act*, FED. TRADE COMM'N (July 2002), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/brief-financial-privacy-requirements-gramm-leach-bliley-act#financial.

365 15 U.S.C. § 6809(9).

366 *Id.* at § 6809(11); *see also In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act*, *supra* note 364.

367 15 U.S.C. § 6809(4).

368 *Id.*

> relating to administrative, technical, and physical safeguards—(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[369]

The Privacy Rules outline the manner in which nonpublic personal information may be shared by the financial institution with other parties, and the permitted purposes under the GLBA for such sharing. At the heart of these privacy protections is the concept of consumer/customer notification.

(a) Notification Obligations

At the creation of a customer relationship with a financial institution, and on a no less than annual basis thereafter, the financial institution must make the customer aware of its policies and practices concerning handling and sharing the customer's nonpublic personal information.[370] The content of such notifications must include the financial institution's policies concerning disclosure of nonpublic personal information to nonaffiliated third parties, both while an individual is a customer of the financial institution and after the customer relationship ends; a description of the type and kind of nonpublic personal information that is collected by the financial institution; a description of the protections in place to safeguard the data; and a listing of any disclosures required under the Fair Credit Reporting Act.[371]

Customers must receive these notices as described above automatically and on an annual basis thereafter (or at the point in time when the privacy practices of the financial institution change in such a way that additional notification is required). *Consumers*, by contrast, receive notifications only when the financial institution shares nonpublic personal information with a nonaffiliated third party in a manner that is not already contemplated within one of the GLBA's exceptions. In the event of such sharing, consumers must be offered the ability to opt out of certain data sharing prior to the transmission of any nonpublic information to a nonaffiliated third party.[372]

(b) Nonaffiliated Third Parties

In general, the GLBA restricts a financial institution's ability to share nonpublic personal information with a nonaffiliated third party.[373] Section 6802 of the GLBA prohibits sharing with such

---

[369] 15 U.S.C. § 6801(b).

[370] *Id.* at § 6803(a).

[371] *Id.* at § 6803(c).

[372] *Id.* at § 6802(b).

[373] "The term 'nonaffiliated third party' means any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of such institution." *Id.* at § 6809(5).

parties unless the sharing is permitted under one of the specifically identified exceptions. The identified exceptions include sharing of nonpublic personal information with parties who perform services for or functions on behalf of the financial institution, which includes marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements that contain provisions requiring all parties to protect the confidentiality of the information shared.[374] Other more general exceptions are also outlined within § 6802, including but not limited to, the relaying of nonpublic personal information to effect the transaction requested by the consumer, the sharing of nonpublic personal information with the consumer's consent, the sharing of nonpublic personal information in order to assist with fraud detection or institutional risk management efforts, and also sharing with law enforcement and regulatory agencies as permitted or required by law.[375] In each instance, the receiving nonaffiliated third party must not further use the nonpublic personal information it receives for any purpose other than that for which it was originally provided.[376]

(c) Model Privacy Form

A variety of agencies[377] have rulemaking authority under § 6804 of the GLBA, and, as directed by § 6803(e) of the GLBA, the groups have combined efforts to develop Model Privacy Forms that can be leveraged by financial institutions looking to comply with these notification requirements.[378] Financial institutions that choose to use their regulating agency's model form qualify for safe harbor and are considered to have acted in compliance with the GLBA.[379]

4. Relationship with State Regulations

Section 6807 of the GLBA affirms that nothing contained within the GLBA shall be interpreted as, "superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this subchapter, and then only to the extent of the inconsistency."[380] In fact, to the extent that related state laws afford an individual more protection than is outlined in the GLBA, it states that such additional protections are not to be construed as "inconsistent."[381] The authority to determine whether a state's financial privacy regulations are inconsistent with the GLBA currently

---

374 *Id.* at § 6802(b)(2).

375 *Id.* at § 6802(e).

376 *Id.* at § 6802(c).

377 CFPB, SEC, CFTC, FTC (15 U.S.C. § 6804(1)). *See also* 15 U.S.C. §6805 for enforcement powers of these agencies.

378 For an example of such Model Privacy Forms, *see* 12 C.F.R. Part 1016 (Appendix), *available at* http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=d98a14fe2ed1d022d4e943885dbb70aa&ty=HTML&h=L&n=pt12.8.1016&r=PART#ap12.8.1016_117.1.

379 15 U.S.C. § 6803(e)(4).

380 *Id.* at § 6807(a).

381 *Id.* at § 6807(b).

rests with the Bureau of Consumer Financial Protection (CFPB) under the GLBA.[382] As a result, some states have taken it upon themselves to enact stricter data privacy regulations for the protection of consumer nonpublic personal information.

(a) California Financial Information Privacy Act

Effective July 1, 2004, the California Financial Information Privacy Act (also known as "SB1" or "FIPA") was put in place by the state legislature because "[t]he policies intended to protect financial privacy imposed by the Gramm-Leach-Bliley Act are inadequate to meet the privacy concerns of California residents."[383] Notably, SB1 does not distinguish between customers who have a continuing relationship with financial institutions and consumers who may have less frequent touch points, opting instead to universally identify "consumers" as parties protected by its provisions.[384] Further, while, like the GLBA, SB1 requires a financial institution obtain "explicit prior consent" from a consumer when sharing the consumer's nonpublic personal information with a nonaffiliated third party,[385] it also requires the institution annually "clearly and conspicuously" notify consumers and obtain their consent to disclose nonpublic personal information with affiliates in certain circumstances.[386] In 2008 this provision came up for review by the Ninth Circuit in *American Bankers Association v. Lockyer* (now known as *ABA v. Brown*), where the Court upheld the affiliate-sharing requirement of SB1 to the extent the nonpublic personal information involved was not considered "consumer report" information under (and is therefore preempted by) the Fair Credit Reporting Act.[387] As with the GLBA, SB1 also provides a safe harbor for financial institutions that leverage the provided Model Form entitled, "Important Privacy Choices for Consumers."[388]

(b) Additional State Financial Privacy Regulations

Other states have adopted an "opt-in" posture for sharing nonpublic personal information with both affiliates and nonaffiliated third parties. Under Title 6 of the Alaska Statutes, the "records of financial institutions relating to their depositors and customers and the information in the records," are to be kept confidential, and the financial institution is required, if possible, to notify a consumer

---

382 *Id.*

383 CAL. FIN. CODE §§ 4051.5(3) (July 1, 2004), *available at* https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=FIN&division=1.4.&title=&part=&chapter=&article.

384 CAL. FIN. CODE § 4052(f).

385 *Id.* at § 4052.5; *see also*, *Your Financial Privacy Rights*, STATE OF CAL. DEP'T OF JUSTICE (June 2014), *available at* https://oag.ca.gov/privacy/facts/financial-privacy/rights.

386 CAL. FIN. CODE § 4053(b).

387 Am. Bankers Ass'n v. Lockyer, 541 F.3d 1214 (9th Cir. 2008).

388 CAL. FIN. CODE § 4053(d), and Model Form, *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/sb1_standards.pdf.

prior to disclosing such information.[389] Vermont's Financial Privacy Act likewise has similar restrictions in place.[390] Still other states have chosen to more closely align with the GLBA standard of providing notification in the context of data sharing with nonaffiliated third parties. Because of the fluctuating nature of state data protection regulations, it is advisable to refer to the current text of a state's statutes for the most up-to-date requirements for that given state or territory.

