CHAPTER 7:

INDIVIDUAL REMEDIES IN US PRIVACY LAW

[1] The US legal system provides numerous ways for an individual to remedy violations of privacy. I have sometimes encountered the view in the EU that the US lacks remedies for privacy violations generally. That is not correct. I am the lead author of the textbook for the International Association of Privacy Professionals (IAPP) for the certification exam on US private-sector privacy law.[1] We published the second edition in 2012, and we are now preparing publication of the third edition. With only an introductory overview of US privacy laws that apply to the private sector, including enforcement mechanisms, the second edition took nearly 200 pages and eleven chapters,[2] and the third edition will be longer. That book documents many aspects of US privacy law that do not fit in this Chapter.

[2] The large quantity of US privacy law sometimes leads to a different critique from the EU: that US remedies are "fragmented" and may for that reason not be adequate under EU standards. This Chapter aims to help explain how the different pieces of US law fit together. The complexity of US law in part comes from the fact that more than one source of enforcement can exist for any given privacy issue. This division of authority can be beneficial for privacy protection, as it allows subject matter experts to enforce in areas they understand best, allows multiple agencies to police categories of activity on behalf of data subjects, and also allows private rights of action for individuals.

[3] Scholars have noted the breadth of remedies available to individuals in the US and their impact on the privacy-protecting behaviors of US companies. Professors Kenneth A. Bamberger and Deirdre K. Mulligan's book *Privacy on the Ground* studied corporate behavior in five countries, and found that US companies often have stronger privacy management practices.[3] Professor Danielle Citron's award-winning article *The Privacy Policymaking of State Attorneys General* similarly shows how the work of state Attorneys General (AGs) in the US serve as "laboratories of privacy enforcement."[4] Citron explains how state AGs can take a more nimble approach to privacy enforcement than a single federal enforcement agency, allowing them to respond faster to concerns raised in the press or by the public.[5] The multiple US privacy laws have a strong influence, in my view, on the practices of US companies, who face enforcement actions if they do not have effective compliance with the law and their stated privacy policies.[6]

---

[1] PETER SWIRE & KENESA AHMAD, U.S. PRIVATE SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS (2012) [hereinafter SWIRE & AHMAD, U.S. PRIVATE SECTOR PRIVACY]. The same year, we published a book providing an introduction to privacy globally. PETER SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS, AND PRACTICES (2012).

[2] *Id.*

[3] *See generally* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015).

[4] Danielle Keats Citron, *Privacy Policymaking of State Attorneys General*, NOTRE DAME L. REV. (forthcoming) (manuscript at 1), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297.

[5] *Id.* (manuscript at 4).

[6] *See, e.g.*, GOOGLE, *Privacy Policy*, https://www.google.com/policies/privacy/ (last updated Aug. 29, 2016) ("We will share personal information with companies, organizations, or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to: meet any applicable law, regulation, legal process or enforceable governmental request"); MICROSOFT, *Privacy Statement*, https://privacy.microsoft.com/en-US/privacystatement (last updated Sep. 2016) ("We share your personal data . . . when required by law or to respond to legal process"); TWITTER, *Privacy Policy*, https://twitter.com/privacy?lang=en (last updated Sep. 30, 2016) ("[W]e may preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation, legal process, or governmental request.").

[4] This Chapter outlines the steps an aggrieved individual, whether in the US or in the EU, may take in response to concerns regarding US privacy violations. Section I examines individual judicial remedies against the US government. These remedies feature two recently-finalized agreements with the EU, the Privacy Shield and the Umbrella Agreement, as well as the Judicial Redress Act whose passage the EU strongly supported. It next examines the civil and criminal remedies that exist where individuals, including government employees, violate the wiretap and other surveillance rules under laws such as the Stored Communications Act, the Wiretap Act, and the Foreign Intelligence Surveillance Act.

[5] Section II examines non-judicial remedies available to individuals concerned about US government actions. I highlight three paths — the Privacy and Civil Liberties Oversight Board, Congressional committees, and recourse to the US free press and privacy-protective non-government organizations. Both US-persons and EU persons can benefit from the ability to make complaints in these ways, and gain a multiplier effect as the agency, Congressional committee, or privacy advocacy organization takes up the cause.

[6] Section III examines individual remedies against US companies, such as service providers of webmail and social networks, should they improperly disclose information to the US government about customers. It then examines privacy enforcement by five federal administrative agencies, including the Federal Trade Commission (FTC) and Federal Communications Commission (FCC). These administrative agencies do not themselves bring actions against intelligence agencies. They can be important, however, because they can bring actions against companies that fail to comply with applicable law or company privacy policies, such as when the companies improperly provide electronic communications to the government.

[7] Section IV introduces privacy enforcement under state law and private rights of action. Each state has an Attorney General tasked with protecting consumers. As documented by Professor Citron, these AGs have emerged as important privacy enforcers. It then examines the numerous private rights of action that exist under US law, using the state of California as one example. These lawsuits on behalf of individuals are a well-known feature of US law. During negotiation of the Safe Harbor in 1999-2000, I heard US Ambassador David Aaron, the lead US negotiator, say more than once to EU negotiators: "We'll take your privacy laws if you'll take our plaintiffs' lawyers." The prevalence of plaintiffs' lawyers and private rights of action in the US means that defendants (including companies and often government agencies) have increased incentive to comply strictly with applicable law.

[8] Section V examines issues of who has standing to sue in the wake of the 2013 US Supreme Court case of *Clapper v. Amnesty International USA*. Section VI offers conclusions.

[9] This chapter contains two Annexes. The first is a chart that lists US privacy remedies and safeguards, specifically noting those that are available to EU persons, and not only to US persons. The second is a chart detailing major privacy settlements in the US from 2006 through 2016. This chart illustrates the substantial magnitude of class action and agency enforcement, as discussed in Section IV of this chapter.

[10] Before turning to the individual remedies, I briefly discuss the intersection of individual remedies with the systemic safeguards discussed in Chapters 3, 4, and 5. Systemic safeguards have a notable advantage in creating limits on intelligence agencies – oversight agencies can gain access to classified information, and methodically examine otherwise-secret agency practices. In the US, oversight actors with access to classified information include the Foreign Intelligence Surveillance Court, the PCLOB, agency Inspectors General, the Senate and House Intelligence Committees, and other bodies such as the Review Group on which I served. With access to the classified information, these actors can detect privacy problems and take action to correct them. By contrast, as discussed in Chapter 8, there is a caveat to the desirability of individual remedies – there are reasons to be cautious about disclosing national security secrets in open court or to an individual who may be probing the intelligence system rather than honestly seeking to correct a privacy violation.

[11] As a related point, systemic safeguards can more specifically bolster or parallel individual remedies. For example, the US system of foreign intelligence law places surveillance authorization in the hands of a court – the Foreign Intelligence Surveillance Court engages in a specific proceeding, determining whether surveillance satisfies statutes and the Constitution.[7] The rules for Section 702 collection require data acquired as a result of a compliance incident to be purged, as would occur through a successful individual deletion request.[8] Transparency mechanisms, such as governmental or corporate transparency reports, provide information about the scope of government surveillance programs akin to what individual information requests may seek.[9] The US system of foreign intelligence safeguards thus reinforces the individual remedies discussed in this Chapter in the interest of protecting the rights those remedies seek to vindicate.

I. Individual Judicial Remedies against the US Government

[12] In the US, persons who suffer a privacy harm can seek remedies in both civil and criminal cases. This section focuses on actions that an individual can bring in state or federal courts in the US. Section II below addresses multiple administrative/regulatory processes that can be undertaken to respond to assertions of privacy related issues. This subsection first discusses civil actions an individual can take, focusing on civil remedies available against the US government,[10] and then provides a parallel analysis for remedies through criminal proceedings. It also responds to specific critiques of US privacy remedies by the Irish Data Protection Commissioner.

---

[7] *See* Chapter 3, Section III(A). An interlocking system of audits and reporting provides the Foreign Intelligence Surveillance Court (FISC) with notices of compliance incidents, and the FISC has responded strongly to compliance incidents. *See* Chapter 5, Section II(A).

[8] In Section 702 collection, "[i]f the data was acquired as a result of a compliance incident," such as a "typographical error" or "an overproduction by the provider," the "acquired communications must be purged." PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 49 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf.

[9] For an extensive discussion on transparency safeguards in US surveillance law, *see* Chapter 3 ("Systemic Safeguards in the US System of Foreign Intelligence Surveillance Law").

[10] Under US law, litigation can be conducted against the government itself as well as actors acting "under the color of governmental authority," such as contractors hired to conduct surveillance or otherwise act on the government's behalf. *See, e.g.*, 42 U.S.C. § 1983 ("Every person who, under color of any statute, ordinance, regulation, custom, or usage . . . shall be liable").

A. US Civil Judicial Remedies

[13] Civil suits allow qualifying individuals, including EU persons, to sue the US government for violations of law that can result in monetary damages and injunction of ongoing illegal actions. Unlike criminal violations of law, which must be prosecuted by an agent of the government, any qualifying individual can bring a civil suit as long as he or she meets the thresholds required for the alleged wrongful act.[11] Likewise, certain administrative agencies can also seek civil penalties for violations of US law and regulations. While the US, like most sovereigns, generally reserves immunity from suit, the US government has waived that sovereign immunity by statute in circumstances that are relevant to redress of individual privacy concerns.[12]

1. Judicial Redress Act, Privacy Shield, and the Umbrella Agreement

[14] The Judicial Redress Act, the EU-US Privacy Shield, and the Data Protection and Privacy Agreement (i.e., the Umbrella Agreement) combine to provide new individual legal remedies for EU persons who believe they have suffered privacy harms, in addition to those specified by the Standard Contractual Clauses (SCCs) themselves.

[15] Under the Judicial Redress Act,[13] the US expressly extended the right to a civil action against a US governmental agency to obtain remedies with respect to the willful or intentional disclosure of covered records in violation of the Privacy Act to qualified individuals.[14] The Judicial Redress Act also extends the right to a civil action against a designated US governmental agency or component when that agency or component declines to amend the record in response to a qualifying individual's request.[15] A qualifying individual is one who has been subject to improper response to a request from a US agency.[16] The Act allows US and qualifying non-US persons to sue a US federal agency for the improper handling of their data; to obtain injunctions

---

[11] *See, e.g.*, 18 U.S.C. § 2707(a) ("[A]ny provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter . . . may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation"); 18 U.S.C. §2520(a) ("[A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity").

[12] *See, e.g.*, 5 U.S.C. § 552a(g)(1) (permitting civil action against a US federal agency which violates the statute).

[13] Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (2015), https://www.congress.gov/bill/114th-congress/house-bill/1428/text (codified at 5 U.S.C. § 552a).

[14] *Id.* at § 2(a) ("With respect to covered records, a covered person may bring a civil action against an agency and obtain civil remedies, in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an individual may bring and obtain with respect to records under: (1) section 552a(g)(1)(D) of title 5, United States Code, but only with respect to disclosures intentionally or willfully made in violation of section 552a(b) of such title; and (2) subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code, but such an action may only be brought against a designated Federal agency or component.").

[15] *Id.* (citing the availability of civil action under subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code, which reads: "Whenever any agency (A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection; (B) refuses to comply with an individual request under subsection (d)(1) of this section . . . the individual may bring a civil action against [a designated Federal agency or component].").

[16] *Id.*

or monetary damages; and to review, copy, and request amendments to their data.[17] In contrast to some of the statutes discussed below, these suits are brought against the agency itself rather than against an individual actor within the agency.[18]

[16] Prior to the passage of the Judicial Redress Act in 2016, an action under the Privacy Act could be brought only by "US persons," who are US citizens or non-citizen permanent residents. Under the Judicial Redress Act, non-US persons may bring a cause of action listed under the Privacy Act if the US Attorney General, in consultation with the Secretaries of State, Treasury, and Homeland Security, designates that the non-US person's country of citizenship "has entered into an agreement with the United States that provides for appropriate privacy protections" and that the country permits the transfer of personal data for commercial purposes to the US.[19] Although EU member states have not to date been individually identified as required under the Judicial Redress Act, my understanding is that the EU and US plan to finalize that process.

[17] Under the EU/US Privacy Shield, the US has created new remedies against the US government available to EU persons. For complaints concerning US government actions, EU data subjects can lodge a complaint with an Ombudsman within the Department of State.[20] The Ombudsman will respond to individuals who file complaints related to the Privacy Shield and inform them whether or not the laws relevant to their situation have been violated.[21] Importantly, this Ombudsman is independent from US national security services.[22] The Ombudsman can be used to process "requests relating to national security access to data transmitted from the EU to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs) [and] binding corporate rules (BCRs)."[23] Indeed, the US and the EU Commission have made clear that the Ombudsman mechanism "is not Privacy Shield specific" and "covers all complaints relating to all personal data and all types of commercial transfers from the EU to companies in the US."[24] Any

---

[17] *Id.* (citing 5 U.S.C. § 552a); see also 5 U.S.C. §§ 552a(g)(2)(A)-(B) (providing that in any suit under 5 U.S.C. § 552a(g)(1), "the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct" and that "[t]he court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed").

[18] *Id.* ("[S]uch an action may only be brought against a designated Federal agency or component").

[19] Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282, § (d)(1) (2015). https://www.congress.gov/bill/114th-congress/house-bill/1428/text.

[20] European Commission Press Release MEMO/16/434, EU-U.S. Privacy Shield: Frequently Asked Questions (Feb. 29, 2016), http://europa.eu/rapid/press-release_MEMO-16-434_en.htm. Note that, as of today, this mechanism is still being organized and is not yet available. *See* PRIVACY SHIELD FRAMEWORK, *How to Submit a Request Relating to U.S. National Security Access to Data* (Oct. 9, 2016), https://www.privacyshield.gov/article?id=How-to-Submit-a-Request-Relating-to-U-S-National-Security-Access-to-Data.

[21] European Commission Press Release, *supra* note 20.

[22] *Id.*

[23] European Commission, Annexes to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, C(2016) 4176 final at 52 (July 12, 2016) [hereinafter "Annexes"], http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf. Note that the Ombudsman can also review requests submitted in response to data transmitted from the EU to the US under derogations and possible future derogations.

[24] European Commission Directorate General for Justice and Consumers, *European Commission Guide to the EU-U.S. Privacy Shield*, at 19 (2016), http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf.

written commitments from the Ombudsman in response to individual inquiries will also be published in the US Federal Register, offering transparent evidence of review.[25]

[18] Individuals in the EU have multiple methods for redress against companies, rather than the US government, for privacy complaints. First, individuals can invoke, free of charge, an independent alternative dispute resolution (ADR) body to handle any complaints against US Privacy Shield companies.[26] Information on and a link to the ADR must be provided on the company's website, and the ADR must be able to "impose effective remedies and sanctions" in response to valid complaints.[27] Second, individuals can file a complaint with an EU Data Protection Authority (DPA), which have their existing enforcement powers today under national law and will gain additional enforcement powers when the General Data Protection Regulation goes into effect in 2018.[28] The Privacy Shield also allows US companies to opt for using an EU DPA as its independent recourse mechanism, and DPA oversight is mandatory when a company handles personnel data transfers from the EU to the US. Individual complaints to the DPA can result in advice delivered to the company and made public to the extent possible. Third, if the company fails to comply with the DPA's advice within 25 days, the DPA may refer the issue to the Federal Trade Commission (FTC) for enforcement. Under Section 5 of the FTC Act, the Commission can bring an enforcement action for a "deceptive" practice if the company promises to comply with Privacy Shield but fails to do so. Fourth, if the company fails to comply with the DPA's advice within 25 days, the DPA may also refer the matter to the Department of Commerce to determine if the company's non-compliance should result in removal from the Privacy Shield List.[29]

[19] The Umbrella Agreement provides remedies for EU citizens whose data is transferred to US law enforcement authorities. Any individual will be entitled to access their personal information – subject to certain conditions, given the law enforcement context – and request corrections if it is inaccurate.[30] Similarly, individuals are entitled to seek correction or rectification of personal information that they assert is either inaccurate or improperly processed.[31] If the petition for access, correction, or rectification is denied or restricted, the authority must provide an explanation of the basis for its denial "without undue delay."[32] The Agreement provides that, if

---

[25] *Id.* The Federal Register is an official record of US government actions, available at https://www.federalregister.gov.