5. Rulemaking and Enforcement

When originally enacted, primary rulemaking authority for the GLBA fell under the purview of the FTC. With the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act in July 2010, that responsibility shifted to the CFPB.[391] Since that time, the CFPB has formally adopted one rule related to the GLBA. In October 2014, the CFPB issued a final rule that relaxed some of the requirements concerning annual customer privacy notifications.[392] Prior to adoption of the final rule, financial institutions had been required to deliver hard-copy notices to all impacted consumers annually (or electronically transmit the notices to consumers who had agreed to electronic delivery), leading to a significant expenditure of time and resources in order to comply with GLBA. The final rule now allowed for the online posting of these notices by financial institutions so long as individuals have been given the option to exercise any available opt-out rights and have not done so, all required notifications have been provided to date, the information included in the privacy notice has not changed since the last notification was delivered, and the financial institution uses the Model Privacy Form as provided by its relevant regulating agency.[393]

The GLBA is enforced by federal banking agencies and other federal regulatory authorities as well as state insurance authorities. The GLBA Privacy Rule is enforced by the FTC.[394]

---

389 ALASKA STAT. § 06.01.028.

390 VT. STAT. ANN. tit. 8, §§ 10201 *et seq.*, tit. 9, § 2480e.

391 12 U.S.C. §§ 5841(12)(J), 5514(b)–(c), 5515(b)–(c). Additional summary information of the CFPB's responsibilities under GLBA and the CFPB's interpretation of the act can be found in CONSUMER FIN. PROT. BUREAU, CFPB SUPERVISION AND EXAMINATION MANUAL, at GLBA Privacy 1–10 (Oct. 2012), relevant portion *available at* http://www.cfpaguide.com/portalresource/Exam%20Manual%20v%202%20-%20GLBA.pdf.

392 Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P), 79 Fed. Reg. 64,057 (Oct. 28, 2014), *available at* http://www.gpo.gov/fdsys/pkg/FR-2014-10-28/pdf/2014-25299.pdf.

393 *Id.*

394 *See* FED. TRADE COMM'N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT (July 2002), at 14, *available at* https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf.

B. The Fair Credit Reporting Act

1. Overview of the FCRA

The Fair Credit Reporting Act (FCRA) was enacted in 1970 to regulate the consumer reporting industry and provide privacy rights in consumer reports.[395] The FCRA mandates accurate and relevant data collection, provides consumers with the ability to access and correct their information, and limits the use of consumer reports to defined permissible purposes.[396] The FCRA applies to "any consumer reporting agency" that furnishes a "consumer report"[397] as well as, in limited circumstances, any person or entity that "furnishes" credit-related information to a consumer reporting agency.[398]

The FCRA defines "consumer reporting agencies" (CRAs) as entities which, for a monetary fee, "regularly engage in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."[399] Well known CRAs include Equifax, TransUnion, and Experian Information Solutions, but there are also thousands of smaller CRAs.

A "consumer report" is any "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used for the sole purpose of serving as a factor in establishing the consumer's eligibility for . . . credit or insurance purposes, employment purposes, or any other purpose authorized under section 1681b of this title."[400] Courts have held that "even if a report is used or expected to be used for a non-consumer purpose, it may still fall within the definition of a consumer report if it contains information that was originally collected by a consumer reporting agency with the expectation that it would be used for a consumer purpose."[401]

---

395 15 U.S.C. § 1681 (1970). FCRA amendments in 1996 strengthened consumer access and correction rights and included provisions for non-consumer-initiated transactions. FCRA was further amended by the Fair and Accurate Credit Transaction Act in 2003, which enacted additional consumer protections.

396 *See, e.g.*, *The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/fcra; Gorman v. Wolpoff & Abramson, LLP, 584 F.3d 1147, 1153 (9th Cir. 2009) ("Congress enacted the Fair Credit Reporting Act . . . to ensure fair and accurate credit reporting, promote efficiency in the banking system, and protect consumer privacy." (internal quotation omitted)).

397 15 U.S.C. § 1681b.

398 *Id.* at §§ 1681b, 1681s-2.

399 *Id.* at § 1681a(f).

400 *Id.* at § 1681(d).

401 Ippolito v. WNS, Inc., 864 F.2d 440, 453 (7th Cir. 1988); Bakker v. McKinnon, 152 F.3d 1007, 1012 (8th Cir. 1998) (quoting *Ippolito*, 864 F.2d at 453).

2. Duties of Consumer Reporting Agencies

The FCRA specifically requires CRAs to adhere to the following requirements:

- Accuracy: "Wherever a consumer reporting agency prepares a consumer report, it shall follow reasonable procedures to assure maximum accuracy of the information concerning the individual about whom the report relates."[402]

- Disclosure: CRAs, at the request of the consumer, must disclose, among other things, "[a]ll the information in the consumer's file at the time of the request."[403]

- Investigation: If a consumer disputes the accuracy of any information, a consumer reporting agency, "shall, free of charge, conduct a reasonable investigation to determine whether the disputed information is inaccurate."[404]

- Free Consumer Reports: CRAs must provide a free consumer report once a year at the request of a consumer. Consumers can obtain their reports at http://annualcreditreport.com.

- Permissible uses: A CRA can furnish a consumer report only for permissible purposes which includes:

    1) in response to a court order or grand jury subpoena;

    2) to the person to whom the report pertains;

    3) to a "person which [the agency] has reason to believe" intends to use the information in connection with:

        a) the extension of credit;

        b) employment purposes;

        c) insurance underwriting;

        d) licensing or the conferral of governmental benefits;

        e) assessment of credit risks associated with an existing credit obligation; or

---

402 15 U.S.C. § 1681e(b).

403 *Id.* at § 1681g.

404 *Id.* at § 1681i(a).

f) a "legitimate business need" when engaging in a "business transaction involving the consumer";

4) to establish a person's capacity to pay child support;

5) to an agency administering a state plan for use to set initial or modified child support award; or

6) to the Federal Deposit Insurance Corporation or National Credit Union Administration.[405]

- Notice and Opt Out: A CRA may share consumer report information with its affiliates. However, consumers whose information is shared with an affiliate must be notified of the disclosure and given an opportunity to opt out.[406] In addition, entities that receive consumer report information from affiliates may not use it to offer products or services to the consumer unless the affiliate gave certain strong disclosures and an opt-out opportunity to the consumer.[407] Disclosure to non-affiliates is governed by the GLBA.

3. Furnishers of Information to CRAs

To ensure that credit reports are accurate, the FCRA imposes some duties on the sources that provide credit information to CRAs, called "furnishers" in the statute.[408] Among those obligations are the duties to provide accurate information to CRAs and upon receiving a report that the consumer disputes the accuracy or completeness of the information provided, to investigate and, if needed, to correct the report of any "inaccurate or incomplete" information.[409] If the completeness or accuracy of any information furnished by any person to any CRA is disputed to such person by a consumer, the person may not furnish the information to any CRA without notice that such information is disputed by the consumer.

4. Users of Consumer Reports

Users of consumer reports include employers who use consumer reports in employment decisions as well as lenders, insurance companies, and others. Users must certify to the CRA the permissible

---

405 *Id.* at § 1681b.

406 *Id.* at § 1681a(d)(2)(A)(iii).

407 *Id.* at § 1681s-3(a)(1).

408 Longman v. Wachovia Bank, N.A., 702 F.3d 148, 150–51 (2d Cir. 2012) (citing 15 U.S.C. § 1681s-2). "The most common . . . furnishers of information are credit card issuers, auto dealers, department and grocery stores, lenders, utilities, insurers, collection agencies, and government agencies." H.R. REP. NO. 108–263, pt. 1, at 24 (2003).