[26] Annexes, *supra* note 23, at 19; *European Commission Guide to the EU-U.S. Privacy Shield*, *supra* note 24, at 12.

[27] *European Commission Guide to the EU-U.S. Privacy Shield*, *supra* note 24, at 15.

[28] *See* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art. 70, 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1476055364678&uri=CELEX:32016R0679 (outlining the tasks of the newly established Data Protection Board under the Directive).

[29] *Id.*

[30] *See* European Commission Proposal for a Council Decision on the conclusion, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses at 10-12, COM (2016) 237 final (Apr. 29, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1476055815798&uri=CELEX:52016PC0237.

[31] *Id.*

[32] *Id.*

the US authority denies a request, the EU citizen may seek judicial review of that decision.[33] An EU citizen may also petition for judicial review of alleged willful or intentional unlawful disclosure of his or her information, for which the court may award compensatory damages where appropriate.[34] The US passed the Judicial Redress Act in part to fulfill this requirement of the Umbrella Agreement.[35]

[20] Standard Contractual Clauses, when implemented by a US company, also offer individual privacy remedies. Under Commission Decision C(2004)5721, "[e]ach party shall be liable to the other parties for damages it causes by any breach of these clauses" and to "data subjects for damages it causes by any breach of third party rights" under the SCCs.[36] Data subjects are also specifically empowered to enforce the SCCs as a third party beneficiary against the data importer or the data exporter with regards to that individual's personal data.[37] The importer and exporter both agree to allow such suit to be adjudicated in the data exporter's country of establishment.[38]

[21] Where a data subject alleges that the data importer has breached the SCCs, the subject is required to request that the data exporter enforce the data subject's rights against the importer.[39] If the data exporter does not take such action within a reasonable period (typically one month) then the data subject may proceed to enforce his or her rights against the data importer directly.[40] The data subject may also file suit against the data exporter in this case for failure "to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses."[41]

2. Electronic Communications Privacy Act – Stored Communications Act

[22] The Electronic Communications Privacy Act (ECPA) specifically creates an individual right of action for individual data subjects, including EU citizens. The Stored Communications Act (SCA) governs access to stored communications data. It provides individual remedies for data subjects whose stored communications data that has been unlawfully accessed or used by either an individual government actor or US agency as a private third party actor which accesses a network without authorization. The protections for access to an individual's stored data are not limited by citizenship and all remedies available under the Act are likewise available to EU citizens as well as US citizens.[42]

---

[33] *Id.* at 12.
[34] *Id.*
[35] *See* European Commission Press Release Memo/15/5612, Questions and Answers on the EU-US data protection "Umbrella agreement" (Sep. 8, 2015), http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.
[36] European Commission Decision C(2004)5217, Set II: Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers), http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_set_ii_c2004-5721.doc.
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] 18 U.S.C. § 2510(6) (defining "person" under the statute without restrictions based on citizenship); *see also Suzlon Energy v. Microsoft*, 671 F.3d 726, 730 (9th Cir. 2011),

[23] Under ECPA, different standards apply for judicial orders for US government access, depending on the type of data requested. The strictest of the applicable standards applies the Fourth Amendment's constitutional rule of probable cause of a crime as determined by an independent judge. That probable cause standard now applies to the stored content of electronic communications, including email.[43] Easier access is permitted to what historically has been called "pen register" and "trap and trace" information, the metadata about the communication. To access this dialing, routing, addressing, and signaling information, the government must certify to the judge that that the information likely to be obtained is relevant to an ongoing criminal investigation.[44] Fourth, basic subscriber information (e.g., account name, information provided during account creation) can be voluntarily disclosed to the government upon request, or can be obtained through other judicial process such as a grand jury subpoena.[45]

[24] For violations of these rules, the data subject may bring a civil suit against the agency and/or the individual, even if the data subject is not a US citizen.[46] Suits against both individual officers and US agencies must demonstrate that the violation of ECPA was "willful."[47] If a suit against an individual officer succeeds, the data subject may receive money damages of at least $1,000 USD, equitable or declaratory relief, reasonable attorney's fees, reimbursement of legal fees, and/or punitive damages.[48] The government employee found to have willfully or intentionally violated ECPA may also be subject to discipline for their actions.[49] Suits against a US agency may result in actual damages or $10,000 USD, whichever is greater, plus litigation costs.[50]

---

http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf ("Thus, the Court remains firm in its initial finding that the ECPA unambiguously applies to foreign citizens.").

[43] The statute itself applies varying standards for access to the content of an email, depending on factors such as whether the email has been opened and how old it is. 18 U.S.C. § 2703. Based on the Fourth Amendment, however, a federal appellate court held in the leading *Warshak* case that individuals have a reasonable expectation of privacy in the contents of an email, and that the relatively strict probable cause standard applies. *United States v. Warshak*, 631 F.3d 266, 274 (6th Cir. 2014), http://www.opn.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf. The US government has publicly stated that it seeks the content of an email under that probable cause standard. *See ECPA (Part 1): Lawful Access to Stored Content: Hearing before the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 14 (2013) (statement of Elana Tyrangiel, Acting Assistant Att'y Gen., Office of Legal Policy, Department of Justice), https://judiciary.house.gov/_files/hearings/printers/113th/113-16_80065.PDF.

[44] 18 U.S.C. §§ 3121-22.

[45] *Id.* §§ 2702-03.

[46] *Id.* § 2510; *see also Suzlon Energy v. Microsoft*, 671 F.3d 726, 730 (9th Cir. 2011), http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf.

[47] 18 U.S.C. § 2520. The civil provision requiring "willful" violation has exceptions for good faith reliance on court orders, grand jury subpoenas, legislative authorizations, statutory authorizations, or a valid request from an investigative or law enforcement officer. 18 U.S.C. § 2520(d). Similarly, there is no "willful" violation where the individual or agency being sued made a good faith determination that the alleged action was valid under ECPA. *Id.*

[48] 18 U.S.C. § 2707(c).

[49] *Id.* § 2707(d).

[50] 18 U.S.C. § 2712(a).

3. ECPA – The Wiretap Act

[25] Like the SCA, the Wiretap Act creates an individual right of action against unlawful government action.[51] The rules for getting a wiretap – a real-time interception of a data subject's communications – are even stricter than the usual probable cause standard. To get a wiretap, in addition to probable cause,[52] the government must meet a number of other standards, including seriousness of the crime[53] and an explanation of why the communications sought could not feasibly be obtained by other means.[54] Authorizations for wiretaps must be for a specific and limited time[55] and must include minimization of non-relevant information to protect the privacy of interceptees.[56] Continued surveillance outside that timeframe without separate judicial authorization is considered unlawful.[57]

[26] Additionally, an application under the Wiretap Act must be approved at the highest levels of the US Department of Justice (DOJ) before it is authorized for submission to a judge.[58] The Wiretap Act requires federal investigative agencies to submit requests for the use of certain types of electronic surveillance (primarily non-consensual interceptions of wire and oral communications) to the DOJ for review and approval before those requests may be submitted for judicial review.[59] The US Attorney General is tasked with reviewing and approving these requests, but is also allowed to delegate that authority to a limited number of high-level DOJ officials, including Deputy Assistant Attorneys General for the Criminal Division. These officials review and approve or deny requests for wiretaps[60] and to install and monitor electronic bugs (e.g., microphones).[61]

[27] As is the case with the SCA, the Wiretap Act provides remedies to data subjects whose communications have been unlawfully intercepted by the US government. Remedies under the Wiretap Act are, as with the SCA, available to EU data subjects.[62] Where an individual has "intentionally" violated the Act,[63] a data subject may be entitled to "appropriate relief."`[64] Relief

---

[51] The Wiretap Act is codified as Title I of ECPA, 18 U.S.C. §§ 2510–22.
[52] 18 U.S.C. § 2518(3)(a).
[53] *Id.*
[54] *Id.* § 2518(3)(c).
[55] *Id.* § 2518(4)(d).
[56] *Id.* § 2518(5).
[57] *Id.* ("Every order . . . shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter").
[58] *See* 18 U.S.C. § 2516(1).
[59] *Id.*
[60] *Id.* § 2510(1).
[61] *Id.* § 2501(2).
[62] *See id.* §§ 2510(6), 2510(11) (defining "person" and "aggrieved person" under the statute); *see also Suzlon Energy v. Microsoft*, 671 F.3d 726, 731 (9th Cir. 2011), http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf ("The ECPA protects the domestic communications of non-citizens."). Since The Wiretap Act is codified under ECPA, *Suzlon* likewise applies to available remedies under 18 U.S.C. § 2520.
[63] 18 U.S.C. § 2511(1)(a).
[64] 18 U.S.C. § 2520.

can include an injunction of the action if ongoing, monetary damages, and additional punitive damages where appropriate.[65]

4. Foreign Intelligence Surveillance Act

[28] The Foreign Intelligence Surveillance Act (FISA) provides individual remedies for data subjects against unlawful acts of individual government officers. If an individual officer conducts surveillance of a data subject without first obtaining statutory or Presidential authorization, misuses surveillance information, or unlawfully discloses surveillance information, that individual officer can be sued by the data subject in US court.[66] Authorizing statutes, such as Section 702 of FISA, provide additional restrictions and safeguards for surveillance activities. A data subject who succeeds in suing an individual for conducting unauthorized surveillance may receive actual damages of not less than $1,000 USD, statutory damages of $100 USD per day of unlawful surveillance, and the award of additional punitive damages and attorney's fees where appropriate.[67] As discussed in Chapter 5, the Foreign Intelligence Surveillance Court (FISC) has been diligent in policing agencies that attempt to circumvent its judicial orders, and conducts ongoing review of surveillance programs. Along with the existence of the individual statutory remedies, the FISC has made clear that failure to comply with its orders can result in the revocation of authorization for surveillance programs.[68] An aggrieved EU data subject may use the FISA cause of action as long as he or she is not a "foreign power" or an "agent of a foreign power."[69]

B. US Criminal Judicial Remedies

[29] In addition to allowing aggrieved individuals to bring civil suits against violators, the US DOJ can also bring criminal charges against any such violators under the SCA, ECPA, FISA, and the Privacy Act. Under the SCA, an individual who unlawfully accesses stored communications "for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act" is subject to a criminal fine, up to five years imprisonment, or both for a first offense.[70] For subsequent offenses, the penalty increases to criminal fines, up to ten years imprisonment, or both.[71] In any other case, a first offense carries a penalty of criminal fine and/or imprisonment up to one year, and subsequent offenses carry a penalty of criminal fine and/or imprisonment up to five years.[72] If a person knowingly makes unlawful use of a pen register or trap/trace device can also face a penalty of criminal fines, up to one year imprisonment, or both.[73] Under ECPA, a person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or

---

[65] *Id.* §2520(b). Unlike the SCA, the Wiretap Act does not expressly grant a waiver of sovereign immunity for suits against US agencies, but rather allows for suit only against individual officers who have intentionally violated the Act. *Id.* § 2511(1).
[66] 50 U.S.C. §§ 1801, 1810.
[67] *Id.* § 1810. Note that the individual may receive either actual damages not less than $1,000 USD or $100 USD per day of surveillance, but not both.
[68] *Id.*
[69] 50 U.S.C. § 1801(a)-(b) (defining foreign power and agent of a foreign power).
[70] 18 U.S.C. § 2701(b)(1)(A).
[71] *Id.* § 2701(b)(1)(B).
[72] *Id.* § 2701(b)(2).
[73] 18 U.S.C. § 3121(d).

electronic communication" can face criminal fines, up to five years imprisonment, or both.[74] The same penalty applies to individuals who unlawfully use or disclose the contents of any wire, oral, or electronic communication.[75] Under FISA, a person who intentionally engages in unauthorized "electronic surveillance under color of law" or knowingly "discloses or uses information obtained under color of law by [unauthorized] electronic surveillance" can face a criminal fine, up to five years imprisonment, or both.[76] Under the Privacy Act, any officer or employee who uses his employment or official position to knowingly and willfully engage in prohibited disclosure of individually identifiable information "in any manner to any person or agency not entitled to receive" can be found guilty of a misdemeanor and fined up to $5,000.[77] These criminal penalties serve as an alternative means of redress for violations of a data subject's privacy rights. The US has strongly committed to effective enforcement of violations of privacy law, as demonstrated in the Judicial Redress Act, the Umbrella Agreement, and the Privacy Shield Framework.[78] Based on those commitments, the US DOJ would take any criminal-level violation of these laws seriously, as well as any request from the EU for criminal enforcement. In particular, the Ombudsman mechanism created by the Privacy Shield Framework demonstrates the US's commitment to cooperation with EU authorities regarding privacy violations.

[30] Along with the affirmative use of the criminal law against violations of privacy laws, I briefly discuss two areas where individuals, including EU citizens, have important rights in criminal prosecution. First is the exclusionary rule. As discussed elsewhere in my materials, the data subject has the ability in criminal cases to suppress unlawfully obtained evidence that the US government seeks to use in court.[79] US courts will not only bar illegally obtained evidence, but will also bar evidence acquired as a result of the illegal search or seizure.[80] If the suppression of illegally obtained evidence leaves the prosecutor without enough facts in evidence to meet the elements of the crime alleged, the case may then be dismissed.[81] Any objection to illegally obtained evidence during trial can later be appealed even if the accused is convicted, allowing for additional, independent judicial review of the government's actions.[82] These remedies are available to all persons facing criminal charges in US court, including EU persons.

---

[74] 18 U.S.C. §§ 2511(1)(a), 2511(4)(a).
[75] *Id.* § 2511(1).
[76] 50 U.S.C. §§ 1809(a), 1809(c).
[77] 5 U.S.C. § 552a(i)(1).
[78] *See* Council Decision (EU) No. 2016/920 of 20 May 2016 on the signing, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, 2016 O.J. (L 154) 1; *see also* PRIVACY SHIELD FRAMEWORK, *Recourse, Enforcement and Liability*, https://www.privacyshield.gov/article?id=7-RECOURSE-ENFORCEMENT-AND-LIABILITY; Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (2015).
[79] *See* Chapter 4; *see also* 18 U.S.C. § 2518(10)(a); *United States v. Warshak*, 631 F.3d 266, 282-89 (6th Cir. 2014) (noting that evidence acquired under the Stored Communications Act without a warrant is subject to the exclusionary rule).
[80] *Wong Sun v. United States*, 371 U.S. 471 (1963), https://scholar.google.com/scholar_case?case=13688369940584894086&hl=en&as_sdt=6&as_vis=1&oi=scholar.
[81] FED. R. CRIM. P. 29 ("After the government closes its evidence or after the close of all evidence, the court on the defendant's motion must enter a judgment of acquittal of any offense for which the evidence is insufficient to sustain a conviction.").
[82] FED. R. EVID. 103 (explaining how a party can preserve the right to appeal a ruling to admit or exclude evidence at trial).

[31] The Classified Information Procedures Act (CIPA) also provides a specific mechanism for allowing criminal defendants to access classified materials at trial that may be helpful to the defense.[83] As with other individual remedies available for individuals who are accused of a crime, CIPA protects the right of an individual to due process in a criminal proceeding. I discuss CIPA and its procedures in greater detail in Chapter 8 (Individual Remedies, Hostile Actors, and National Security Considerations).[84]

II. Non-Judicial Individual Remedies in the US against the US Government

[32] In addition to judicial remedies, there are important administrative, legislative, and public channels for data subjects to seek redress for privacy harms by the US government. This section examines specific avenues for such complaints and the relevant actions each entity may take in response to such a complaint. I highlight three such channels: the PCLOB; Congressional committees; and recourse to the free press and privacy-protective non-government organizations. Both US and EU persons can benefit from the ability to make complaints in these ways, and gain a multiplier effect as the agency, Congressional committee, or privacy advocacy organization takes up the cause.

A. The Privacy and Civil Liberties Oversight Board (PCLOB)

[33] The PCLOB, discussed in greater detail in Chapter 3, is an independent agency within the US government's executive branch with oversight authority over US intelligence practices, and the ability to respond to individual complaints. The PCLOB has extensive investigative powers, including access to necessary classified information. The PCLOB provides contact information to the public, and any person may submit concerns regarding US intelligence practices. The PCLOB has published lengthy reports on US intelligence procedures, including the numerous recommendations for reform of practices under Section 702, discussed in Chapter 3.[85] An EU data subject or DPA is free to contact the PCLOB and lodge a complaint or request for further investigations.

B. Congressional Committees

[34] The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence are discussed in greater detail in Chapter 3. Using their oversight authority, the Committees can investigate individual complaints from US and EU data subjects. These Committees were created to "oversee and make continuing studies of the intelligence activities and programs of the United States Government," and "provide vigilant legislative oversight over the intelligence activities of the United States to assure that such activities are in conformity with the Constitution and laws of the United States."[86] As with the PCLOB, members of the committees

---

[83] 18 U.S.C. app. §§ 1-16.
[84] Chapter 8, Section IV ("US Criminal Proceedings under the Classified Information Procedures Act").
[85] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 134-148 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf.
[86] U.S. SENATE SELECT COMMITTEE ON INTELLIGENCE, *Overview of the Senate Select Committee on Intelligence: Responsibilities and Activities*, SENATE.GOV, http://www.intelligence.senate.gov/about.

and staff obtain top-secret clearances as necessary to conduct their oversight. Senate and House Judiciary committees play a similar oversight role for criminal law, as opposed to intelligence law. Individuals and DPAs can report their concerns to the relevant congressional committees and request follow-up investigations.

C. Individual Remedies through Public Press and Advocacy

[35] The free press of the US can serve as an important remedy for persons harmed by US surveillance. In contrast to the Official Secrets Acts in other countries, the First Amendment of the US Constitution has been interpreted to strictly protect the freedom of US journalists to report on national security issues such as surveillance. It similarly protects against overuse of defamation and libel claims by requiring strict proof for any such suit.[87] Complaints made to US reporters can be investigated, and those reporters enjoy significant protection from state censorship even where national security secrets are at issue. One such protection is that the US government may not engage in prior restraint of journalists, whether they are the New York Times or an independent journalist publishing online. [88] In other words, the US can respond to a published story but may not prevent the journalist from publishing at all. So, while an individual with a classified clearance may be guilty of a crime for sharing classified information with an unclassified party, the journalist is likely protected under the First Amendment for publishing any documents so acquired.[89]

[36] The US Supreme Court supported the ability of journalists to publish in *Bartnicki v. Vopper*, where the Court explained that this protection extends even to journalists who disclose illegally obtained or sourced information.[90] In *Bartnicki*, the Court examined what protection the First Amendment provides to speech that discloses the contents of an illegally intercepted communication.[91] The Court held that the First Amendment protects a journalist who receives and publishes unsolicited but illegally acquired information of public interest.[92]

---

[87] U.S CONST. amend. I, *New York Times Co. v. Sullivan*, 376 U.S. 254, 727 (1964) (requiring proof of actual malice "to award damages for libel in actions brought by public officials against critics of their official conduct").

[88] *See New York Times Co. v. United States*, 403 U.S. 713, 717 (1971) ("Both the history and language of the First Amendment support the view that the press must be left free to publish news, whatever the source, without censorship, injunctions, or prior restraints.") (Black, J., concurring).

[89] The US's Espionage Act prohibits the communication, publication, or transmission of classified information related to communication intelligence activities. 18 U.S.C. § 798. Scholars believe the First Amendment's prohibition of prior restraint would bar enforcement of the Espionage Act against journalists and other independent speakers *See* Patricia L. Bellia, *Wikileaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448, 1526 (2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2033207 (concluding that the Pentagon Papers case used the possibility of criminal responsibility and an ethical responsibility to prevent harm to influence how publishers used the Pentagon papers); Stephen I. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press*, 1 HARV. L. & POL'Y REV. 219, 234 (2007), https://ssrn.com/abstract=963998 (noting that while the Espionage Act could criminalize some journalist activities, the First Amendment "could be seen as conferring at least *some* minimal privilege on reporters who are, in good faith, attempting to uncover illicit governmental activity").

[90] *Bartnicki v. Vopper*, 532 U.S. 514, 535 (2001) https://supreme.justia.com/cases/federal/us/532/514/case.html ("We think it's clear that parallel reasoning requires the conclusion that a stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern.")

[91] *Id.* at 517.

[92] *Id.* at 535.

[37] In contrast, under EU Member State laws, it would appear that the facts of *Bartnicki* may have left the New York Times guilty under an Official Secrets Act.[93] Under the UK Official Secrets Act, for instance, a person "into whose possession the [protected] information, document or article has come is guilty of an offence if he discloses it without lawful authority knowing, or having reasonable cause to believe, that it is protected against disclosure"[94] by the Act if "the disclosure . . . is damaging, and he makes it knowing, or having reasonable cause to believe, that it would be damaging."[95] Likewise, under Irish law "[a] person shall not communicate any official information to any other person unless he is duly authorized to do so or does so in the course of and in accordance with his duties as the holder of a public office or when it is his duty in the Interest of the State to communicate it."[96] In either case, there is not the same level of protection or defense for a newspaper publishing state secrets that may be in the public interest but may also be damaging or against the interest of the State.

[38] This means that a US journalist would be able to respond directly to complaints by EU persons, affording a path of action for aggrieved individuals. Major US publications such as the New York Times and the Washington Post published disclosures of classified information that came from Edward Snowden. US publications similarly are willing to publish information from EU persons. EU persons' redress to the US press can have direct effects, such as the government canceling a program, and indirect effects, such as helping lay the groundwork for legislation eventually enacted in Congress.[97] Since the press can use classified information in making these claims, it is more difficult for the US to ignore well-sourced journalism of this type.

[39] Along with going directly to the press, individuals can directly petition companies to report their own sharing of data in response to national security and law enforcement requests. As discussed in the Chapter 3, companies today are publishing detailed "transparency reports" about the number and type of government requests for personal data.[98] The Open Technology Institute has also provided a "Transparency Reporting Toolkit" to better assist companies in generating these reports to share relevant information as permitted under US law.[99] The Privacy Shield Framework explicitly permits participating organizations to provide transparency reports on lawful

---

[93] *See* Official Secrets Act 1989, c. 6, § 5 (U.K.), http://www.legislation.gov.uk/ukpga/1989/6/pdfs/ukpga_19890006_en.pdf, Official Secrets Act 1963 (Act. No. 1/1963) (Ir.), http://www.irishstatutebook.ie/eli/1963/act/1/enacted/en/print.html.

[94] *See* Official Secrets Act 1989, c. 6, § 5(2) (U.K.), http://www.legislation.gov.uk/ukpga/1989/6/pdfs/ukpga_19890006_en.pdf

[95] *Id.* § 5(3).

[96] Official Secrets Act 1963, § 4 (Act. No. 1/1963) (Ir.), http://www.irishstatutebook.ie/eli/1963/act/1/enacted/en/print.html.

[97] *See The Watergate Story*, WASH. POST SPECIAL REPORTS, http://www.washingtonpost.com/wp-srv/politics/special/watergate/ (reporting on how the publication of the Pentagon Papers led, in part, to the cessation of President Nixon's taping policies and his eventual impeachment). There is little doubt, in my view, that the disclosures by Edward Snowden through the press played an important causal role in the reforms in the US since 2013.

[98] *See generally* RYAN BUDISH, ET AL., NEW AMERICA, OPEN TECHNOLOGY INSTITUTE, THE TRANSPARENCY REPORTING TOOLKIT (Mar. 31, 2016), https://www.newamerica.org/oti/policy-papers/the-transparency-reporting-toolkit/ (providing guidance on transparency reporting best practices for companies).

[99] *Id.*

access requests from the US government.[100] Making this data public allows more individuals and the press to be aware of the scope of lawful access taking place and to petition for restraint or cancellation of programs where appropriate.

[40] Non-governmental privacy advocate organizations in the US use their expertise and resources to pursue systemic change and recourse on behalf of aggrieved individuals.[101] The Electronic Privacy Information Center (EPIC), for example, which is participating in the current proceeding, undertakes numerous privacy protective activities, including petitions to the Federal Trade Commission regarding individual complaints.[102] The Center for Democracy and Technology engages in numerous privacy related activities, including publications, filing of official comments, and advocacy before Congress and executive agencies on issues such as secrecy and surveillance.[103] The American Civil Liberties Union, Electronic Frontier Foundation, Open Technology Institute, and many other non-governmental organizations conduct similar efforts, including accessing and compiling government documents through the Freedom of Information Act.[104] An individual concerned about his or her privacy rights can petition to any or all of these organizations, who can then work independently or in concert to bring their resources to bear on remedying an individual wrong or influencing changes in US policies and procedures.[105]

---

[100] *See* US DEP'T OF COMMERCE, PRIVACY SHIELD FRAMEWORK, *Access Requests by Public Authorities* (2016), https://www.privacyshield.gov/article?id=16-Access-Requests-by-Public-Authorities.

[101] *See, e.g.*, ELECTRONIC PRIVACY INFORMATION CENTER, *EPIC Administrative Procedure Act (APA) Comments*, EPIC.ORG, https://epic.org/apa/comments/.

[102] *Id.*

[103] *See* CENTER FOR DEMOCRACY & TECHNOLOGY, *About CDT*, https://cdt.org/about/.

[104] *Section 215 Documents*, AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/foia-collection/section-215-documents.

[105] In connection with press-related remedies, The US Freedom of Information Act (FOIA) is sometimes cited as a potential individual remedy, as it generally permits individuals to require the US federal government to disclose information in its possession. *See* 5 U.S.C. § 552(a). FOIA will likely not result in access, however, when the information sought is classified national security information. FOIA does not require US agencies to disclose such information. *Id.* § 552(b).

FOIA's national-security exclusion is longstanding and well known. For example, the EU Commission's Privacy Shield Adequacy Decision noted that FOIA will not permit individuals to obtain data from US intelligence agencies because such "agencies may withhold . . . classified national security information." Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, para. 114, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL.

In several EU Member States, freedom-of-information statutes similarly exclude classified national security information from access rights. *See, e.g.*, (1) France: CODE DES RELATIONS ENTRE LE PUBLIC ET L'ADMINISTRATION [CODE OF RELATIONS BETWEEN THE PUBLIC AND THE ADMINISTRATION], Art. L. 311-5 (excluding documents that may compromise defense secrets, foreign relations, the security of the State, or public safety from access rights), (in French) https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000031366350&idArticle=LEGIARTI000031367708; (2) Germany: Informationsfreiheitsgesetz [Freedom of Information Act], § 3 (excluding information that "may have detrimental effects on" international relations, military interests, or internal or external security interests from access rights), (in English) https://www.gesetze-im-internet.de/englisch_ifg/englisch_ifg.html#p0016; (3) Ireland: Freedom of Information Act 2014, (Act. No. 30/2014), § 33 ("A head may refuse to grant an FOI request . . . if . . . access to [a record] could reasonably be expected to affect adversely (a) the security of the State, (b) the defence of the State . . . (d) the international relations of the State."), http://www.irishstatutebook.ie/eli/2014/act/30/enacted/en/print#sec33.

[41] Lawyers sometimes assume that legal action is the most effective way to remedy a problem and effect change. In the discussion here, I highlight the crucial ways that remedies occur in the US through a free press, advocacy to the companies about their practices, and the efforts of non-governmental organizations. The role of the press and non-governmental organizations is often substantial in the US for surveillance and privacy issues. In my view, a fair assessment of the checks and balances that exist against surveillance abuse should include consideration of the role of the free press and public advocacy.

III. Additional US Privacy Remedies under Federal Law

[42] This Section first examines individual remedies against US companies, such as service providers of webmail and social networks, should they improperly disclose information to the US government about customers. It then examines privacy enforcement by federal administrative agencies, including the FTC and FCC.

A. Privacy Remedies against Service Providers

[43] Individual remedies are available against US companies, such as service providers of webmail and social networks, should they engage in activities that violate either relevant state or federal privacy laws or their own public privacy policies.[106] Using its law enforcement and foreign intelligence authorities, the US government can seek to compel the production of personal data from a US company, or compel the aid of a company in conducting wiretaps or surveillance.[107] These service providers have strong incentives to follow the law and their stated company policies. Violations can result in lawsuits against the service provider, as well as business harms if consumers lose trust in the ability of the companies to safeguard communications and other personal data. Lawsuits are notably available for violation of the Stored Communication Act or Wiretap Act.

[44] In light of the legal and business risks that face companies that violate law and policy, companies have considerable incentive to comply with applicable laws and policies. Compliance, in turn, means companies have reason to scrutinize government requests for information. Major Internet companies have become even stricter in this area since 2013 in the face of government requests for data. For instance, companies have adopted strong encryption in many new settings, protecting communications from wiretaps and other government efforts to access data.[108] In addition, major companies have increasingly challenged US government data requests in court,

---

[106] Although I use the term "service provider" in the text here to describe webmail and social network services, the statutory definition of "service provider" in US law is quite broad, as described in Chapter 9.

[107] *See* Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. § 1001 (requiring telecommunications carriers to make their equipment capable of enabling government wiretaps), 18 U.S.C. § 2703(a) (detailing how US law enforcement can compel the production of individuals' stored content).

[108] The increased prevalence of strong encryption has been a topic of several of my writings, including Peter Swire & Justin Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, N.Y.U. ANN. SURVEY AM. L. (forthcoming 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728478.

including in the 2015 *Microsoft Ireland* case.[109] A suit by individuals against a non-compliant company can pay at least statutory damages and attorney's fees. In addition, under the liberal American rules for discovery in court cases, individual suits can become an engine for generating more information that is critical of the company and the government request. In short, the risk of such individual suits shape what information companies are willing to provide the government.

1. Stored Communications Act

[45] Just as the SCA provides a cause of action for individuals against the US government, so too does it allow for civil actions against private companies that unlawfully disclose personal data.[110] Under the SCA, a data subject can obtain preliminary relief (e.g., injunctions) where appropriate, actual damages in an amount of no less than $1,000 USD (with an option for punitive damages where the violation was "willful"). Claimants can also recover court costs and attorney's fees, where appropriate. If a company shares data in good faith reliance on "a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization" then it cannot be found liable for any damages. Here again, the law allows for the systemic safeguards present in obtaining a valid instrument, but still allows a suit to continue if those checks are allegedly improperly circumvented. Just as noted earlier, the SCA allows any aggrieved person, including an EU data subject, to exercise its right of action.[111]

[46] In 2006, USA Today reported that telephone companies had supplied the US government with "the phone call records of tens of millions of Americans."[112] With a co-author, I published an article explaining how telecommunications companies who had shared stored phone records with the NSA could be liable for large amounts of statutory damages.[113] Since the providers appeared to have shared information with the NSA absent the required legal authority (e.g., a warrant) those companies that shared their subscribers' information could have been held liable for at least $1,000 USD per customer. The statutory minimum damage of $1,000 can be particularly important where the violations affect many individuals. For the records of fifty million individuals, that would mean liability of a staggering $50 billion. In 2008, Congress provided immunity to suit against the telephone companies for providing these records. In retrospect, it appears that the records were provided under a judicial order for the Section 215 telephone metadata program. The continued existence of the $1,000 USD per person statutory damages provides a powerful reason for both the government and service providers to comply with the Stored Communications Act.

---

[109] *Microsoft v. United States*, No. 14-2985, 2016 U.S. App. LEXIS 12926, at *46–49 (2d Cir. July 14, 2016), http://www.ca2.uscourts.gov/decisions/isysquery/2ec5a1b3-97ee-47c4-9224-1ea5b86ebbd4/6/doc/14-2985_complete_opn.pdf.

[110] 18 U.S.C. § 2707.

[111] *Id.* § 2707(a); *Suzlon Energy v. Microsoft*, 671 F.3d 726, 730 (9th Cir. 2011), http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf.

[112] Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA TODAY (May 11, 2006, 10:38 PM), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[113] Peter Swire, *Questions and Answers on Potential Telco Liability*, THINK PROGRESS (May 12, 2006), https://thinkprogress.org/questions-and-answers-on-potential-telco-liability-e5fa4bdd4c0d#.1qokc850w.