409 15 U.S.C. § 1681s–2(a); *see Longman*, 702 F.3d at 150 ("Among these are duties to refrain from knowingly reporting inaccurate information, *see* § 1681s-2(a)(1), and to correct any information they later discover to be inaccurate, *see* § 1681s-2(a)(2).").

purpose for which the report is being obtained and that the report will be used for no other purpose.[410] Users must also notify consumers when adverse action is taken with respect to any consumer that is based in whole or in part on any information contained in a consumer report.[411] The notice must point out the adverse action, explain how to reach the agency that reported on the consumer's credit, and tell the consumer that he can get a free copy of the report and dispute its accuracy with the agency.[412]

The FCRA provides that a person may not procure a consumer report for employment purposes unless the employer or potential employer discloses in writing to the consumer that a report is to be obtained and the consumer authorizes in writing that a report can be obtained. A CRA may not furnish a consumer report for employment purposes unless the person who obtains such report certifies to the CRA that the consent of the individual was obtained and that the information in the consumer report will not be used in violation of any equal employment opportunity law or regulation.[413]

5. Limitations on Information Contained in Credit Reports

No CRA may make any consumer report containing any of the following items of information:

1) cases under Title 11 or under the Bankruptcy Act that, from the date of entry of the order for relief or the date of adjudication, antedate the report by more than ten years;

2) civil suits, civil judgments, and records of arrest that, from date of entry, antedate the report by more than seven years or until the governing statute of limitations has expired, whichever is the longer period;

3) paid tax liens which, from date of payment, antedate the report by more than seven years;

4) accounts placed for collection or charged to profit and loss which antedate the report by more than seven years;

5) any other adverse item of information, other than records of convictions of crimes which antedates the report by more than seven years; or

6) the name, address, and telephone number of any medical information furnisher that has notified the agency of its status, unless (A) such name, address, and telephone number are restricted or reported using codes that do not identify, or provide information sufficient to infer, the specific provider or the nature of such

---

410 15 U.S.C. § 1681e(a).

411 *Id.* at § 1681m.

412 *Id.*

413 *Id.* at § 1681b(b)(1)(A)(i).

> services, products, or devices to a person other than the consumer; or (B) the report is being provided to an insurance company for a purpose relating to engaging in the business of insurance other than property and casualty insurance.[414]

The above provisions, however, are not applicable in the case of any consumer credit report to be used in connection with (1) a credit transaction involving, or which may reasonably be expected to involve, a principal amount of $150,000 or more; (2) the underwriting of life insurance involving, or which may reasonably be expected to involve, a face amount of $150,000 or more; or (3) the employment of any individual at an annual salary that equals, or which may reasonably be expected to equal $75,000, or more.

6. Private Rights of Action and Damages

Private rights of action exist to enforce negligent or willful violations of the FCRA. It permits consumers to recover actual damages from "any person who is negligent in failing to comply with a requirement" it imposes; or actual, statutory, and potentially punitive damages from a person whose violation was willful.[415] "Actual damages" has been interpreted to include damages for emotional distress.[416]

While consumers have a private remedy against "negligent or willful misconduct by a furnisher" of consumer credit information, this right only arises once the furnisher has received a notice from the CRA disputing the accuracy or completeness of the information provided.[417] The FCRA's statute of limitations extends to two years after the date when plaintiff discovers the violation or five years after the date of the violation, whichever occurs earlier.

7. Rulemaking and Enforcement

In addition to private litigants, the FCRA is enforced by the FTC and the CFPB. The Dodd-Frank Act of 2010 assigned the CFPB primary federal authority for enforcement and rule making regarding the FCRA. The Dodd-Frank Act also created a Consumer Financial Civil Penalty Fund to receive civil penalties obtained by the CFPB for violations of consumer financial protection statutes.

C. The Right to Financial Privacy Act of 1978

In response to a string of court decisions declaring that an individual has no reasonable expectation of privacy in his or her financial records, most notably the Supreme Court's decision in *United States*

---

414 *Id.* at § 1681c.

415 *Id.* at §§ 1681o–n.

416 S*ee* Taylor v. Tenant Tracker, Inc., 710 F.3d 824, 828 (8th Cir. 2013); Robinson v. Equifax Info. Servs., LLC, 560 F.3d 235, 239 (4th Cir. 2009); Guimond v. Trans Union Credit Info. Co., 45 F.3d 1329, 1333 (9th Cir. 1995).

417 15 U.S.C. §§ 1681s-2(a)–(b); Boggio v. USAA Fed. Sav. Bank., 696 F.3d 611 (6th Cir. 2012).

v. Miller,[418] Congress enacted the Right to Financial Privacy Act of 1978 (RFPA).[419] The RFPA prohibits agencies of the federal government from obtaining such records from financial institutions without first giving the individual notice and an opportunity to object to the disclosure.[420]

1. Overview of the RFPA

The RFPA explicitly governs requests made by "any agency or department of the United States, or any officer, employee, or agent thereof," and does not apply to equivalent agencies at the state and local government levels.[421] As discussed below several states have chosen to enact similar legislation on their own, but the RFPA only applies to federal government agencies.

As with the GLBA, the RFPA defines "financial institutions" required to comply with its terms broadly. This includes entities you might expect to be a financial institution such as depository banks, loan companies, savings associations, and credit unions; but also pulls in "card issuers" as defined by the Truth in Lending Act.[422] As a result, any entity that issues a credit card to a consumer, including entities such as retailers and gas stations, must follow RFPA notification provisions prior to making disclosures to the federal government.

The records protected by the RFPA are all documentation (i.e., financial records) that evidences a customer's relationship with the financial institution. The RFPA is limited, however, to the records of individuals or a partnership "of five or fewer individuals."[423] For that reason, the accounts of companies or entities comprising more than five individuals are not considered "financial records" under the RFPA.

2. Obligations of the RFPA

The RFPA places obligations on both the federal agency requesting a customer's financial records and on the financial institution that releases the data to the federal government.

(a) Limitations on Federal Government Requests

A federal agency seeking the financial records of an individual must be able to clearly state the purpose for which the information is sought, including the provision of a valid and properly served administrative or judicial subpoena, summons, or search warrant, or a formal written request from the agency if such vehicles are not available.[424] The RFPA provides required notification language to be

---

418 United States v. Miller, 425 U.S. 435, 442–43 (1976).

419 12 U.S.C. §§ 3401–3422 (1978), *available at* https://www.law.cornell.edu/uscode/text/12/chapter-35.

420 *Id.* at § 3402.

421 *Id.* at § 3401.

422 15 U.S.C. § 1602(o).

423 12 U.S.C. § 3401(4).

424 *Id.* at § 3402.

included in the request document that identifies the specific basis for the government's request and the nature of its inquiry into the financial records.[425] Once the data has been received, the agency may not further transmit the information provided to another agency or department unless "the transferring agency or department certifies in writing that there is reason to believe that the records are relevant to a legitimate law enforcement inquiry, or intelligence or counterintelligence activity, investigation or analysis related to international terrorism within the jurisdiction of the receiving agency or department."[426]

(b) Financial Institution's Obligations

Upon receipt of the government's request for a customer's financial records, financial institutions subject to the RFPA must obtain from the customer a signed and dated form of consent that:

1) authorizes disclosure of the customer's financial records for a period not in excess of three months;

2) states that the customer may revoke such authorization at any time before the financial records are disclosed;

3) identifies the financial records which are authorized to be disclosed;

4) specifies the purposes for which, and the Government authority to which, such records may be disclosed; and

5) states the customer's rights under the RFPA.[427]

The financial institution cannot make a customer's consent to release information a condition upon which the institution will do business with the customer, and the customer under most circumstances has the right to obtain a copy of the data that was released to the government.[428]

(c) Exceptions

Under § 3409 of the RFPA, notification to a customer may be delayed under a proscribed set of circumstances. More specifically, if the government is able to evidence that the request is being made pursuant to an ongoing investigation and notification would jeopardize the investigation or the life or safety of another, or the notification would otherwise create the opportunity for the intimidation of a witness to the matter or create a flight risk for the individual being investigated, a court is able

---

425 *Id.* at §§ 3405(2), 3406(b), 3407(2), 3408(4)(A).