2. Wiretap Act

[47] The Wiretap Act provides a right of action against any person or entity, other than the US government, that violates the statute in intercepting, disclosing, or using surveillance data.[114] Barring an exception, the interception of communications is a criminal offense.[115] Exceptions to the rule are narrow. For example, interception is permitted if there is valid consent.[116] Another exception exists for interception done "in the ordinary course of business."[117] For example, routine call monitoring in a call center would qualify as exempted interception in the normal course of business.[118] An employer listening to an employee's personal call, however, would not fall under the exemption and would therefore still constitute a criminal interception under the Act.[119]

[48] A person whose communications are unlawfully intercepted may also bring suit against the intercepting party.[120] If the suit succeeds, then the individual is eligible for preliminary relief where appropriate, including enjoining ongoing surveillance, reasonable attorney's fees and costs if appropriate, and monetary damages.[121] These damages can either be the sum of actual damages caused by the violation or statutory damages. Statutory damages are determined as the greater of either $100 USD per day of the ongoing violation or $10,000 USD.[122] As with the SCA, companies can again rely on documents compelling cooperation with the US government as a defense in any action under the Wiretap Act.[123] Also like the SCA, an EU data subject can directly bring suits against companies for violation of the Wiretap Act.[124]

B. Enforcement by Federal Administrative Agencies

[49] I next discuss five major administrative agencies in the US that also serve as privacy enforcers: The FTC, the FCC, the Consumer Financial Protection Bureau (CFPB), the Securities and Exchange Commission (SEC), and the Department of Health and Human Services (HHS). As shown in my textbook on US private-sector privacy law, other federal agencies also play roles in privacy enforcement, usually depending on the sector that each agency oversees.

---

[114] *See* SWIRE & AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 142.
[115] *Id.*
[116] *Id.* Note that the required consent can vary depending on the state. The Wiretap Act itself allows for a single party's consent, but some states require all parties to a call to consent to the interception. In practice, this means many companies will use a notification, such as "This call may be recorded for quality assurance purposes" to ensure all parties have an opportunity to disconnect or object.
[117] *Id.*
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] 50 U.S.C. § 1810.
[122] *Id.*
[123] *Id.* § 1810(a).
[124] 18 U.S.C. § 2510(6) (defining "person" under the statute without restrictions based on citizenship), http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2703&num=0&edition=prelim; *see also Suzlon Energy v. Microsoft*, 671 F.3d 726, 730 (9th Cir. 2011), http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf ("Thus, the Court remains firm in its initial finding that the ECPA unambiguously applies to foreign citizens.").

These administrative agencies do not themselves bring actions against intelligence agencies. They can be important, however, because they can bring actions against companies that fail to comply with applicable law or company privacy policies, such as when the companies improperly provide electronic communications to the government.

1. The Federal Trade Commission (FTC)

[50] The FTC is tasked with regulating and enforcing actions in US commerce for the protection of consumers and the public welfare.[125] In 1938, the FTC's mission was expanded from its original mission to enforce antitrust laws to include protecting consumers generally.[126] The FTC exists independently from other executive agencies, meaning it is not under the direct control of the US President.[127] Instead, the Commission is headed by a chairman and four other commissioners who govern its activities, no more than three of whom can be from the same political party.[128]

[51] The FTC's authority comes from the Federal Trade Commission Act (FTC Act), which includes arguably the "single most important piece of US privacy law":[129] "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[130] While the statute does not explicitly mention data privacy, US law today has thoroughly established that the prohibition against unfair and deceptive practices applies to privacy and information security.[131] Unfair and deceptive practices can include company actions that violate the company's privacy statement,[132] inadvertent sharing of subscriber email addresses,[133] and misleading statements about the level of data security present in a website or Internet service.[134] Over time, the FTC's role as privacy enforcer was expanded by Congress to include regulatory and enforcement authority over misuse of children's data[135] and spam email practices.[136]

[52] FTC enforcement investigations are often in response to consumer complaints made directly to the agency, press reports, complaints from business competitors, or from internal research at the FTC.[137] The FTC has broad authority to investigate these claims, including the ability to subpoena witnesses, make civil investigative demands, and require companies to submit written reports under oath.[138] Once the FTC investigation is complete, the Commission decides if it will issue a legal complaint to begin an administrative trial before an Administrative Law Judge, whose

---

[125] *See* FEDERAL TRADE COMMISSION, *About the FTC*, https://www.ftc.gov/about-ftc.
[126] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 14.
[127] *Id.*
[128] *Id.*
[129] *Id.*
[130] 15 U.S.C. § 45.
[131] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 14.
[132] *Id.* at 17 (discussing *In the Matter of GeoCities, Inc.*).
[133] *Id.* (discussing *In the Matter of Eli Lilly & Co.*).
[134] *Id.* (discussing *In the Matter of Microsoft Corp.*).
[135] *Id.* at 14 (discussing the FTC's authority under the Children's Online Privacy Protection Act).
[136] *Id.* (discussing the FTC's authority under the Controlling the Assault of Non-Solicited Pornography and Marketing Act).
[137] *Id.* at 15.
[138] *Id.*

decision can be appealed to a federal district court in the US.[139] Companies found to engage in unfair or deceptive practices can be fined up to $16,000 USD per violation, and the FTC can seek damages to compensate those harmed by the unlawful activity.[140] In practice, the FTC often settles these enforcement actions through consent decrees and accompanying consent orders.[141] Consent decrees are public documents which bind a company to abide by changes to its business practices.[142] Consent decrees often require the company to prove compliance over time and to inform all related persons of obligations under the consent decree.[143] Companies under a consent decree must also inform the FTC if any changes in company operations will affect the company's ability to abide by the consent degree's terms.[144] These decrees also typically require periodic outside audits or reviews of company practices and may even require a company to adopt and implement a comprehensive privacy program.[145] If a company violates a consent decree, the FTC can bring another enforcement action in federal district court to seek additional fines as well as injunctions and other forms of relief.[146]

[53] These actions not only provide a remedy for unfair or deceptive actions but also function as a de facto common law of privacy norms and best practices. Professors Daniel J. Solove & Woodrow Hartzog's article, *The FTC and the New Common Law of Privacy*, examines FTC complaints, consent decrees, reports, and other materials and how these document can "impos[e] certain default standards" for privacy.[147] Solove and Hartzog argue "that today FTC privacy jurisprudence is the broadest and most influential regulating force on information privacy in the United States."[148] They also point out that while the US's sectoral approach can appear to leave large areas unregulated, the FTC actually regulates those parts through its "sprawling jurisdiction to enforce privacy."[149] To illustrate this point, the following examples are some of the FTC's more notable enforcement actions from the past ten years:

1. ***United States v. Google, Inc.*:** The FTC entered into a consent decree with Google resulting in a $22,500,000 USD civil penalty for failing to comply with a previous consent order restricting Google's ability to make representations about the control users had over their information and its collection.[150] In this case, the FTC fined Google for overriding default cookie collection settings in Safari browsers. Google remained under control of the previous consent order,

---

[139] *Id.*
[140] *Id.*
[141] *See id.*; *see also Cases and Proceedings*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/enforcement/cases-proceedings.
[142] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 15.
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA L. REV. 583, 676 (2014) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.
[148] *Id.* at 587.
[149] *Id.* at 588.
[150] *See United States v. Google Inc.*, No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012) (order), http://www.ftc.gov/sites/default/files/documents/cases/2012/11/121120googleorder.pdf.

and was additionally required to report on their continued maintenance after the incident.

2. ***United States v. Xanga.com, Inc.*:** The FTC entered into a consent decree with Xanga, Inc. resulting in a $1,000,000 USD civil penalty.[151] The FTC alleged that Xanga, Inc. inadequately prevented children under the age of 13 from registering for an account and sharing personal information and failed to provide proper notice of their practice. Xanga, Inc. was also required to stop violating the Children's Online Privacy Protection Act (COPPA), provide conspicuous notice of its practices, and delete all information collected from children.

3. ***United States v. Sony BMG Music Entertainment*:** The FTC entered into a consent decree with Sony resulting in a $1,000,000 USD civil penalty.[152] The FTC alleged that, despite Sony's privacy policy's representations that children under 13 were not able to register for Sony sites, those sites accepted registrations with an entered age under 13. Since parents of these children were not notified nor did the parents provide verifiable consent, the FTC alleged violations under COPPA. In addition to the civil penalty, Sony's consent decree required that Sony delete all information that was unlawfully collected, provide prominent notice about usage and collection of children's data on their website, and provide parents of children under 13 using Sony sites with actual notice of the collection and use of children's personal information.

4. ***United States v. Path, Inc.*:** The FTC entered into a consent decree with Path, Inc., resulting in an $800,000 USD fine and twenty year commitment to biennial assessments and reports.[153] Path was charged with misleading customers concerning information use, failing to obtain consent to data collection from a user's address book, and collecting personal information from children under the age of 13 without verifiable parental consent in violation of COPPA.

[54] Notably, as part of the US's participation in the Privacy Shield Framework, the FTC has committed to assistance in four areas: "(1) referral prioritization and investigations; (2) addressing false or deceptive Privacy Shield membership claims; (3) continued order monitoring; and (4) enhanced engagement and enforcement cooperation with EU DPAs."[154] This assistance includes information sharing and investigative assistance, including sharing information obtained in connection with an FTC investigation, issuing compulsory process on behalf of an EU DPA

[151] *See United States v. Xanga.com, Inc.*, No. 06 CV 6853 (S.D.N.Y. Sep. 12, 2006), https://www.ftc.gov/sites/default/files/documents/cases/2006/09/xangaconsentdecree_image.pdf.
[152] *See United States v. Sony BMG Music Entertainment*, No. 08 Civ. 10730 (S.D.N.Y. Dec. 15, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/12/081211consentp0823071.pdf.
[153] *See United States v. Path, Inc.*, No. 3:13-CV-00448-RS (N.D. Cal. Feb. 8, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.
[154] Letter dated July 7, 2016 from Edith Ramirez, Chairwoman, FTC, to Věra Jourová, Comm'r for Justice, Consumers and Gender Equality, European Commission 2, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0v.

conducting its own investigation, and seeking oral testimony from witnesses or defendant in connection with an EU DPA's enforcement proceeding.[155] To assist in these commitments, the FTC will create a standardized referral process and provide guidance to EU Member States on the type of information that would best assist the FTC in its inquiry following a referral.[156] The FTC has also committed to exchanging information on referrals with referring enforcement authorities and to working closely with EU DPAs in providing enforcement assistance.[157]

2. The Federal Communications Commission (FCC)

[55] The FCC is responsible for regulating and enforcing rules for "interstate and international communications by radio, television, wire, satellite and cable" in the US.[158] Like the FTC, the FCC is independent from the President's control. While the FTC focuses primarily on enforcement actions,[159] the FCC both issues legal regulations for industries under its oversight and enforces telecommunications law and regulations, including for privacy.[160] The FCC's primary privacy oversight function traditionally centered around rules for customer proprietary network information (CPNI). Under the Telecommunications Act and an accompanying FCC rule, telecommunications carriers were restricted in how they could access, use, and disclose their subscribers CPNI. CPNI includes subscription information, services used, network and billing information, phone features and capabilities, and more.[161] Today, a telecommunications carrier that shares a subscriber's CPNI without the express, opt-in consent of the subscriber is subject to enforcement and fines by the FCC.[162] The FCC has vigorously pursued enforcement of violations of these rules, including a $1,300,000 USD settlement with Verizon Wireless over the use of "supercookies."[163] Like the FTC, the FCC may begin an investigation on its own volition or in response to petitions from outside parties, including EU data subjects and DPAs, though it is not required to investigate each complaint.

[56] Examples of recent privacy enforcement from the FCC include:

1. ***In the Matter of AT&T Services, Inc.*:** In this case, the FCC entered into a consent decree with AT&T requiring a civil penalty of $25,000,000 USD.[164] The FCC's investigation alleged the unauthorized disclosure of approximately 280,000 customer names, social security numbers, and other CPNI.[165] Specifically, the FCC alleged that employees at AT&T call centers in Central and South America were able to access CPNI while obtaining other personal

[155] *Id.* at 6.
[156] *Id*.
[157] *Id*.
[158] *See* FEDERAL COMMUNICATIONS COMMISSION, *What We Do*, https://www.fcc.gov/about-fcc/what-we-do.
[159] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 14-15.
[160] *See What We Do*, *supra* note 160.
[161] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 100.
[162] *Id*.
[163] *In the Matter of Cellco Partnership, d/b/a Verizon Wireless*, FCC Rcd DA 16-242 (Mar. 7, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DA-16-242A1.pdf.
[164] *In the Matter of AT&T Services, Inc.*, FCC Rcd DA 15-399, 1 (Apr. 8, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DA-15-399A1.pdf.
[165] *Id.* at 4.

information used to unlock stolen cell phones.[166] AT&T was also required to notify all customers whose accounts were improperly accessed, appoint a senior compliance manager, conduct a privacy risk assessment, implement an information security program, prepare an appropriate compliance manual, and regularly train employees on the company's privacy policies and applicable privacy laws.[167]

2. ***In the Matter of Verizon*:** In this case, the FCC entered into a consent decree with Verizon Wireless requiring a fine of $7,400,000 USD.[168] The FCC's investigation alleged that Verizon had failed to notify customers of their privacy and opt-out rights before using personal information for marketing purposes in violation of the CPNI requirements.[169] Verizon was also required to notify customer of their opt-out rights on every bill for three years from the date of the order, put systems in place to monitor and test its billing and opt-out process, and develop and implement a three-year compliance plan including annual compliance reports.[170]

3. ***In the Matter of TerraCom, Inc. and YourTel America, Inc.*:** In this case, the FCC entered into a consent decree with TerraCom and YourTel, requiring a fine of $3,500,000 USD.[171] The FCC alleged that the companies failed to protect the confidentiality of customer proprietary information provided for demonstrating eligibility for the Lifeline program, and engaged in unjust and unreasonable practices in failing to employ reasonable data security practices to protect customers' proprietary information.[172] The FCC further alleged that the companies misrepresented that they employed reasonable data security practices to protect customer proprietary information in their respective privacy statements.[173]

[57] In 2015, the FCC reclassified Internet service providers as a covered telecommunications company, moving them from the FTC's jurisdiction to the FCC's jurisdiction.[174] Since then, the FCC has engaged in the formal process for a new regulation governing privacy for broadband Internet service providers.[175] On October 27, 2016, the FCC adopted its final privacy rule for

---

[166] *Id*.
[167] *Id.* at 6-13.
[168] *In the Matter of Verizon Compliance with the Commission's Rules and Regulations Governing Customer Proprietary Network Information*, FCC Rcd DA 14-1251, *1 (Sept. 3, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1251A1_Rcd.pdf.
[169] *Id.*at *5.
[170] *Id.* at *6-9.
[171] *In the Matter of TerraCom, Inc., and YourTel America, Inc.*, FCC Rcd DA 15-776, *19 (July 9, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DA-15-776A1_Rcd.pdf.
[172] *Id.* at *1.
[173] *Id*.
[174] *See Protecting and Promoting the Open Internet*, 80 Fed. Reg. 19737 (Apr. 13, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-04-13/pdf/2015-07841.pdf.
[175] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 81 Fed. Reg. 23360 (Apr. 20, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-04-20/pdf/2016-08458.pdf.

broadband Internet service providers, requiring affirmative opt-in consent before using or sharing any sensitive information, such as geolocation data, financial information, health information, children's information, web browsing history, app usage history, and the content of communications.[176]

3. The Consumer Financial Protection Bureau (CFPB)

[58] In 2010, the CFPB was created under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank).[177] The CFPB is responsible for overseeing relationships between consumers and the providers of financial products and services.[178] Under Dodd-Frank, the CFPB has broad authority to examine, regulate, and enforce actions of business that provide financial services and products.[179] The CFPB is also able to make rules under other existing financial privacy acts, including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Fair Debt Collection Practices Act.[180] Like the FTC, the CFPB can bring enforcement actions against businesses under its oversight for unfair and deceptive practices.[181] The CFPB is also authorized to enforce against "abusive acts and practices," including materially interfering with a consumer's ability to understand a term or condition of a consumer financial product; taking unreasonable advantage of a lack of understanding by the consumer of material risks, costs, and conditions; and taking unreasonable advantage of a consumer's inability to protect its interests.[182]

[59] The CFPB is authorized to conduct investigations, issue subpoenas, hold hearings, and commence civil actions against offenders.[183] For violations of federal consumer privacy law, a company can face of $5,000 USD per day.[184] If the company's violation of law was reckless, they can instead be held liable for $25,000 USD per day.[185] Finally, if the company knowingly violated federal consumer protection law, companies can face fines of up to $1,000,000 USD per day. The CFPB can also seek to impose "limits on the activities or functions" of the offender.[186] While the CFPB has not engaged in prominent privacy enforcement to date, it is worth examining its actions as a consumer protection enforcer generally as evidence of how it carries out its enforcement authority under Dodd-Frank and other Acts.