426 *Id.* at § 3412(a).

427 *Id.* at § 3404(a).

428 *Id.* at §§ 3404(b), (c).

to grant a request for a delay in notification with an initial period not to exceed 90 days.[429] Further, the RFPA does not apply to requests for financial records that do not particularly identify an individual, records whose disclosure is required by federal rule, disclosures made pursuant to the Federal Rules of Civil or Criminal Procedure, disclosures made to uncover crimes made against the financial institution by criminal insiders, and disclosures made to certain regulatory agencies like the Federal Housing Finance Agency and the CFPB, among other identified exceptions in § 3413 of the act.[430] In early 2015, legislation introduced in the House of Representatives sought to remove the CFPB's exemption in the RFPA.[431] At the time of the publication of this Primer, the legislation was still pending review in the House Committee on Financial Services.

3. Civil Penalties for Non-Compliance

The RFPA provides recourse for individuals who are able to successfully demonstrate that either their financial institution or the government acted in a manner contrary to the provisions of the RFPA. Liability under the RFPA can equal the sum of:

1) $100 without regard to the volume of records involved;

2) any actual damages sustained by the customer as a result of the disclosure;

3) such punitive damages as the court may allow, where the violation is found to have been willful or intentional; and

4) in the case of any successful action to enforce liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.[432]

Federal agents found to have violated the RFPA may be subject to further internal discipline from the Director of the Office of Personnel Management.[433] Financial institutions have immunity from civil liability for disclosures made as a part of reporting criminal activity evidence contained in records to a government authority via mechanisms such as a Suspicious Activity Report (SAR) with Financial Crimes Enforcement Network (FinCEN).[434]

---

[429] *Id.* at § 3409.

[430] *Id.* at § 3413.

[431] Consumer Right to Financial Privacy Act of 2015, H.R. 1262, 114th Cong. (Mar. 4, 2015), *available at* https://www.congress.gov/bill/114th-congress/house-bill/1262.

[432] 12 U.S.C. § 3417(a).

[433] *Id.* at § 3417(b).

[434] *Id.* at § 3403(c).

4. Relationship with State Regulations

As mentioned above, the RFPA does not apply to requests made by state or local government agencies. Several states, however, have enacted regulations with terms similar or equivalent to those of the RFPA, including Alabama, Alaska, Connecticut,[435] California,[436] Illinois,[437] Louisiana,[438] Maryland,[439] Maine, New Hampshire, North Carolina,[440] North Dakota, Oklahoma, Oregon, Utah, and Vermont. For the most up-to-date information regarding a state's financial privacy regulations, consult the current text of a state's statutes.

---

[435] CONN. GEN. STAT. § 36a-43, *available at* http://cga.ct.gov/current/pub/chap_664a.htm#sec_36a-43.

[436] CAL GOV'T CODE §§ 7460–7493.

[437] 205 ILL. COMP. STAT. 5/48.1.

[438] LA. REV. STAT. § 6:333, *available at* http://law.justia.com/codes/louisiana/2011/rs/title6/rs6-333.

[439] MD. CODE ANN., FIN. INST. §§ 1-301 to 1-306 (2014).

[440] North Carolina Financial Privacy Act, N.C. GEN. STAT. ANN. § 53B-1 *et seq.*, *available at* http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/ByChapter/Chapter_53B.pdf.

SIDE BAR – FINANCIAL PRIVACY

The regulations in place protecting personal financial data of individuals are wide-ranging, and can impact more than just financial institutions.

Take care when sharing nonpublic personal information with third parties. Financial institutions that want to share such data with nonaffiliated third parties should validate that the data is being shared under one of the permitted purposes specifically outlined in the GLBA or obtain the individual's consent prior to transferring the data.

The obligations concerning protection of personal information contained in a credit report can extend to parties beyond Credit Reporting Agencies. Under the FCRA, producers of consumer credit reports, parties that furnish data to credit reporting agencies, and recipients of consumer credit reports all have specific obligations for handling of credit reports, ranging from sharing to future use of the data. Companies should become familiar with their role in the process and whether there are restrictions in place on their behavior vis-à-vis credit reports.

Become familiar with both the federal and state laws that may apply to your company as it manages personal financial data. At times, state regulations can be even more restrictive and protective of a consumer's right to privacy than the federal standards.

VII. WORKPLACE PRIVACY

More than ever before, employers have a wealth of powerful and new technologies that allow them to monitor employee communications, such as telephone calls, email and text messages, and Internet access; and to monitor employees' movements using video cameras and satellite-based Global Positioning System (GPS) tracking devices. There are legitimate and well-accepted business reasons for employee monitoring: to make certain that employees spend working hours actively engaged in work-related activities; to protect confidential information and trade secrets; to ensure compliance with governmental regulations; and to guard against illegal activities.[441]

Employee monitoring and surveillance is not without limits. As discussed below, while there have been advances in the enactment and application of workplace privacy laws, technology continues to test their limits.

A. Legal Framework

1. Regulatory Protections

The Electronic Communications Privacy Act[442] (ECPA) is a key privacy law that applies in the context of network surveillance and monitoring of employees.[443] The ECPA prohibits the intentional interception of "any wire, oral or electronic communication" while those communications are being made, are in transit, and while stored on computers. There are two exceptions to the ECPA that generally exempt employers from its prohibitions.[444] First, an employer is exempt if an employee is using a company computer or device and the employer can show a valid business reason for monitoring an employee's communications or activities.[445] Second, an employer is exempt from the ECPA if the employee has consented to email or telephone call monitoring.[446]

---

441 According to a 2007 survey conducted by the American Management Association and the ePolicy Institute, 66% of employers surveyed monitored employee Internet connections, nearly half tracked content, keystrokes, and time spent at the keyboard, and only slightly fewer employers stored and reviewed computer files. Of the 43% of companies that monitored email communications, nearly three-quarters used technology to automatically monitor email, and over a third assigned an individual to manually read and review email. *The Latest on Workplace Monitoring and Surveillance*, AM. MGMT. ASS'N (Nov. 17, 2014), http://www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx.

442 18 U.S.C. §§ 2510–2520, 2701 (2012).

443 Title I of the ECPA, known as the "Wiretap Act," regulates the interception of transmitted communications. Title II, referred to as the "Stored Communications Act," governs access to stored communications and records held by communications service providers. Both are aimed at protecting private communications, such as email, from unwarranted government and private intrusion.

444 18 U.S.C. §§ 2510 *et. seq.* (2012).

445 *Id.* at § 2511(2)(a)(i).

446 *Id.* at § 2511(2)(c).

2. U.S. Constitution

The Fourth Amendment to the U.S. Constitution provides an additional layer of privacy protection available to government employees by guaranteeing "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[447] A pivotal determination in cases involving governmental invasion of privacy is whether the government employee has a reasonable expectation of privacy in relation to the conduct of the governmental employer.[448] Please refer to Section III.A.4 of this Primer for further information regarding the right to privacy under the Fourth Amendment.

3. State Issues

As discussed in Section II.A of this Primer, common law privacy rights afford varying degrees of protection for individuals, including private employees. These rights are generally predicated on a reasonable expectation of privacy by the employee and a highly offensive violation by the employer.[449] Employees, in proving a claim based on this tort, must establish that the employer's intrusion "would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object."[450]

Given the increasing use of technology by employees in their private lives and the growth of technology permitting employee monitoring, there is an emerging trend among states to favor the protection of personal information of private employees.[451] Two states, Connecticut and Delaware, have passed legislation requiring employers to give notice to employees prior to monitoring email communications or Internet access.[452] Connecticut[453] requires employers engaged in electronic monitoring to give prior written notice to all employees, informing them of the types of monitoring implemented. An employer is exempt from giving this notice if it has reasonable grounds to believe that (1) employees are engaged in illegal conduct, and (2) electronic monitoring may produce evidence of the misconduct. Delaware[454] prohibits employers from monitoring or intercepting electronic mail or

---

447 U.S. CONST. amend. IV.

448 O'Connor v. Ortega, 480 U.S. 709, 716 (1987).

449 *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977) ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of is privacy, if the intrusion would be highly offensive to a reasonable person.").