[60] As an example of strong enforcement by the CFPB, in 2014, the Board entered into a consent order with GE Capital Retail Bank, requiring payment of an estimated $225,000,000 USD in relief

---

[176] *See* Press Release, Federal Communications Commission, FCC Adopts Privacy Rules to Give Broadband Consumers Increased Choice, Transparency, and Security for their Personal Data (Oct. 27, 2016) http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1027/DOC-341937A1.pdf.
[177] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 71.
[178] *Id.*
[179] *Id.*
[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *Id.* at 72.
[184] *Id.*
[185] *Id.*
[186] Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, § 1055(a)(2)(G), 124 Stat. 1376, https://www.sec.gov/about/laws/wallstreetreform-cpa.pdf.

to consumers allegedly harmed by illegal and discriminatory credit card practices.[187] The CFPB found two of GE Capital's promotions were discriminatory in not offering settlement and statement credit offers to individuals who preferred to communicate in Spanish or had a mailing address in Puerto Rico, even if the individual otherwise met the program's requirements.[188] In addition to the money GE Capital was required to reimburse to harmed consumers, GE Capital was required to end its deceptive practices and illegal discrimination and to notify credit reporting agencies of updated information. GE Capital was also required to pay an additional $3,500,000 USD penalty for its deceptive and unfair practices.

4. The Securities and Exchange Commission (SEC)

[61] Under the Securities Act, the SEC is empowered "to protect investors; maintain fair, orderly, and efficient markets, and facilitate capital formation."[189] Like the FCC, the SEC may also issue appropriate regulations and enforce against companies under its oversight that violate these laws and regulation.[190] In 2000, along with the other financial services regulatory agencies, the SEC adopted Regulation S-P on the Privacy of Consumer Financial Information.[191] Under the regulation, companies are required to provide adequate notice to their customers about privacy policies and practices, are restricted in how they may disclose nonpublic personal information about consumers to nonaffiliated third parties, and must provide a method for consumers to opt-out of any disclosure of their nonpublic personal information.[192] The regulation also includes a requirement that covered companies must safeguard customer records and information.[193]

[62] Examples of recent enforcement of these rules include:

1. ***In the Matter of Morgan Stanley Smith Barney, LLC*:** In this case, the SEC settled allegations of failure to protect consumer information, some of which was hacked and sold online, resulting in a $1,000,000 USD penalty.[194] The SEC's order found that Morgan Stanley had failed to adopt written policies and procedures to reasonably protect customer data.[195] The SEC further sanctioned the individual employee who downloaded and transferred confidential data to

[187] CFPB Consent Order, *In the Matter of Synchrony Bank, f/k/a GE Capital Retail Bank* (Jun. 19, 2014), http://files.consumerfinance.gov/f/201406_cfpb_consent-order_synchronybank.pdf.
[188] *Id.*
[189] *See About the SEC*, SEC, https://www.sec.gov/about.shtml.
[190] *See* The Securities Act § 19(a), 15 U.S.C. § 77s (granting the Commission authority to issue regulations and enforce violations under the Act), https://www.sec.gov/about/laws/sa33.pdf.
[191] SEC Final Rule: Privacy of Consumer Financial Information (Regulation S-P), 17 C.F.R. § 248, https://www.sec.gov/rules/final/34-42974.htm.
[192] *Id.* § 248.1.
[193] *Id.* § 248.30.
[194] *In the Matter of Morgan Stanley Smith Barney LLC*, File No. 3-17280, 6 (Jun. 8, 2016), https://www.sec.gov/litigation/admin/2016/34-78021.pdf.
[195] *Id.*

his personal server, and he was criminally convicted for his actions and received a sentence of 36 months' probation and a $600,000 USD restitution order.[196]

2. ***In the Matter of R.T. Jones Capital Equities Management, Inc.*:** In 2015, the SEC brought an enforcement action against an investment adviser for failing to properly protect its clients' personal information prior to a data breach.[197] Here, the adviser had failed to properly adopt written policies and procedures to protect its customer records and information for a 4-year period. The adviser settled with the SEC, agreeing to cease and desist from committing or causing future violations of the rule, and to pay a $75,000 USD fine.[198] As with an FTC consent decree, if the adviser were to fail to abide by the requirements of the settlement, it could be brought back into court to face additional penalties.[199]

[63] Safeguarding personal information is an essential element of privacy protection, and these recent cases highlight the SEC's interest in enforcement in this area.

5. The Department of Health and Human Services (DHHS)

[64] The approximately 17 percent of the US economy devoted to health care is governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.[200] In my role as Chief Counselor for Privacy, I was the White House coordinator of the proposed HIPAA Privacy Rule in 1999, and the final issue published in 2000. The rule was modified in 2003, and additional modifications were included in the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) and the regulations implementing that Act.

[65] The HIPAA Privacy Rule creates a comprehensive system for protecting the privacy of individual's medical information, including requirements for privacy notices, authorizations for the use and disclosure of protected health information (PHI), limits to only use and disclose PHI to the minimum extent necessary, individual access and accounting rights, and security safeguards.[201]

[66] Within the HHS, the Office for Civil Rights (OCR) leads a large-scale enforcement program. OCR receives numerous complaints each year, and as of September 30, 2016, has resolved a total of 137,861 HIPAA complaints, with 39 such cases settled for a total of $45,889,200

---

[196] Press Release, SEC, Morgan Stanley Failed to Safeguard Customer Data, (Jun. 8, 2016), https://www.sec.gov/news/pressrelease/2016-112.html.
[197] Press Release, SEC, SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to the Breach, (Sep. 22, 2015), https://www.sec.gov/news/pressrelease/2015-202.html.
[198] *Id.*
[199] *See* 15 U.S.C. § 77i (explaining the procedure for having a Court review, and subsequently enter into force, any cease and desist or other order issued by the SEC), https://www.sec.gov/about/laws/sa33.pdf.
[200] *See* Health Insurance Portability and Accountability Act Privacy Rule, 45 C.F.R. § 160, https://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/content-detail.html; Health Expenditure, Total (% of GDP), The World Bank, http://data.worldbank.org/indicator/SH.XPD.TOTL.ZS.
[201] *See* SWIRE AND AHMAD, *supra* note 1, at 48.

USD in civil money penalties.[202] In 15,746 cases, OCR provided early intervention and technical assistance to resolve the issue without the need for an investigation.[203] In 2014 alone, OCR investigated and resolved a total of 17,748 complaints.[204] OCR performs a combination of investigations of complaints and compliance reviews to determine where enforcement is needed.[205] If OCR reviews and accepts a complaint for investigation it will notify the filer and the cover entity named in the complaint to begin the investigation.[206] Covered entities are required by law to cooperate with these investigations.[207] Once the investigation is complete, OCR reviews the evidence gathered to determine whether the covered entity violated the Privacy or Security Rule.[208] If the covered entity was not in compliance with the rules, OCR may obtain voluntary compliance, corrective action, or a resolution agreement.[209] OCR may also impose a penalty between $100 USD and $50,000 USD /per violation, with a calendar year cap of $1,500,000 USD.[210] OCR publishes statistics on complaints and enforcement actions, which show an increasing trend in the number of total complaints resolved with 17,748 total resolutions in 2014 up from 14,293 in 2013, and less than 10,000 per year between 2004 and 2012.[211]

[67] In addition to investigations based on complaints, OCR conducts audits of covered entities to ensure HIPAA compliance.[212] OCR is currently developing a new audit program to better assess HIPAA compliance, identify best practices, discover risks and vulnerabilities, and address problems prior to a breach of data.[213] OCR is overseeing on-site auditing of a wide variety of covered entities and business associates in order to sample criteria across the spectrum of covered entities.[214]

[68] In 2003, HHS also issued a final version of the HIPAA Security Rule, which reinforces the safeguards in the Privacy Rule. The Security Rule establishing minimum security requirements for PHI that "a covered entity receives, creates, maintains or transmits in electronic form (ePHI)."[215] Under the Security Rule, covered entities and their business associates must maintain

---

[202] *See* US DEP'T OF HEALTH AND HUMAN SERVICES, *Enforcement Highlights*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (last updated Sep. 30, 2016).
[203] *Id.* Of the remaining cases, 11,099 investigations found that no violation had occurred, and 86,515 cases resulted in a determination that the complaint did not present an eligible case for enforcement.
[204] US DEP'T OF HEALTH AND HUMAN SERVICES, *Enforcement Results by Year*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html.
[205] US DEP'T OF HEALTH AND HUMAN SERVICES, *How OCR Enforces the HIPAA Privacy & Security Rules*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-OCR-enforces-the-HIPAA-privacy-and-security-rules/index.html.
[206] *Id.*
[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] *Summary of the HIPAA Privacy Rule*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/; US DEP'T OF HEALTH AND HUMAN SERVICES, *Summary of the HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/.
[211] *Enforcement Results by Year*, *supra* note 206.
[212] *Id.*
[213] US DEP'T OF HEALTH AND HUMAN SERVICES, *HIPAA Privacy, Security, and Breach Notification Audit Program*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/#program.
[214] *Id.*
[215] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 49.

the "confidentiality, integrity, and availability of all ePHI the covered entity creates, receives, maintains, or transmits"; protect against reasonable threats or hazards; protect against use or disclosure of ePHI not permitted under the Privacy Rule; and make sure the organization's workforce complies with the Security Rule.[216] The Security Rule also allows organizations to comply by means appropriate to the organization, accounting for factors like size, complexity, costs, technical infrastructure, and the probability and criticality of potential risks to ePHI.[217] Lastly, the Security Rule requires that covered entities conduct ongoing risk assessments, implement security awareness and training for its workforce, and designate an individual responsible for implementing and overseeing the entity's Security Rule compliance program.[218]

[69] Examples of recent OCR enforcement actions include:

1. ***Cignet Health of Prince George's County, Maryland*:** OCR issued a Notice of Final Determination finding that Cignet violated the HIPAA Privacy Rule, imposing a civil money penalty of $4,300,000 USD.[219] OCR found that Cignet had violated 41 patients' rights by denying them access to their medical records.[220] OCR fined Cignet $1,300,000 USD for the violations, and an additional $3,000,000 USD for willful neglect in failing to cooperate with OCR's investigation.[221]

2. ***Massachusetts General Hospital*:** OCR entered into a settlement with Massachusetts General Hospital related to an investigation of the loss of protected health information of 192 patients of its Infectious Disease Associates outpatient practice, including patients with HIV/AIDS.[222] The documents were lost when an employee left them on a subway train while commuting to work.[223] The settlement required Massachusetts General Hospital to pay $1,000,000 USD and enact a robust compliance program to avoid future compliance issues.[224]

3. ***Advocate Health Care Network*:** OCR entered into a settlement with Advocate Health Care Network following an investigation of three reported breaches of ePHI. OCR alleged that Advocate failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities of its ePHI, failed to implement proper policies and procedures to limit access to ePHI, failed to

---

[216] *Id.* at 50-51.
[217] *Id.*
[218] *Id.* at 51.
[219] *See Cignet Health fined a $4.3M Civil Money Penalty for HIPAA Privacy Rule Violations*, US DEP'T OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cignet-health/.
[220] *Id.*
[221] *Id.*
[222] *Massachusetts General Hospital Settles Potential HIPAA Violations*, US DEP'T OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/massachusetts-general-hospital/index.html.
[223] *Id.*
[224] *Id.*

obtain satisfactory assurances that a business associate would properly handle all ePHI in its possession, and failed to reasonably safeguard an unencrypted laptop.[225] The settlement required Advocate to pay $5,550,000 USD and adopt a corrective action plan to address its privacy and security shortcomings.[226]

4. ***University of Mississippi Medical Center (UMMC)*:** OCR entered into a settlement with UMMC related to multiple alleged violations of HIPAA security and privacy requirements, resulting in a penalty of $2,750,000 USD.[227] OCR's investigation alleged that UMMC failed to prevent, detect, contain, and correct security violations; failed to implement physical safeguards for workstations with access to ePHI; failed to assign a unique user name and/or number for identifying and tracking individuals on systems containing ePHI; and failed to notify each individual whose unsecured ePHI was reasonably believed to be at risk as a result of the breach.[228] In addition to the fine, UMMC was required to adopt a corrective action plan to ensure future compliance with HIPAA privacy and safeguard rules.[229]

5. ***Oregon Health & Science University (OHSU)*:** OCR entered into a settlement agreement with OHSU resulting in a comprehensive three-year corrective action plan and a penalty of $2,700,000 USD.[230] OCR investigation began after OHSU submitted multiple breach reports, including two reports involving unencrypted devices and a stolen unencrypted storage device.[231] OCR found that the risk analyses that OHSU conducted did not properly cover all ePHI in OHSU's operation as required.[232] OCR further alleged that OHSU did not act in a timely manner to implement measures to address documented risks and vulnerabilities, nor did it have proper policies and procedures to prevent, detect, contain, and correct security violations.[233] Lastly, OCR alleged that OHSU failed to implement a mechanism to encrypt and decrypt ePHI, or a functional alternative measure, despite knowing that lack of encryption was a risk.[234]

---

[225] *Id.*
[226] *Id.*
[227] *Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC)*, US DEP'T OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/UMMC/index.html.
[228] *Id.*
[229] *Id.*
[230] Press Release, US Dep't of Health and Human Services, Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University (Jul. 18, 2016), http://www.hhs.gov/about/news/2016/07/18/widespread-hipaa-vulnerabilities-result-in-settlement-with-oregon-health-science-university.html.
[231] *Id.*
[232] *Id.*
[233] *Id.*
[234] *Id.*

IV. Enforcement under US State Law and Private Rights of Action

[70] Section IV introduces privacy enforcement under state law and federal or state private rights of action. Each state has an Attorney General tasked with protecting consumers. As documented by Professor Citron, these AGs have emerged as important privacy enforcers. This Section then examines the numerous private rights of action that exist under both federal and state law, using the state of California as one example. The prevalence of plaintiffs' lawyers and private rights of action in the US means that defendants (including companies and often government agencies) have increased incentive to comply strictly with applicable law.

A. State Attorney General (AG) Enforcement

[71] I next describe an important but sometimes overlooked set of actors in privacy enforcement in the US – the state AGs. The AG in each state serves as the chief law enforcement officer for that state, with a wide range of powers and responsibilities. Professor Danielle Citron of the University of Maryland Law School has recently completed award-winning research about the role of these AGs in US privacy policy and privacy enforcement.[235]

[72] To avoid the complexity of discussing fifty states, my comments here focus on the office of the California AG, which has been a leader in the enforcement of privacy and security related issues.[236] Other state AGs have often taken the lead on specific privacy related issues; my comments here explain the workings in one large state. As Professor Citron's research shows, similar authorities and interest in privacy enforcement exist in other states as well.

[73] California is the most populous state in the US, encompassing approximately 40 million people.[237] Its laws regulating data security broadly encompass any person or business that conducts business in California.[238] Because so much business is online and the population of California is so large, a wide range of businesses headquartered outside of California "conduct business" there and are subject to its data breach and other laws. The impact of enforcement by the California AG is increasing because of the growing use of multi-state collaborations among state AGs, including for large-scale enforcement actions across the country.[239]

[74] A well-known instance of California as a privacy innovator is its passage of the first US state data breach notification law in 2002.[240] Today, at least 46 states and territories have data

---

[235] Citron, *supra* note 4 (manuscript at 9).This research received the best paper award in the 2016 Privacy Law Scholars Conference.

[236] KAMALA D. HARRIS, ATTORNEY GENERAL CALIFORNIA DEPARTMENT OF JUSTICE, CALIFORNIA DATA BREACH REPORT (2016) ("California was the first to enact a data breach notification law, which took effect in 2003. In the twelve years since then, 46 other states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, as well as foreign jurisdictions around the world, have enacted similar laws."), https://oag.ca.gov/breachreport2016.

[237] UNITED STATES CENSUS BUREAU, *California QuickFacts*, http://www.census.gov/quickfacts/table/PST045215/06.