450 *Id.* at § 652B cmt. d.

451 *Access to Social Media Usernames and Passwords*, NAT'L CONFERENCE OF STATE LEGIS. (July 6, 2016), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

452 CONN. GEN. STAT. ANN. § 31-48d; DEL. CODE. ANN. tit. 19, § 705; *see also generally*, NAT'L CONFERENCE OF STATE LEGIS., *supra* note 451.

453 CONN. GEN. STAT. ANN. § 31-48d.

454 DEL. CODE. ANN. tit. 19, § 705.

Internet access/use of an employee unless the employer has first given a one-time written or electronic notice to the employee. A Delaware employer is exempt from providing prior notice for processes that are performed solely for the purpose of computer system maintenance and/or protection, and for court-ordered actions.

There is no "one size fits all" when it comes to determining whether employee privacy claims trump the rights of an employer to access an employee's personal information. Resolution of workplace privacy issues are intensely fact-driven and often turn on such considerations as who owns the device, the existence and scope of a computer usage policy, and whether an employee has consented to being monitored.

B. Use of Company Equipment and Email

Underpinning court decisions on an employer's alleged violations of an employee's right to privacy, is whether the employee had a *reasonable expectation* of privacy in the personal information sought to be protected. The conclusion reached on this issue often turns on whether the employer or the employee owns the device.

In 2010, the Supreme Court was faced with applying the law of privacy in the broader context of technological advances in electronic communications in *City of Ontario v. Quon*.[455] *Quon* involved the privacy interest of a government employee in text messages that he sent on a government-owned pager.[456] Without resolving the issue of whether the employee had a reasonable expectation of privacy in the text messages, the Court held that the government's search of the messages was reasonable since it was "justified at its inception" and "the measures adopted [were] reasonably related to the objectives of the search and [were] not excessively intrusive in light of the circumstances giving rise to the search."[457]

The Court was, however, reluctant to establish precedent on broader employee privacy rights given the rapid pace of evolving technologies, explaining, "[t]he Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[458]

Since *Quon*, numerous courts around the country have found that employer-supplied electronic devices, such as computers, cell phones, and tablets, may be subject to monitoring regardless of whether the specific device is identified by an employer as being monitored. However, monitoring

---

455 560 U.S. 746 (2010).

456 Although *Quon* involved Fourth Amendment privacy issues of governmental searches, the Court concluded that the search would be regarded as reasonable and normal in the private-employer context. *Quon*, 560 U.S. at 764–765.

457 *Id.* at 761.

458 *Id.* at 759.

the content of employees' private communications may present legal risks to employers in certain circumstances. In addition to ownership of the device, courts consider the existence and scope of a company's computer usage policy, steps taken by the employee to maintain the privacy of personal emails, the use of the company-owned computer system, and the content of the communication at issue. For example, in *Stengart v. Loving Care Agency, Inc.*, the New Jersey Supreme Court held that a private company employee had a reasonable expectation of privacy in personal emails on company computers, such that employers should not read the specific contents of such emails.[459] The court noted the important public policy concerns at issue in the case because the personal emails between the employee and her attorney were protected by the attorney-client privilege, but the case is instructive regarding an employee's reasonable expectation of privacy more generally.

C. Bring Your Own Device Policies

More and more, employers are transitioning from employer-owned devices to employee-owned devices.[460] With the widespread usage of smartphones, tablets, and personal laptops, employers and employees alike are finding that policies that permit employees to utilize their own devices in the workplace provide both convenience and cost savings. But while connecting an employee-owned personal device to an employer computer system to access email and data on the employer network allows an employee to work anytime, anywhere, the bring-your-own-device revolution is causing tensions between how much access an employer is permitted to have to an employee's device and how much privacy the employee can expect.[461] Companies are concerned about related issues, such as keeping confidential data from falling into a competitor's hands and preventing disclosure of other corporate or personally identifiable data to outsiders, while employees want to keep personal photographs, text messages, and personal emails private.[462]

Issues also arise as to how to effectively deal with company and personal information on the devices after employment terminates. In a case out of the Southern District of Texas, *Rajaee v. Design Tech Homes, Ltd*, an employee who had worked in the home construction sales industry was required to have open and constant communication with clients.[463] The employee chose to not use an employer-owned cell phone and instead utilized his own iPhone for work calls, emails, calendars, and business

---

459 990 A.2d 650, 663 (N.J. 2010).

460 In a 2012 survey conducted by SANS, 60% of employers allowed employees to bring their own devices to work. Kevin Johnson, *SANS Mobility/BYOD Security Survey*, SANS INST. (2012), http://www.sans.org/reading-room/whitepapers/analyst/mobility-byod-security-survey-35210. Notably, the same year, a survey conducted by Ovum revealed that only 30% of employers required their employees to a sign BYOD agreement. Adrian Drury & Richard Absalom, *BYOD: An Emerging Market Trend In More Ways Than One*, OVUM (2012), http://www.us.logicalis.com/globalassets/united-states/whitepapers/logicalisbyodwhitepaperovum.pdf.

461 Marilyn Odendahl, *Bring Your Own Device Creates Privacy Issues for Employees*, INDIANAPOLIS BUS. J. (August 20, 2014), http://www.ibj.com/articles/49128-bring-your-own-device-creates-privacy-issues-for-em.

462 *Id.*

463 Rajaee v. Design Tech Homes, Ltd., Civ. A. No. H-13-2517, 2014 U.S. Dist. LEXIS 159180, at *2 (S.D. Tex. Nov. 11, 2014).

contacts.[464] Upon notifying his employer that he would be resigning, the employee was immediately terminated and the employer's network administrator remotely wiped his phone—deleting all data—both personal and work related.[465] The court rejected the employee's claim under the ECPA, reasoning that information an individual stores on a hard drive or cell phone does not qualify as electronic storage under the statute.[466] Accordingly, the plaintiff could not recover damages arising from the loss of videos, pictures, and other personal data on the plaintiff's personal device.[467]

D. Social Media Privacy

From Twitter and Facebook to LinkedIn, Pinterest, and YouTube, social media offers a vast array of opportunities for companies to engage with both job applicants and employees. However, employer exposure to the potentially costly and protracted risks associated with social media is greater now than ever before. Employers may face harassment, discrimination, and invasion of privacy claims, and in some cases, find that their electronic business connections may be compromised with the departure of particular employees. Social media sites nevertheless offer significant benefits to employers such as the ability to screen candidates prior to hiring and to monitor employees while they are on the clock.

1. Passwords and Other Login Information

The most significant privacy violations in the context of workplace social media monitoring are employer policies that compel employees to hand over their passwords and other login information. Since 2012, nineteen states have enacted laws that protect employee privacy in this regard. For example, Illinois,[468] Colorado,[469] Oregon,[470] and Washington[471] prohibit an employer from requesting

---

464 *Id.*

465 *Id.* at *3.

466 *Id.* at *5 (citing Garcia v. City of Laredo, Tex. 702 F.3d 788, 791 (5th Cir. 2012) and 18 U.S.C. § 2701(a)(1)).

467 An overview of BYOD policies in the context of litigation may be found at Andrew Hinkes, *BYOD Polices: A Litigation Perspective*, AM. BAR ASS'N (July 8, 2013), *available at* http://apps.americanbar.org/litigation/committees/corporate/articles/spring2013-0713-byod-policies-litigation-perspective.html.