[238] HARRIS, *supra* note 238. The statute also applies to any state or local agency that owns or licenses "computerized data." *Id.*

[239] *Id.*

[240] CAL. CIV. CODE §§ 1798.29, 1798.80 *et seq.*

breach laws, with many of them modeled on the California law.[241] California similarly played the innovator role in other areas, such as when California's laws on restrictive use of consumer data for marketing purposes preceded similar regulations eventually adopted by the FCC.[242] As another example, California was an innovator in credit reporting as the first state to pass credit "freeze" legislation that allows a consumer to lock their credit report, prohibiting access by new credit issuers.[243] These regulations were eventually incorporated into federal law as well.[244]

[75] Enforcement by AGs in California and other US states provides individuals an accessible opportunity for redress for privacy-related violations, within the consumer's own state. The AG solicits complaints from individuals regarding consumer privacy-related violations. Form complaints can be filed by individuals on AG websites, which are accessible to anyone.[245] The AG is permitted to investigate petitions from any persons, including EU data subjects. Once the AG has received complaints relating to a breach of security or other privacy-related violation, the AG may launch an investigation, using a range of investigative tools, such as Civil Investigative Demands requiring companies to turn over information based "merely on suspicion that the law is being violated, or even just because [they] want assurance that it is not."[246]

[76] AG investigations have led to increasingly strict state enforcement of privacy laws. In roughly the past year, investigations by the California AG have resulted in significant settlements with corporate entities for violations of privacy-related laws.[247] For instance, Wells Fargo agreed to an $8.5 million settlement for violating California privacy laws by recording consumers' phone

---

[241] *See* NATIONAL CONFERENCE OF STATE LEGISLATURES, *Security Breach Notification Laws* (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (listing all current state data breach notification laws).

[242] *See, e.g.*, Chris Hoofnagle, European Commission Directorate General Justice, Freedom and Democracy, *Commission Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, B.1 – United States of America*, at 15 (May 2010), http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_country_report_b1_usa.pdf ("Long before the Federal Communications Commission adopted opt in rules for sharing of telephone subscriber information, the California Public Utilities Code required written consent for transfer of such information.").

[243] *Id.* All fifty states in the U.S. have some form of credit freeze legislation, with 24 states allowing any consumer to place a "freeze" on their credit report. *See, e.g.*, ALA. CODE § 8-35-1 *et seq.*, CAL. CIVIL CODE § 1785.11.2 *et seq.*, KY. REV. STAT. ANN. § 367.363 *et seq.* Others may require a person be a victim of identity theft or a resident of the state. *See, e.g.*, MISS. CODE ANN. § 75-24-201 *et seq.* (allowing credit freezes for victims of identity theft), WASH. REV. CODE § 19.182.170 *et seq.* (allowing credit freezes for any consumer who is a resident of the state). Some also specifically allow for credit freezes on behalf of a "protected consumer" who is either below a certain age or otherwise in guardianship. *See, e.g.*, 815 ILL. COMP. STAT., §505/2MM (allowing a representative on behalf of a disabled person or the guardian of a minor to request a credit freeze on behalf of the minor or disabled person), IND. CODE §§24-5-24-1 *et seq.*, 24-5-24.5-10 *et seq.* (allowing a representative of a "protected consumer" to request a credit freeze on behalf of that protected consumer).

[244] *Id.*, Duties of Card Issuers Regarding Changes of Address, 16 C.F.R. § 681.2(c).

[245] *See, e.g.*, STATE OF CALIFORNIA OFFICE OF THE ATTORNEY GENERAL, *Consumer Complaint Against a Business/Company*, https://oag.ca.gov/contact/consumer-complaint-against-business-or-company (soliciting complaints); *see also* NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL, *New York State Security Breach Reporting Form*, https://forms.ag.ny.gov/CIS/breach-reporting.jsp.

[246] *United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950), https://supreme.justia.com/cases/federal/us/338/632/case.html.

[247] *See* STATE OF CALIFORNIA OFFICE OF THE ATTORNEY GENERAL, *Privacy Enforcement Actions*, https://oag.ca.gov/privacy/privacy-enforcement-actions.

calls without a timely disclosure to consumers, as required by the California Penal Code.[248] Comcast resolved an investigation into allegations that it posted consumer information on-line by agreeing to strengthen its restrictions on use of consumer information and paid $25 million in penalties and $8 million to its consumers for restitution.[249] Similarly, Houzz, an online platform for home remodeling that violated California privacy laws through unauthorized recording of telephone calls, appointed a Chief Privacy Officer to oversee its compliance with California and federal privacy laws and paid a fine of $175,000. Warnings to corporate entities by the AG of an impending investigation often serve to facilitate the redress of corporate wrong-doing related to consumer privacy.[250]

[77] If initial investigations do not lead to resolution of a problem, the AG has full power to enforce the laws of the state and the nation on behalf of its constituents.[251] Notably, all fifty states have what are often called "baby FTC Acts." Above, I described the power of the FTC to enforce against deceptive and unfair acts in commerce. California and the other states have "unfair and deceptive acts and practices" (UDAP) laws, with essentially the same enforcement powers as the FTC if a company breaks its privacy promises or acts in an unfair manner toward consumers.

B. Private Rights of Action

[78] It is something of a cliché (and often a true observation) that the US favors plaintiffs more than most other countries. During negotiation of the Safe Harbor in 1999-2000, I heard US Ambassador David Aaron, the lead US negotiator, say more than once to EU negotiators: "We'll take your privacy laws if you take our plaintiffs' lawyers." The prevalence of plaintiffs' lawyers and private rights of action means that defendants (including companies and often government agencies) have increased incentive to comply strictly with applicable law. In the US, the written law is usually not aspirational – it is the basis for enforcement and litigation.

[79] For the many private rights of action under federal and state law, I highlight four ways that US law favors the bringing of such actions:

1. ***Attorney's fees.*** The "American rule" for attorney's fees is that each party generally pays its own lawyers and court expenses. By contrast, the "British rule" is generally that the loser pays the costs of the winning party. This

---

[248] *Id.*
[249] *Id.*
[250] *See, e.g., Massachusetts Attorney General Reaches Settlement with Boston Hospital Over Data Security Allegations*, HUNTON & WILLIAMS PRIVACY & INFORMATION SECURITY LAW BLOG (Nov. 25, 2014), https://www.huntonprivacyblog.com/2014/11/25/massachusetts-attorney-general-reaches-settlement-boston-hospital-data-security-allegations/; FLORIDA OFFICE OF THE ATTORNEY GENERAL, *Attorneys General Reach Settlement with Zappos over Data Breach*, (Jan. 7, 2015), http://www.myfloridalegal.com/newsrel.nsf/newsreleases/F12E26235A23E57785257DC60063AEE9; NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL, *A.G. Schneiderman Announces Settlement with Trump Hotel Collection after Data Breaches Expose over 70K Credit Card Numbers*, (Sep. 23, 2016), http://www.ag.ny.gov/press-release/ag-schneiderman-announces-settlement-trump-hotel-collection-after-data-breaches-expose.
[251] *See* STATE ATTORNEYS GENERAL: POWERS AND RESPONSIBILITIES 14 (Emily Myers, Nat'l Ass'n of Attorneys General eds., 3d ed. 2013).

American rule clearly makes it easier for non-wealthy individuals to pursue a lawsuit.

2. ***Contingency fees.*** The US legal system often features plaintiff lawyers working on contingency fees. A common practice, for instance, is that the attorney will receive one-third or more of any settlement or judgment in a case. The combination of the American rule and contingency fees has created the phenomenon of plaintiff-side law firms that can take a portfolio of cases on contingency. If even a few of the cases succeed, then the law firm can succeed financially.

3. ***Jury trial.*** The right to jury trial, protected in the Seventh Amendment of the US Constitution,[252] remains an important feature of American law. Plaintiffs' lawyers, in my experience, often prefer to have a jury decide a case and the amount of damages rather than the judge. Where juries are outraged by a defendant's behavior, judgments can become quite large and may include punitive damages.

4. ***Broad discovery.*** A fourth feature of US law is relatively broad pre-trial discovery of evidence from the other parties. Although defendants may complain that discovery requests are "fishing expeditions," plaintiffs often can begin a case with a relatively small number of supporting facts, and develop considerably more evidence in the course of discovery.

The combined pro-plaintiff effect of these four factors is substantial compared to a regime that differs on all or most of the factors.

[80] With this pro-plaintiff litigation system in mind, I turn to private rights of action in California as an example of the sorts of laws that also exist in other states. As an initial matter, the California Constitution provides an inalienable right to pursue and obtain privacy.[253] The Privacy Clause "[p]rotects against the unwarranted, compelled disclosure of various private or sensitive information regarding one's personal life, including his or her financial affairs, political affiliations, medical history, sexual relationships, and confidential personnel information."[254]

---

[252] U.S. CONST. amend. VII. ("In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury, shall be otherwise re-examined in any Court of the United States, than according to the rules of the common law.").

[253] The text provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." CAL. CONST. Art. 1 § 1; California's Constitution is similar to some other state constitutional provisions protecting privacy. *See, e.g.*, ALASKA CONST. Art. I § 22 ("The right of the people to privacy is recognized and shall not be infringed."); *see also* FLA. CONST. Art. I, § 23 ("Every 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."); *see also* MONT. CONST. Art. 2, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.").

[254] *Tien v. Superior Court*, 139 Cal. App. 4th 528, 539 (Cal. Ct. App. 2006).

Violations of the Privacy Clause are actionable as torts among private actors.[255] California common law has incorporated four privacy torts under which an aggrieved party may sue: (1) intrusion into private matters; (2) public disclosure of private facts; (3) publicity placing a person in a false light; and (4) misappropriation of a person's name or likeness.[256] Depending on the facts alleged for an invasion of privacy, a plaintiff may also include causes of action for fraud and negligence.[257]

[81] In addition to the common law acting under this constitutional guarantee, California has enacted multiple statutes under which aggrieved individuals may seek redress.[258] The following statutes provide a private right of action under California law against any person or business that conducts business in California, and any state or local agency that owns or licenses computerized data.[259]

1. ***California Unfair Competition Law*** (UCL) is the state's "Baby FTC Act" that targets deceptive and unfair behavior. It is a broad and generally-worded statute that protects consumers and businesses from unfair competition described in Section 17200 as: "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising" among other defined acts relating to deceptive practices.[260] The broad coverage of UCL applies to all non-government entities so long as a plaintiff has suffered actual damages as a result of an entity's actions.[261] The UCL provides for injunctive relief, restitution and civil penalties. Injunctive relief and restitution are available in both private-party and government actions.[262] Civil penalties may be imposed in government enforcement actions for violations under UCL but are not available for private actions.[263]

2. ***Confidentiality of Medical Information Act*** (CMIA) protects the confidentiality of individually identifiable medical information obtained from a patient by a health care provider.[264] The CMIA provides that "[n]o provider

[255] *Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633 (Cal. 1994), https://scholar.google.com/scholar_case?case=9304848346192844 22&hl=en&as_sdt=6&as_vis=1&oi=scholar.
[256] *See* RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1965) (commonly cited as common law for all fifty states).
[257] *See, e.g.*, *In re EasySaver Rewards Litig.*, 921 F.Supp.2d 1040 (S.D. Cal. 2013), https://casetext.com/case/in-re-easysaver-rewards-litig; *In re Consumer Priv. Cases*, 175 Cal. App. 4th 545, (Cal. Ct. App. 2009), http://www.leagle.com/decision/In%20CACO%2020090701035/CONSUMER%20PRIVACY%20CASES.
[258] California is just an example of one of multiple states that have a robust regulatory scheme for privacy related violations. *See, e.g.*, MASS. GEN. LAWS ch. 214, § 1B, entitled The Massachusetts Privacy Act ("A person shall have a right against unreasonable, substantial or serious interference with his privacy.").
[259] HARRIS, *supra* note 221.
[260] CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*
[261] *See Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 811 (N.D. Cal. 2011) (holding that plaintiffs sufficiently alleged a loss of money or property based on potential unpaid compensation where Facebook used plaintiffs' Facebook profiles to endorse third-party products and services).
[262] *See* CAL. BUS. & PROF. CODE § 17203.
[263] *See id.* § 17206.
[264] The CMIA safeguards much of the same information protected by federal law under HIPAA, but unlike HIPAA, the CMIA creates a private right of action for those affected by a breach of the Act.

of health care, health care service plan, or contractor shall disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization, except as provided in subdivision (b) or (c)."[265] Remedies for breach of the CMIA include nominal damages of $1,000 and/or actual damages from "any person or entity who has negligently released confidential information or records."[266]

3. ***California Invasion of Privacy Act*** (CalCIPA) regulates telephone call monitoring and prohibits the intentional recording or eavesdropping of telephone calls without the consent of all parties.[267] A plaintiff may bring an action under CalCIPA so long as one of the parties on the telephone call is located in California. CalCIPA imposes both criminal and civil liability for violators of the statute. For private causes of action, the plaintiff need not suffer actual damages as the statute establishes a $5,000 penalty for each CalCIPA violation.[268] These penalties can quickly accrue as companies who may record or monitor hundreds, if not thousands, of calls each week could be potentially liable for millions of dollars in penalties.[269]

4. ***California Spam Laws*** regulate unsolicited commercial email with misleading or falsified headers or information.[270] They apply to emails sent to or from a California email address and authorize a recipient, an email service provider, or the AG to bring an action for actual damages and liquidated damages of $1,000 per email ad sent in violation, up to one million dollars per incident. They also authorize attorney's fees and costs to a prevailing plaintiff.

5. ***Consumers Legal Remedies Act*** (CLRA) declares unlawful several "methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer."[271] For instance, a plaintiff may rely on the

---

[265] CAL. CIV. CODE § 56 *et seq.*
[266] *Id*. § 56.36(b).
[267] CAL. PENAL CODE § 632(a) makes it unlawful for any person to intentionally eavesdrop upon or record a confidential communication without consent of all parties, whether the communication is in person or by telephone, but excluding cellular or cordless phones; CAL. PENAL CODE § 632.7 makes it unlawful for any person to intercept, receive, or intentionally record a communication without the consent of all parties, and applies where at least one party uses a cellular or cordless phone. This Section has been construed as not requiring that the recorded communications be confidential.
[268] *Id*.
[269] *See, e.g.*, *Young v. Hilton Worldwide*, 565 Fed. App'x 595 (9th Cir. 2014), http://cdn.ca9.uscourts.gov/datastore/memoranda/2014/03/20/12-56189.pdf.
[270] CAL. BUS. & PROF. CODE §§ 17529, 17538.45, http://leginfo.legislature.ca.gov/faces/codes.xhtml.
[271] CAL. CIV. CODE §§ 1750 *et seq.*; *see, e.g.*, NEB. REV. STAT. § 87-302(14) (prohibiting knowingly making a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public.), http://nebraskalegislature.gov/laws/statutes.php?statute=87-302; 18 PA. CONS. STAT. § 4107(a)(10) (Pennsylvania's deceptive or fraudulent business practices statute prohibits false and misleading statements in privacy policies published on the Internet), https://govt.westlaw.com/pac/index.