468 820 Ill. Comp. Stat. 55/1 makes it illegal for an employer to request a password or related account information from an employee or prospective employee in order to access their social media accounts.

469 The Colorado Social Media and the Workplace Law, COLO. REV. STAT. § 8-2-127, prohibits employers from requesting, suggesting, or compelling an employee or job applicant to change, submit, or disclose login information related to the person's social media site.

470 OR. REV. STAT. § 659A.330 (prohibits employers from accessing employees' private social media sites).

471 WASH. REV. CODE § 49.44.200 (bans employers from requesting user names and passwords of current or prospective employees' personal social media accounts).

access to an employee's personal social media accounts, and California[472] and Michigan[473] prohibit an employer from requesting an employee to access his or her personal account in the *presence* of the employer.[474] Generally, many state social media laws bar employers from requiring or even requesting that an applicant or employee disclose the login information for his or her personal social media account.[475] Other restrictions include prohibiting applicants and employees from changing the privacy settings on his or her accounts, "following" coworkers or employers, or adding either as "friends."[476] Although these laws have a common goal of protecting employee privacy and speech, they are often inconsistent and have, in turn, caused confusion for multistate employers.

2. Content Monitoring

There is a delicate balance between protecting employee speech and privacy while simultaneously protecting the reputations of employers. In *Ehling v. Monmouth*, the U.S. District Court for New Jersey found that a nonprofit hospital did not violate the Federal Stored Communications Act (SCA) or the employee's right to privacy after it used screenshots of the employee's social media page as grounds for suspension.[477] In *Ehling*, the plaintiff alleged that her employer violated the SCA by accessing her Facebook wall posts that were limited by her privacy settings to only be accessible by her "friends."[478] Although the court found that nonpublic Facebook wall posts *are* protected by the SCA, it reasoned that the employer did not violate the SCA because the employer viewed the content from a person who was "authorized" to view the posts without any coercion or pressure.[479]

Employers also face challenges by accessing employee social media accounts for other legitimate purposes such as candidate evaluations, promotions, or terminations because both state and federal laws prohibit employers from making employment related decisions based upon legally-protected characteristics such as religion, national origin, age, citizenship, sexual orientation, pregnancy or

---

472 CAL. LAB. CODE § 980 (limits employers from asking employees for social media account information).

473 Michigan Internet Privacy Protection Act, MICH. COMP. LAWS ANN. §§ 37.271 *et seq.* (prohibits employers and educational institutions from accessing the social media accounts of employees, job applicants, students, and prospective students).

474 Christine Lyon and Melissa Crespo, *Employer Access to Employee Social Media: Applicant Screening, 'Friend' Requests and Workplace Investigations*, MORRISON & FOERSTER LLP (Mar. 17, 2014), http://media.mofo.com/files/Uploads/Images/140317-Employee-Social-Media.pdf.

475 *Id.*

476 *Id.*

477 961 F. Supp. 2d 659, 671 (D.N.J. 2013).

478 The employee who had become Facebook "friends" with her coworkers was terminated after one of her coworkers took screenshots of a post in which she criticized Washington, D.C., paramedics for saving the life of an 88-year-old white supremacist after he opened fire in the Holocaust museum. *Id.* at 663.

479 *Id.* at 669. Similarly, in Roberts v. CareFlite, No. 02-12-105-CV, 2012 WL 4662962 (Tex. Ct. App. Oct. 4, 2012), an employee was terminated after she publicly posted that she wanted to "slap" an unruly patient. *Id.* at *1. The employee alleged that her employer invaded her privacy by reading her posts but was unable to present any evidence that her employer invaded her privacy by terminating her based on her public posts. *Id.* at *5.

medical conditions, marital status, or other lawfully-protected (yet frowned upon) conduct.[480] For example, in *Gaskell v. Univ. of Kentucky,* the court held that an employee's discriminatory failure-to-hire claim could proceed at summary judgment where the employer had knowledge of the candidate's religious faith learned through social media screening.[481]

The National Labor Relations Board (NLRB) has ruled on issues arising in the context of social media monitoring in the unionized workplace. In *Three D, LLC*, the NLRB set a high bar for employers before they can terminate employees based on online speech and determined that "liking" a post constitutes protected dialogue.[482] Two employees were terminated after their employer viewed a Facebook exchange that was highly critical of the employer. In finding for the employee, the NLRB found a key provision in the employer's social media policy to be overbroad.[483]

In another decision, the NLRB concluded that Costco was in violation of the National Labor Relations Act (NLRA) by maintaining and enforcing a rule prohibiting employees from electronically damaging the company or any employee's reputation.[484] The NLRB stated that a violation is dependent upon a showing that: (1) employees would reasonably construe the language to prohibit protected activity under Section 7 of the NLRA; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights.[485] Using this analysis, the NLRB disregarded the employer's intent not to apply the policy to protected activity, and effectively questioned any policy that states that employees can be disciplined or fired for social media posts, stating that these policies are overbroad.[486]

---

480 Melissa M. Crespo and Christine E. Lyon, *Social Media Can Be An Employer's Friend Or Its Foe*, L.A. DAILY J. (Jul. 29, 2014), *available at* http://www.mofo.com/~/media/Files/Articles/140729SocialMediaCanBe.pdf.

481 Civ. A. No. 09-244-KSF, 2012 WL 2867630, at *7–*9 (E.D. Ky. Nov. 23, 2010).

482 Three D, LLC, 361 N.L.R.B. No. 31 (2014). The case is listed on the NLRB website as *Triple Play Sports Bar*. https://www.nlrb.gov/cases-decisions/board-decisions?volume=361&=Apply.

483 "An employer rule is unlawfully overbroad when employees would reasonably interpret it to encompass protected activities." Three D, LLC, 361 NLRB No. 31, at 7 (2014).

484 Costco Wholesale Corp. *et al.*, 358 NLRB No. 106, at 1101 (2012).

485 *Id.*

486 *Id.*

SIDE BAR – WORKPLACE PRIVACY

Navigating the legal framework, policies, and best practices applicable to workplace privacy and technology in the workplace can be challenging for both employers and employees alike. Employers are well-advised to follow these best practices:

Employers should ensure that hiring practices comply with governing state technology monitoring and privacy laws. Both employers and employees should understand the restrictions imposed by applicable state privacy laws and should draft policies that are in accordance with their jurisdictional requirements.

Employers should implement strict guidelines to mitigate risks. Employers should ensure that all levels of management understand the legal and ethical guidelines imposed by their respective jurisdictions and corporate programs, and should allow for transparency about the programs in order to facilitate compliance and bolster employee trust.

Employers should provide sufficient notice about monitoring practices to employees. Both current employees and job candidates should be provided with sufficient notice about the monitoring technologies that are utilized and employers should ensure that employees are reminded when new technologies replace their current systems.

VIII. STUDENT PRIVACY

For institutions that receive federal funding, privacy protections are afforded under U.S. law to educational records, including grades, disciplinary actions, and other school information about a particular student. The following federal laws govern the privacy protections for education records.

A. Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA)[487] was enacted to protect the privacy of student education records by limiting the transferability of those records without "eligible student" or parental consent. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

1. Overview

FERPA prohibits educational entities from releasing or providing access to "any personally identifiable information in education records" without the written consent of a parent.[488] The regulation implementing FERPA provides that personally identifiable information includes:

- the student's name;
- the name of the student's parent or other family members;
- the address of the student or student's family;
- a personal identifier, such as the student's social security number, student number, or biometric record;
- other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and
- information requested by a person the school reasonably believes knows the identity of the student to which the educational record is linked.[489]

---

[487] 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

[488] 20 U.S.C. § 1232g(b)(2).

[489] 34 C.F.R. § 99.3.

For the purposes of FERPA, the term "education records" is broadly defined as those records, files, documents, and other materials which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution, or by a person acting for such agency or institution.[490] However, an educational institution is allowed to disclose "directory information" if it has given public notice to parents of students in attendance and eligible students in attendance at the institution of: (1) the types of PII the institution has designated as directory information; (2) the right to refuse to let the institution disclose any or all of those types of information about the student; and (3) the period of time to notify the institution in writing that he or she does not want any or all of those types of information about the student designated as directory information.[491] In addition, educational institutions may disclose directory information of former students regardless of notice, provided that they honor valid opt-out requests made while the student was enrolled.[492]

FERPA rights initially belong to the parent/guardian of a student. When a student either turns 18 or attends an institution of post-secondary education, FERPA rights transfer from the parent to the student. At the college level, FERPA rights always belong to the student, regardless of age.

2. Consent Requirements and Exceptions

As a general rule, FERPA provides that no funds shall be made available to any educational agency or institution with a policy or practice of releasing educational records without written consent.[493] This written consent must be signed and dated by the eligible student or parent, and must indicate which records are to be released, the purpose of the release, and to whom the records are to be released.[494] The eligible student or parent may also request a copy of the records to be disclosed.[495]

Written consent is not required, however, to release educational records to certain categories of recipients, including:[496]

---

490 20 U.S.C. § 1232g(a)(4)(A). The following records are not considered "education records" under FERPA: (a) campus police records; (b) employment records; (c) treatment records (i.e., health records that are created or maintained by a professional health practitioner for the purpose of treating a student, and not disclosed to anyone except those providing the treatment); (d) applicant records of those who are not enrolled in the university; (e) alumni records created by the school after the individual is no longer a student; and (f) grades on peer-graded papers before they are collected and recorded by a faculty member or other university representative.

491 34 C.F.R. § 99.37(a). Directory information is "a type of personally identifiable information not usually considered harmful [or an invasion of privacy] if disclosed." It includes, but is not limited to, the student's name; address; telephone number; email address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance (e.g., academic years, semesters, or quarters when enrolled); degrees, honors, and awards received; and the most recent educational agency or institution attended. *Id.* at § 99.3.

492 *Id.* at § 99.37(b).

493 20 U.S.C. § 1232g(b)(1).

494 34 C.F.R. § 99.30.

495 *Id.* at § 99.30.

496 *Id.* at § 99.31(a).

- certain officials, including school officials and officials of schools where a student intends to enroll;
- accrediting organizations or organizations conducting certain types of studies;
- parents; or
- victims of certain offenses, limited to the final results of the relevant disciplinary proceeding.

In addition, disclosure can be made without consent when it is:

- in connection with financial aid applications or awards;
- to comply with a judicial order or subpoena;
- in connection with a health or safety emergency;
- in connection with a disciplinary proceeding at a postsecondary educational institution;
- related to sex offenders and the information was provided to the educational institution under applicable federal guidelines; or
- directory information.[497]

Finally, written consent is not required when the educational records have been de-identified such that all PII has been removed and the educational institution has made a reasonable determination that the student's identity is not identifiable.[498]

3. Intersection with COPPA

As educational institutions increasingly begin to rely on web-based technologies for their students, notice and consent issues can arise that may have implications under the Children's Online Privacy Protection Act (COPPA). Enacted in 1998, COPPA grants the FTC the authority to govern the controls around the online collection of information from children younger than thirteen years old.[499] Acknowledging that some concerns related to this collection can arise in a classroom environ-

---

[497] *Id.* at § 99.31(a).

[498] *Id.* at § 99.31(b).

[499] 15 U.S.C. §§ 6501–6505. For additional details concerning COPPA, *see supra* Section IV.A.2.

ment, the FTC included a section on "COPPA and Schools" in its published series of FAQs concerning the regulation.[500] In essence, the FTC advised that under certain circumstances a web-based service provider who is acting for a specific educational purpose on behalf of and at the direction of an educational institution may accept the institution's representation that consent has been obtained from the child's parent when it collects personal information.

The service provider must provide the school with all of the notices required under COPPA, and, upon request from the school, provide information concerning the type of personal information being collected and how it will be used, and give the school the opportunity to delete any provided information and/or limit its use by the service provider.[501] This exchange of information does not eliminate any notification obligations outlined under FERPA, or the Protection of Pupil Rights Amendment (PPRA), as discussed below.

4. Right of Access

FERPA provides students with the right to access and review their education records. Once a student has issued the request, the educational institute must provide access to the records within 45 days of that request.[502] It also must respond to reasonable requests from students for explanation of the records.

Students, however, do not have the right to inspect the financial records of their parents, confidential letters of recommendation, treatment records, attorney-client privileged information, or records excluded from the definition of education records (i.e., law enforcement records). Also, when the request pertains to a record containing information about more than one student, the requesting students may access only the parts pertaining to themselves.[503]

5. Enforcement

In 2002, the Supreme Court held that FERPA does not create a private right of action that can be enforced through 42 U.S.C. § 1983.[504] Rather than file a lawsuit, parents or eligible students who wish to allege a FERPA violation may instead file a written complaint with the Family Policy Compliance Office (FPCO). This complaint must be filed within 180 days from the time when the violation was known or reasonably should have been known to the complainant, and it must provide specific allegations.

---

500 *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (Mar. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools.

501 *Id.*

502 34 C.F.R. § 99.10.

503 *Id.* at § 99.12(a); 20 U.S.C. § 1232g(a)(1)(A).

504 Gonzaga Univ. v. Doe, 536 U.S. 273 (2002).

Upon initiating an investigation, the FPCO will issue a notice to the complainant and educational agency or institution involved outlining the allegations and requesting a written response from the educational agency or institution. After it completes its investigation, the FPCO will issue written findings. If a violation is found to have occurred, the FPCO may require corrective action such as policy revisions or training. The complaint is closed when the educational agency or institution has completed the corrective action.

B. Protection of Pupil Rights Amendment

The Protection of Pupil Rights Amendment (PPRA),[505] which is complementary to FERPA, was enacted to protect the rights of parents and students in the collection of student personal information by schools in connection with federally funded surveys and survey-related instructional materials. Whereas FERPA requires schools to protect the confidentiality of certain student information, the PPRA is intended to prevent schools and third parties from learning certain information about students.[506]

The PPRA protects the collection of student information in two ways:

1) It seeks to ensure that schools and their contractors make all instructional materials related to surveys, analysis, or evaluations in which their child is to participate available for inspection by parents or guardians.

2) It seeks to ensure that parents provide schools and their contractors with written parental consent of a minor student before the student is required to participate in any survey, analysis, or evaluation that reveals information concerning:

    a) political affiliations or beliefs of the student or the student's parent;

    b) mental or psychological problems potentially embarrassing to the student or the student's family;

    c) sex behavior or attitudes;

    d) illegal, anti-social, self-incriminating, and demeaning behavior;

    e) critical appraisals of other individuals with whom respondents have close family relationships;

    f) legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;

---

505 20 U.S.C § 1232h; 34 C.F.R. Part 98.

506 The PPRA defines "student" as any elementary school or secondary school student. Thus, the PPRA does not apply to post-secondary educational institutions. 20 U.S.C. § 1232h(c)(6)(F).

g) religious practices, affiliations, or beliefs of the student or student's parent; or

h) income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).[507]

For the purposes of the PPRA, the term "instructional material" is broadly defined as instructional content that is provided to a student, regardless of its format, including printed or representational materials, audio-visual materials, and materials in electronic or digital formats. The definition does not include academic tests or academic assessments.