CLRA for misrepresentations for purported tracking of Internet activity.[272] The CLRA allows consumers who suffer damage as a result of a practice declared unlawful to obtain actual damages, an order enjoining the methods, acts, or practices, restitution of property, punitive damages, court costs and attorney's fees, and any other relief that the court deems proper.[273]

[82] In addition to the California statutes that provide a private right of action for corporate actors' wrongdoing, the broad language of the Unfair Competition Law effectively allows private enforcement of a more fulsome regulatory scheme where a plaintiff has suffered damages as a result of "unlawful" actions.[274] California statutes that may be enforced through a private plaintiff's action under a UCL claim include:

1. ***The California Electronic Communications Privacy Act*** (CalECPA) requires government entities to obtain a search warrant before accessing data on an electronic device or from an online service provider.[275]

2. ***The Computer Misuse and Abuse*** law makes it a crime to knowingly access and, without permission, use, misuse, abuse, damage, contaminate, disrupt or destroy a computer, computer system, computer network, computer service, computer data or computer program.[276]

3. ***The California Data Protection Statute*** mandates that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[277] It requires a company to notify affected individuals of a data breach "in the most expedient time possible and without unreasonable delay."[278]

4. ***The Financial Information Privacy Act*** prohibits financial institutions from sharing or selling personally identifiable nonpublic information without obtaining a consumer's consent, as provided.[279] The law requires that (1) a consumer "opt in" before a financial institution may share personal information with an unaffiliated third party, (2) consumers be given an opportunity to "opt

---

[272] *Lane v. Facebook, Inc.*, No. C 08-2010 3845 RS (N.D. Cal., Mar. 17, 2010).
[273] CAL. CIV. CODE § 1780.
[274] *See* CAL. BUS. & PROF. CODE § 17200.
[275] CAL. PENAL CODE § 1546 *et seq.*
[276] *Id.* § 502.
[277] Similarly, Nevada and Minnesota require Internet Service Providers (ISPs) to keep private certain information concerning their customers, unless the customer gives permission to disclose the information. Both states prohibit disclosure of personally identifying information, but Minnesota also requires ISPs to get permission from subscribers before disclosing information about the subscribers' online surfing habits and Internet sites visited. MINN. STAT. §§ 325M.01-.09; NEV. REV. STAT. § 205.498.
[278] CAL. CIVIL CODE §§ 1798.29, 1798.82; *see also* Suevon Lee, *Sprouts' W2 Leak In Data-Phishing Scam Prompts Suit*, LAW360 (Apr. 21, 2016), http://www.law360.com/articles/787592.
[279] CAL. FIN. CODE §§ 4050 – 4060.

out" of sharing with a financial institution's financial marketing partners, and (3) consumers be given the opportunity to "opt out" of sharing with a financial institution's affiliates, with some exceptions.

5. ***The Online Privacy Protection Act of 2003*** (CalOPPA) requires operators of commercial web sites or online services that collect personal information on California consumers through a web site to conspicuously post a privacy policy on the site and to comply with its policy.[280] The privacy policy must, among other things, identify the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information.[281] The privacy policy must also provide information on the operator's online tracking practices. An operator is in violation for failure to post a policy within 30 days of being notified of noncompliance, or if the operator either knowingly and willfully or negligently and materially fails to comply with the provisions of its policy.

[83] California has had a consistently growing set of legal rules providing remedies for violations of privacy and data security. For the reasons discussed at the start of this section, these many private rights of action are more likely to be pursued due to the combination of the American rule for attorney's fees, the prevalence of contingency fees, the use of jury trial, and the availability of broad discovery.

C. Privacy-related Litigation Results in Large Class Action Settlements

[84] There is an important additional reason that US law favors plaintiffs – the use of class actions. Under Rule 23 of the Federal Rules of Civil Procedure, class actions are often available where there are "questions of law or fact common to the class" and "the claims or defenses of the representative parties are typical of the claims or defenses of the class."[282] Applied to privacy and security cases, it is easy to see how a class action can arise – there is one data breach or unlawful privacy practice that applies to numerous consumers. The single violation can lead to issues of law and fact common to the class, and a class can be certified.

[85] My review shows that settlements alone have resulted in approximately $425 million in payments to plaintiffs and government enforcement agencies nationwide over the last ten years.[283] A table at the end of this Chapter lists the major cases. A few examples of cases that yielded multi-million dollar settlements for private plaintiffs in various states include:

1. ***In re Trans Union Corp. Privacy Litigation***, filed in Illinois, resulted in a $75 million settlement where a class of aggrieved plaintiffs alleged that a consumer

[280] CAL. BUS. & PROF. CODE §§ 22575-22579, http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=.
[281] Connecticut and Delaware have implemented similar regulation. *See* CONN. GEN. STAT. § 42-471; *see also* DEL. CODE ANN. tit. 6, § 1205C.
[282] FED. R. CIV. P. 23.
[283] *See* Annex 1: Class Action Settlements 2006-2016 at 36.

reporting agency violated the Fair Credit Reporting Act and common law invasion of privacy torts by using consumer information to generate unauthorized target marketing lists.[284]

2. ***Kehoe v. Fidelity Federal Bank and Trust***, filed in Florida, yielded a $50 million settlement for a class of plaintiffs alleging that defendant bank violated the Drivers Privacy Protection Act (DPPA) by purchasing driver information for use in direct marketing.[285]

3. ***Snow v. LensCrafters, Inc.***, filed in California, resulted in a $20 million settlement for a class of plaintiffs alleging that LensCrafters mishandled and misused patients' medical and prescription information in violation of the CMIA and other consumer protection laws.[286]

4. ***In re: WebLoyalty.com, Inc., Marketing and Sales Practices Litigation***, filed in Maryland, resulted in a settlement of $10 million to a class of Plaintiffs alleging that Webloyalty secretly enrolled consumers in a sham discount program as a result of information they provided on various websites in violation of Electronic Funds Transfer Act (EFTA) and ECPA.[287]

[86] In large-scale litigation, plaintiffs serve a functionally similar role as the US government in enforcing consumer protection laws and regulating industries.[288] Private litigation – and the threat of it – continues to lead to more effective compliance by organizations to protect consumers' privacy.

V. Standing to Sue after *Clapper*

[87] The Irish Data Protection Commissioner (DPC) has filed an Affidavit which states that "the 'standing' admissibility requirements of the US federal courts operate as a constraint on all forms of relief available" in the US.[289] This statement appears to refer to the discussion of the US

---

[284] *In re Trans Union Corp. Priv. Litig.*, No. 13-1613 (7th Cir. Jan. 23, 2014), http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2014/D01-23/C:13-1613:J:Hamilton:aut:T:fnOp:N:1278615:S:0 (holding that Trans Union did not violate $75 million settlement when it used those funds to resolve claims arising after the settlement was finalized).

[285] *Kehoe v. Fidelity Federal Bank and Trust*, No. 03-80593-CIV (S.D. Fla. August 1, 2006); *see* K.C. Jones, *Bank to Pay $50 Million for Buying Personal Data*, INFORMATIONWEEK (Aug. 29, 2006), http://www.informationweek.com/bank-to-pay-$50-million-for-buying-personal-data/d/d-id/1046571.

[286] *Snow v. LensCrafters, Inc.*, CGC-02-405544 (Cal. App. Dep't Super. Ct. July 11, 2008); *see* Pete Brush, *LensCrafters Settles $20 Million Indemnification Battle*, LAW360 (Mar. 31, 2009), http://www.law360.com/articles/94630/lenscrafters-settles-20m-indemnification-battle.

[287] *In Re: Webloyalty.com, Inc., Marketing and Sales Practices Litigation*, No. 1:07-MD-018-JLT (D. Mass. Jan. 28, 2009); *see* Julie Zeveloff, *Webloyalty To Pay Back $10M In Fees In MDL Deal*, LAW360 (Feb. 24, 2009), http://www.law360.com/articles/88713/webloyalty-to-pay-back-10m-in-fees-in-mdl-deal.

[288] *See* W. Olson, *Regulation through Litigation*, POINTOFLAW (Aug. 30, 2005) http://www.pointoflaw.com/regulation/overview.php.

[289] *See* Affidavit of John V. O'Dwyer, *Data Protection Comm'r v. Facebook Ireland Ltd*, No. 2016/4809P, para. 93 (filed July 4, 2016) (H.C.).

Supreme Court case *Clapper v. Amnesty International USA* in the DPC's Draft Decision.[290] In *Clapper*, Amnesty International and other plaintiffs brought a constitutional challenge to Section 702 of FISA on the day after it entered into force in 2008.[291] The Supreme Court dismissed the challenge because it found the plaintiffs did not show an injury that granted them standing to sue.

[88] It would be a mistake to read more into *Clapper* than it actually holds. In one sense, I agree with the quotation from the DPC, in the sense that a plaintiff does have to establish standing to sue in order to get relief from a US court. The case should not, however, be read to create a *per se* ban on cases involving US foreign intelligence or counterterrorism programs. Two lower courts, for instance, have found that individuals had standing in the foreign intelligence realm, to challenge the Section 215 telephone metadata program.[292] Another court found, in a counter-terrorism setting, that an individual had standing to challenge suspected placement on the terrorist watch list.[293] The facts and law of the individual case will determine whether an individual has standing to sue.

[89] One concern the Supreme Court identified in *Clapper* is that when US surveillance is challenged in court, affirming or denying an individual's standing to bring the challenge permits him – or an adversary watching the case – "to determine whether he is currently under US surveillance simply by filing a lawsuit."[294] This statement in *Clapper* is consistent with my discussion in Chapter 8, on how hostile actors can seek to use individual remedies to probe an intelligence agency and to learn its national security secrets. Chapter 8 explains in detail how an adversary intelligence agency could deploy an individual remedy to conduct such probes.[295] It also documents how courts in both the EU and US have a clear history of caution about disclosing national security secrets in open court.[296]

[90] Nor has *Clapper* turned out to prevent individuals from bringing lawsuits against companies that commit privacy violations, even in the absence of out-of-pocket damages. Since *Clapper* was decided in 2013, US courts have accepted major class-action litigation against companies such as Adobe Systems[297] and Sony[298] following data breaches. In a number of these cases, courts have affirmed individuals' standing on allegations that data was obtained by unauthorized third parties, without requiring individuals to show any financial or other loss.[299]

---

[290] *See* Draft Decision of the Data Protection Comm'r, *Schrems v. Facebook Ireland Ltd*, No. 3/15/766, para. 55 (May 24, 2016).
[291] *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013).
[292] *See, e.g., Am. C.L. Union v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015) (finding that standing existed to challenge the Section 215 metadata program); *Klayman v. Obama*, 142 F. Supp. 3d 172, 186 (D.D.C. 2015) (same).
[293] *Shearson v. Holder*, 725 F.3d 588, 593 (6th Cir. 2013) (holding that individual had standing to challenge her suspected placement on the terrorist watch list, even though the court found "it is impossible for [her] to prove that her name remains on that list").
[294] *Clapper*, 131 S. Ct. at 1149 n.4.
[295] *See* Chapter 8, Section I(C).
[296] *See* Chapter 8, Sections II-IV.
[297] *See In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014).
[298] *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014).
[299] *See, e.g., Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, 2016 WL 4728027, at *3 (6th Cir. Sept. 12, 2016); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 694 (7th Cir. 2015); *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-08617, 2016 WL 5720370, at *4 (N.D. Ill. Oct. 3, 2016), https://docs.justia.com/cases/federal/district-

[91] In addition, the doctrine of standing addressed in *Clapper* pertains only to the US federal courts, and thus at most impacts judicial remedies. This Chapter has identified multiple ways that individuals can seek to address privacy violations in the US, including: judicial remedies; non-judicial remedies (such as the PCLOB and the free press); administrative agency remedies (such as the FTC and FCC); state Attorneys General; and new remedies provided by the Ombudsman and the Umbrella Agreement. Only federal judicial remedies are affected by even the broadest reading of *Clapper*.

[92] All of the above gives reason for caution in interpreting the implications of *Clapper*. Moreover, the DPC has suggested that her findings on the effects of standing may need to be reassessed in light of the Ombudsman and the Umbrella Agreement.[300] Through the Ombudsman mechanism, EU individuals can now lodge complaints regarding US government collection of data. Ombudsman complaints can be brought regardless of whether individuals can show that personal data has been collected, and without needing to show that harm or other adverse consequences were suffered. Similarly, individuals can exercise access rights under the Umbrella Agreement without having to show harm.

VI. Conclusion

[93] This Chapter has sought to present in an organized and understandable way the US system for individual remedies for privacy violations. Section I described judicial remedies against the US government. Section II described non-judicial remedies against the US government, including through complaints to potentially effective organizations. Section III described how suits against non-governmental entities operate, including suits against service providers who provide more information to the government than is allowed. Section IV filled out the enforcement landscape by explaining the role of state law, private rights of action, and class actions in promoting privacy compliance.

[94] As stated in the introduction to this Chapter, these individual remedies complement the systemic safeguards in the US system. Both individual remedies and systemic safeguards play important roles, as discussed further in my Summary of Testimony.

courts/illinois/ilndce/1:2012cv08617/275913/130; *In re Anthem, Inc. Data Breach Litig*., 162 F. Supp. 3d 953, 995 (N.D. Cal. 2016) (holding that "loss of value of personally identifiable information" following a data breach was an injury sufficient to confer standing); *Moyer v. Michaels Stores, Inc*., No. 14 C 561, 2014 WL 3511500, at *6 (N.D. Ill. July 14, 2014), http://il.findacase.com/research/wfrmDocViewer.aspx/xq/fac.20140714_0001468.NIL.htm/qx.

[300] *See* Plaintiff's Reply to the Defence of the First Named Defendant, *Data Protection Comm'r v. Facebook Ireland Ltd*, No. 2016/4809P (filed Sept. 30, 2016) (H.C.), paras. 6(1) & 6(2). The DPC states that "the Draft Decision also needs to be read in the context of the new [Ombudsman mechanism]," and "may need to be read in light of the signing of the 'Umbrella Agreement.'" The DPC states it "could not have had regard" to the Ombudsman or the Umbrella Agreement in reaching its Draft Decision, because neither mechanism had been "implemented at the date of the adoption of the Draft Decision." *Id.*

Annex 1: US Privacy Remedies and Safeguards: Availability to EU Persons

Protection	Authority	Available to EU persons?
Remedy – Petition to US State Department Ombudsman for privacy violations under Privacy Shield, SCCs, or BCRs.[301]	EU-US Privacy Shield Framework	Yes
Remedy – Independent alternative dispute resolution body for privacy violations by Privacy Shield.[302]	EU-US Privacy Shield Framework	Yes
Remedy – Petition for access, correction, or rectification of data sent to US law enforcement.[303]	Umbrella Agreement	Yes
Remedy – Suit against importing or exporting data controller under Standard Contractual Clauses.[304]	Standard Contractual Clauses	Yes
Remedy – Civil suit against US agency and/or individual who unlawfully shares stored content.[305]	Stored Communications Act	Yes
Remedy - Suit against US federal agency for improper handling of data.[306]	Judicial Redress Act, Privacy Act	Yes
Remedy – Civil suit against individuals who unlawfully intercept communications.[307]	Wiretap Act	Yes

[301] *See* Chapter 7, Section I(A)(1) ("Judicial Redress Act, Privacy Shield, and the Umbrella Agreement").
[302] *See id.*
[303] *See id.*
[304] *See id.*
[305] *See* Chapter 7, Section I(A)(2) ("Electronic Communications Privacy Act – Stored Communications Act").
[306] *See* Chapter 7, Section I(A)(1) ("Judicial Redress Act, Privacy Shield, and the Umbrella Agreement").
[307] *See* Chapter 7, Section I(A)(3) ("ECPA – The Wiretap Act").

Protection	Authority	Available to EU persons?
Remedy – Civil suits against individual government officer for unauthorized surveillance.[308]	Foreign Intelligence Surveillance Act	Yes[309]
Remedy – Criminal charges for unlawful access to stored communications.[310]	Stored Communications Act	An EU or US person can petition the US government to pursue criminal charges under its sovereign authority.
Remedy – Criminal charges for unlawful interception of communications.[311]	Electronic Communications Privacy Act	An EU or US person can petition the US government to pursue criminal charges under its sovereign authority.
Remedy – Criminal charges for unauthorized surveillance or disclosure of unauthorized surveillance.[312]	Foreign Intelligence Surveillance Act	An EU or US person can petition the US government to pursue criminal charges under its sovereign authority.
Remedy – Exclusion of unlawfully obtained electronic evidence in a criminal proceeding.[313]	US Constitution, Fourth Amendment	Yes
Remedy – Access to classified evidence necessary to a fair criminal defense.[314]	Confidential Information Procedures Act	Yes
Remedy – Lodge a complaint or request for further investigation with the Privacy and Civil Liberties Oversight Board.[315]	Privacy and Civil Liberties Oversight Board	Yes

[308] *See* Chapter 7, Section I(A)(4) ("Foreign Intelligence Surveillance Act").
[309] Except for individuals who are a "foreign power" or an "agent of a foreign power." 50 U.S.C. § 1801(a)-(b).
[310] *See* Chapter 7, Section I(B) ("US Criminal Judicial Remedies").
[311] *See id.*
[312] *See id.*
[313] *See id.*
[314] *See id.*
[315] *See* Chapter 7, Section II(A) ("The PCLOB").