1. Parental Rights

The PPRA requires educational institutions that receive funding under any applicable Department of Education program to develop and adopt local policies, in consultation with parents, regarding:

- the parent's or guardian's right to inspect (and in some cases opt out of) surveys created by a third party or any instrument used in the collection of personal information before they are administered or distributed to a student, and beyond those surveys or instructional materials for which affirmative consent is required;[508]

- the parents' right to inspect any instructional material, in addition to those in federally funded programs and used as part of the educational curriculum for the student;[509]

- advance notice and an opportunity to opt out of certain non-emergency, invasive physical examinations or screenings to be administered to a student;[510]

---

[507] 20 U.S.C. § 1232h(b).

[508] *Id.* at § 1232h(c)(1)(A)(i); *id.* at § 1232h(c)(1)(F)(i).

[509] *Id.* at § 1232h(c)(2)(C)(i).

[510] *Id.* at § 1232h(c)(2)(C)(iii).

- advance notice and an opportunity to opt out of the collection, disclosure, or use of personal information[511] collected from students for the purpose of marketing or for selling that information.[512]

The general notice of rights under the PPRA may include specific local policies, as described in the Model Notification of Rights Under the Protection of Pupil Rights Amendment. Notices of rights under the PPRA are available on the FPCO website.[513]

Parents are not required by the PPRA to be notified about the collection, disclosure, or use of personal information collected from students for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, students or educational institutions, such as:

- colleges or other post-secondary education recruitment, or military recruitment;
- book clubs, magazines, and programs providing access to low-cost literary products;
- curriculum and instructional materials used by elementary schools and secondary schools;
- tests and assessments used by elementary schools and secondary schools to provide cognitive, evaluative, diagnostic, clinical, aptitude, or achievement information about students (or to generate other statistically useful data for the purpose of securing such tests and assessments) and the subsequent analysis and public release of the aggregate data from such tests and assessments;

---

511 The PPRA defines "Personal Information" as individually identifiable information including:

(i) a student or parent's first and last name;
(ii) a home or other physical address (including street name and the name of the city or town);
(iii) a telephone number;
(iv) or a Social Security identification number.

Id. at § 1232h(c)(6)(E).

512 *Id.* at § 1232h(c)(1)(E).

513 Family Policy Compliance Office (FPCO), Model Notification of Rights Under the Protection of Pupil Rights Amendment (PPRA), and the PPRA Model Notice and Consent/Opt-Out for Specific Activities, are *available at* http://www2.ed.gov/policy/gen/guid/fpco/index.html, and http://www2.ed.gov/policy/gen/guid/fpco/hottopics/index.html.

- the sale by students of products or services to raise funds for school-related or education-related activities; and

- student recognition programs.[514]

The notification exceptions under the PPRA are not to be interpreted as preempting provisions of state law that require parental notification and do not apply to any physical examination or screening that is permitted or required under state law, including those examinations that are permitted without parental notification.[515]

2. Enforcement

Like FERPA, the PPRA provides no express private right of action. Instead, a student, parent, or guardian of a student directly affected by a violation of their rights under the PPRA may file a written complaint with the FPCO located within the Department of Education. This complaint must contain (1) specific allegations of fact that provide reasonable cause to believe that a violation has occurred, and (2) evidence of attempted resolution of the complaint at the local level (and at the state level if a state complaint resolution process exists), including the names of local and state officials contacted and significant dates in the attempted resolution process.[516] The FPCO investigates each complaint that it receives to determine whether the educational institution (recipient) or contractor failed to comply with the PPRA.[517]

After receiving a complaint, the FPCO issues a written notice to the complainant and the educational institution or contractor involved that describes the substance of the alleged violation and informs the educational institution or contractor that the FPCO will investigate the complaint. The recipient or contractor may then submit a written response to the complaint.[518] After it completes its investigation, the FPCO then issues written findings and the basis for its findings. If a violation is found to have occurred, the FPCO may require that specific corrective steps be taken and provide a reasonable period of time during which the educational institution or contractor may comply voluntarily.[519] The remedies available under the PPRA if the educational institution does not voluntarily comply are limited to the termination of federal funding.[520] If a contractor fails to voluntarily com-

---

514 20 U.S.C. 1232h(c)(4).

515 *Id.*

516 34 C.F.R. § 98.7.

517 *Id.*

518 *Id.* at § 98.8.

519 *Id.* at § 98.9.

520 *Id.* at § 98.10.

ply, a notice may be issued for the contractor to (i) suspend operations or (ii) to terminate for default. If no violation is found, written notice of the decision and the basis of the decision are provided to all parties involved.[521]

3. Proposed Legislation

On May 14, 2015, Senator David Vitter proposed significant amendments to section 444 of the General Education Provisions Act in an effort to improve privacy protections available to students and their parents.[522] Among other things, the proposed "Student Privacy Protection Act" seeks to strike a balance and insert language that defines "student data" with greater particularity. It also prohibits any school that receives federal funding from disseminating student data, including PII to third parties without (i) obtaining parental consent; (ii) providing 30 days' notice that the data is to be accessed and that it will only be available with consent; (iii) permitting parents to access the data; (iv) requiring that all student data be destroyed when the student is no longer a student; and (v) holding the third party liable for any violation.[523] The bill was reviewed and referred to the Committee on Health, Education, Labor and Pensions in May 2015 but has not been updated since.

C. State Laws

While the primary focus of this section has been on federal legislation concerning the privacy rights of students and protections over student personal information, it is important to note that many states have enacted or are in the process of enacting similar regulations. In 2015 alone, 14 states enacted such legislation, including Arkansas, Connecticut, Georgia, Louisiana, Maine, Maryland, Nevada, New Hampshire, North Dakota, Oregon, Texas, Utah, Virginia, and Washington.[524] Still other states, such as California, had previously adopted regulations concerning student privacy rights.[525] Because of the ever-evolving state of data protection regulations, it is advisable to refer to the current text of a state's statutes for the most up-to-date requirements for that given state or territory.

---

521 *Id.*

522 *See* S. 1341, 114th Cong. (2015).

523 *Id.*

524 *See U.S. State Education Privacy Legislation 2015*, INT'L ASS'N OF PRIVACY PROF'LS, *available at* https://iapp.org/resources/article/u-s-state-education-privacy-legislation-2015/ (information current as of 8/7/15).

525 *E.g.*, California's Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE § 22584; *see also* CAL. EDUC. CODE §§ 49060–49083.

SIDE BAR – STUDENT PRIVACY

Institutions receiving federal or state funding must remain aware of the complex scheme of regulations designed to protect student privacy.

Parental notice and consent is often the key to proper handling of student personally identifiable information. In most instances, this right transfers to the student when he or she turns eighteen (18) years of age, or enrolls in a post-secondary institution (regardless of his/her age).

Protected material can be broadly defined. Under FERPA, "education records" is broadly defined and, with limited exception, encompasses all files and material maintained by the institution that directly relate to a student. The PPRA extends protection to personal information that includes not only traditional identifiers like social security numbers, but also survey responses that may give insight into political beliefs, religious affiliation, or sex behavior or attitudes, among other topics.

Primary educational institutions need to take care with student information handled online. To remain in compliance with COPPA, FERPA, and the PPRA, the personally identifiable information of children younger than thirteen (13) years old should only be relayed to online service providers after the institution has properly obtained consent from the child's parent and has reviewed the notifications the online service provider will provide to users of its site.

IX. CONCLUSION

Privacy laws have evolved considerably over the past several decades, and today, there exists a complex patchwork of state and federal privacy laws in the U.S. Many of these laws are esoteric, presenting significant compliance challenges for organizations, as well as confusion among a wide variety of stakeholders, from practitioners to legislators to the judiciary. It is our hope that this Primer proves to be a useful resource on privacy laws as they exist today, providing an understanding of the key U.S. privacy laws, along with their applicability and general requirements.