Protection	Authority	Available to EU persons?
Remedy – Lodge a complaint or request for further investigation with Congressional Intelligence Committees.[316]	Rules of the House of Representatives, Rules of the Senate	Yes
Remedy – Petition the US free press to investigate and report on alleged privacy harms.[317]	US Constitution, First Amendment	Yes
Remedy – Petition companies to communicate data sharing practices through transparency reports.[318]	USA FREEDOM Act	Yes
Remedy – Petition US non-governmental organizations to address alleged privacy harms.[319]	US Constitution, First Amendment	Yes
Remedy – Civil suit against companies that unlawfully share stored communications data with the US government.[320]	Stored Communications Act	Yes
Remedy – Civil suit against persons or entities that unlawfully intercept, disclose, or use surveillance data.[321]	Wiretap Act	Yes
Remedy – Petition to the Federal Trade Commission to investigate alleged privacy harms.[322]	Federal Trade Commission Act	Yes

[316] *See* Chapter 7, Section II(B) ("Congressional Committees").
[317] *See* Chapter 7, Section II(C) ("Individual Remedies through Public Press and Advocacy")
[318] *See id.*
[319] *See id.*
[320] *See* Chapter 7, Section III(A)(1) ("Stored Communications Act").
[321] *See* Chapter 7, Section III(A)(2) ("Wiretap Act").
[322] *See* Chapter 7, Section III(B)(1) ("The FTC").

Protection	Authority	Available to EU persons?
Remedy – Petition to the Federal Communications Commission to investigate alleged privacy harms.[323]	Telecommunications Act	Yes
Remedy – Petition to the Consumer Financial Protection Bureau to investigate alleged privacy harms.[324]	Dodd-Frank Wall Street Reform and Consumer Protection Act	Yes
Remedy – Petition to the Securities and Exchange Commission to investigate alleged privacy harms.[325]	Securities Act	Yes
Remedy – Petition to the Department of Health and Human Services Office of Civil Rights to investigate alleged privacy harms.[326]	Health Insurance Portability and Accountability Act	Yes
Remedy – Petition to US state Attorneys General to investigate and/or prosecute alleged privacy harms.[327]	Various state laws	Yes
Remedy – Private rights of action against US companies for violations of privacy laws and protections under US state and federal law.[328]	Various state and federal laws.	Any limitations on who may bring a suit are determined according to the statute the suit alleges was violated.
Remedy – Class-action litigation for alleged privacy harms.[329]	Various state and federal laws.	Any limitations on who may bring a suit are determined according to the statute the suit alleges was violated.

[323] *See* Chapter 7, Section III(B)(2) ("The FCC").
[324] *See* Chapter 7, Section III(B)(3) ("The CFPB").
[325] *See* Chapter 7, Section III(B)(4) ("The SEC").
[326] *See* Chapter 7, Section III(B)(5) ("The Department of Health and Human Services").
[327] *See* Chapter 7, Section IV(A) ("State Attorney General ('AG') Enforcement").
[328] *See* Chapter 7, Section IV(B) ("Private Rights of Action").
[329] *See* Chapter 7, Section IV(C) ("Privacy-related Litigation Results in Large Class Action Settlements").

Protection	Authority	Available to EU persons?
Safeguard – Oversight of law enforcement searches by independent judicial officers.[330]	US Constitution, Article III	Yes
Safeguard – Requirement of probable cause for physical and digital law enforcement searches.[331]	US Constitution, Fourth Amendment	Yes
Safeguard – "Probable cause plus" requirement for law enforcement wiretaps and real-time interception.[332]	Wiretap Act	Yes
Remedy – Civil suit against law enforcement officials that perform an unlawful search under the Fourth Amendment.[333]	US Constitution, Fourth Amendment	Yes if in the US at the time of the search
Safeguard – Proof-based legal standard for government access in US non-search situations.[334]	Electronic Communications Privacy Act	Yes
Safeguard – Transparency requirements for searches, including notice requirements.[335]	Electronic Communications Privacy Act	Yes
Safeguard – Lack of data retention requirements for Internet communications.[336]	N/A	Yes
Safeguard – Lack of limits on use of strong encryption by persons and businesses.[337]	N/A	Yes

[330] *See* Chapter 4, Section II(A) ("Oversight of Searches by Independent Judicial Officers").
[331] *See* Chapter 4, Section II(B) ("Probable Cause of a Crime as a Relatively Strict Requirement for Both Physical and Digital Searches").
[332] *See* Chapter 4, Section II(C) ("Even Stricter Requirements for Government Use of Telephone Wiretaps and Other Real-time Interception").
[333] *See* Chapter 4, Section II(D) ("The Exclusionary Rule, Preventing Prosecutors' Use of Evidence that Was Illegally Obtained, and Civil Suits").
[334] *See* Chapter 4, Section II(E) ("Other Legal Standards that are Relatively Strict for Government Access in Many Non-Search Situations, such as the Judge-Supervised 'Reasonable and Articulable Suspicion' Standard under ECPA").
[335] *See* Chapter 4, Section II(F) ("Transparency Requirements, such as Notice to the Service Provider of the Legal Basis for a Request").
[336] *See* Chapter 4, Section II(G) ("Lack of Data Retention Rules for Internet Communications").
[337] *See* Chapter 4, Section II(H) ("Lack of Limits on Use of Strong Encryption").

Protection	Authority	Available to EU persons?
Safeguard – Institutional checks and balances on US government authority.[338]	US Constitution	Yes
Safeguard – Independent judicial review of alleged privacy harms.[339]	US Constitution, Article III	Yes
Safeguard – Constitutional protections of individual rights, including privacy.[340]	US Constitution, Bill of Rights	Yes
Safeguard – Democratic accountability for government officials.[341]	US Constitution	Yes
Safeguard – Surveillance reforms after the Snowden disclosures and Presidential Review Group on Intelligence and Communications Technology Report.[342]	EU-US Privacy Shield, Judicial Redress Act, Umbrella Agreement, others.	Yes
Safeguard – Foreign Intelligence Surveillance Court review and oversight of foreign intelligence surveillance practices.[343]	Foreign Intelligence Surveillance Act	Yes
Safeguard – Removal of authority for bulk collection surveillance practices.[344]	USA FREEDOM Act	Yes
Safeguard – Limits on surveillance practices under Section 702 of the FISA Act.[345]	Foreign Intelligence Surveillance Act, Privacy and Civil Liberties Oversight Board Report on Section 702	Yes

[338] *See* Chapter 3, Section I(A) ("A Time-Tested System of Checks and Balances").
[339] *See* Chapter 3, Section I(B) ("Judicial Independence").
[340] *See* Chapter 3, Section I(C) ("Constitutional Protections of Individual Rights").
[341] *See* Chapter 3, Section I(D) ("Democratic Accountability").
[342] *See* Chapter 3, Section II(C) ("The Reforms after the Snowden Disclosures").
[343] *See* Chapter 3, Section III(A)(1) ("The Structure of the FISC under FISA").
[344] *See* Chapter 3, Section III(B) ("Collection of Documents and Other Tangible Things under Section 215").
[345] *See* Chapter 3, Section III(C)(1) ("The Legal Structure of Section 702").

Protection	Authority	Available to EU persons?
Safeguard – Tasking selector limitations on Upstream collection.[346]	Privacy and Civil Liberties Oversight Board Report on Section 702	Yes
Safeguard – Oversight by executive agency Inspectors General.[347]	Inspector General Act	Yes
Safeguard – Congressional oversight and investigation of foreign intelligence activities.[348]	US Constitution Article II, Rules of the House of Representatives, Rules of the Senate	Yes
Safeguard – Independent review by the Presidential Review Group.[349]	N/A	Yes
Safeguard – Independent oversight and review by the Privacy and Civil Liberties Oversight Board.[350]	9/11 Commission Act	Yes
Safeguard – Office of the Director of National Intelligence oversight of the intelligence community.[351]	US Constitution, Article II	Yes
Safeguard – Federal Privacy Council for US government agencies stewardship and assistance to federal agency privacy professionals.[352]	Executive Order 13,719	Yes
Safeguard – Executive branch transparency about surveillance activities, including declassified FISC opinions.[353]	USA FREEDOM Act	Yes

[346] *See* Chapter 3, Section III(C)(3) ("The Upstream Program").
[347] *See* Chapter 3, Section IV(A) ("Executive Agency Inspectors General").
[348] *See* Chapter 3, Section IV(B) ("Legislative Oversight").
[349] *See* Chapter 2, Section (B)(4) ("President Obama's Review Group on Intelligence and Communications Technology, 2013-14").
[350] *See* Chapter 3, Section IV(C) ("Independent Review: Review Group and PCLOB").
[351] *See* Chapter 3, Section IV(D) ("The Federal Privacy Council and Privacy and Civil Liberties Offices in the Agencies").
[352] *See id.*
[353] *See* Chapter 3, Section V(A) ("Greater Transparency by the Executive Branch about Surveillance Activities").

Protection	Authority	Available to EU persons?
Safeguard – USA FREEDOM Act provisions mandating public law about major FISC decisions.[354]	USA FREEDOM Act	Yes
Safeguard – Transparency reports by the US Government regarding national security investigations.[355]	USA FREEDOM Act	Yes
Safeguard – US intelligence community Statistical Transparency Reports.[356]	USA FREEDOM Act	Yes
Safeguard – Company issued transparency reports on the range of orders they have replied to.[357]	USA FREEDOM Act	Yes
Safeguard – Principle in signals intelligence activities to protect the privacy rights of non-US persons.[358]	Presidential Policy Directive 28	Yes
Safeguard – Protection of civil liberties of foreign persons beyond privacy.[359]	Presidential Policy Directive 28	Yes
Safeguard – Minimization of personal information acquired during signals intelligence activities.[360]	Presidential Policy Directive 28	Yes
Safeguard – Limits on the retention and dissemination of signals intelligence.[361]	Presidential Policy Directive 28	Yes

[354] *See* Chapter 3, Section V(B) ("USA FREEDOM Act Provisions Mandating Public Law about Major FISC Decisions").
[355] *See* Chapter 3, Section V(D) ("Transparency Reports by the US Government").
[356] *See id.*
[357] *See* Chapter 3, Section V(E) ("Transparency Reports by Companies").
[358] *See* Chapter 3, Section VI(B)(1) ("Privacy is Integral to the Planning of Signals Intelligence Activities").
[359] *See* Chapter 3, Section VI(B)(2) ("Protection of Civil Liberties in Addition to Privacy").
[360] *See* Chapter 3, Section VI(B)(3) ("Minimization Safeguards").
[361] *See* Chapter 3, Section IV(B)(4) ("Retention, Dissemination, and Other Safeguards for Non-US Persons Similar to Those for US Persons").

Protection	Authority	Available to EU persons?
Safeguard – Purpose limitations on signals intelligence collected in large quantities without the use of discriminants.[362]	Presidential Policy Directive 28	Yes
Safeguard – Prohibition of the use of signals intelligence to gain a competitive advantage for US companies and the US business sector commercially.[363]	Presidential Policy Directive 28	Yes
Safeguard – Publication of implementation procedures under Presidential Policy Directive 28.[364]	Presidential Policy Directive 28	Yes
Safeguard – Requirement to use selectors and identifiers to focus intelligence collections.[365]	Presidential Policy Directive 28	Yes
Safeguard – White House oversight of foreign intelligence procedures.[366]	Presidential Policy Directive 28	Yes
Safeguard – White House process to disclose software vulnerabilities.[367]	US Constitution, Article II	Yes
Safeguard – Umbrella Agreement data protection framework for data exchanged between the EU and US for law enforcement purposes.[368]	Umbrella Agreement	Yes
Safeguard – Privacy Shield creation of commitments from the US government to	US EU Privacy Shield Framework	Yes

[362] *See* Chapter 3, Section IV(B)(5) ("Limits on Bulk Collection of Signals Intelligence").
[363] *See* Chapter 3, Section IV(B)(6) ("Limits on Surveillance to Gain Trade Secrets for Commercial Advantage").
[364] *See* Chapter 3, Section IV(B)(7) ("Discussion of PPD-28").
[365] *See id.*
[366] *See* Chapter 3, Section IV(C) ("New White House Oversight of Sensitive Intelligence Collection, including of Foreign Leaders").
[367] *See* Chapter 3, Section IV(D) ("New White House Process to Help Fix Software Flaws, rather than Use Them for Surveillance").
[368] *See* Chapter 3, Section IV(F) ("The Umbrella Agreement as a Systemic Safeguard").

Protection	Authority	Available to EU persons?
address EU data protection concerns and work with EU DPAs.[369]		

[369] *See* Chapter 3, Section IV(G) ("Privacy Shield as a Systemic Safeguard").

Annex 2: Class Action Settlements 2006-2016

Total Settlement Amount: $425,005,400

Case	Claims	Settlement Amount	Case Citation
In re Trans Union Corp. Privacy Litigation, No. 1:00-cv-04729 (N.D. Ill. May 30, 2008)	Plaintiffs alleged that consumer reporting agency violated the FCRA by using consumer credit information to generate target marketing lists and by providing those lists to its consumers. Claims included violations of the FCRA, invasion of privacy, misappropriation, violation of the Cal. UCL, and unjust enrichment.	$75,000,000	*In re Trans Union Corp. Priv. Litig.*, No. 13-1613 (7th Cir. Jan. 23, 2014) (holding that Trans Union did not violate $75 million settlement when it used those funds to resolve claims arising after the settlement was finalized), http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2014/D01-23/C:13-1613:J:Hamilton:aut:T:fnOp:N:1278615:S:0.
Kehoe v. Fidelity Federal Bank and Trust, No. 03-80593-CIV (S.D. Fla. Aug. 1, 2006)	Plaintiffs alleged bank violated the DPPA when it purchased 565,000 names and addresses for use in direct marketing.	$50,000,000	K.C. Jones, *Bank to Pay $50 Million for Buying Personal Data*, INFORMATIONWEEK (Aug. 29, 2006, 4:32 PM), http://www.informationweek.com/bank-to-pay-$50-million-for-buying-personal-data/d/d-id/1046571.

Case	**Claims**	**Settlement Amount**	**Case Citation**
United States v. Google, Inc., 3:12-cv-04177-SI (N.D. Cal. Aug. 9, 2012)	FTC alleged that Google violated a consent order by circumventing privacy settings for Apple's Safari browser despite promising to honor them. The FTC claimed violations of the FTCA arising from collecting information covered in the consent order, serving targeted advertisements, and misrepresenting code compliance. Google also settled with the Attorneys General of 37 states.	$39,500,000	Claire Cain Miller, *Google to Pay $17 Million to Settle Privacy Case*, N.Y. TIMES, Nov. 18, 2013, http://www.nytimes.com/2013/11/19/technology/google-to-pay-17-million-to-settle-privacy-case.html?_r=0.
In re: EasySaver Rewards Litigation, MDL No. 09-2094 (S.D. Cal. Feb. 4, 2013)	Plaintiffs alleged that Provide Commerce transmitted its consumers' private payment information to third-party marketing partners, who then charged consumer's credit accounts without permission under the guise that the consumer supposedly joined savings programs such as EasySaver Rewards. Plaintiffs claimed violations of the California unfair competition law, the California Consumers Legal Remedies Act, and the Federal Electronics Funds Transfer Act. They also alleged fraud, breach of contract, breach of the implied covenant of good faith and fair dealing, invasion of privacy, unjust enrichment and negligence.	$21,365,000	Megan Leonhardt, *ProFlowers Parent Co. Arranges $38M Deal Over Data Policies*, LAW360 (June 14, 2012, 2:19 PM), http://www.law360.com/articles/350092/proflowers-parent-co-arranges-38m-deal-over-data-policies.

Case	**Claims**	**Settlement Amount**	**Case Citation**
In Re: Department of Veterans Affairs (VA) Data Theft Litigation, MDL No. 1796, Action No. 06-0506 (D.D.C. Sep. 11, 2009), https://www.courtlistener.com/opinion/2667294/in-re-department-of-veterans-affairs-va-data-theft/.	This litigation centered on a stolen external hard drive that contained the personal information of millions of veterans. The plaintiffs claimed that the VA showed a reckless disregard for veterans' privacy rights and an intentional and willful disregard for Privacy Act requirements by failing to interview the employee in question until 12 days after the theft and five days after the VA's inspector general learned of the theft.	$20,000,000	Associated Press, *$20 Million Settlement Reached for Veterans in ID Theft Suit*, N.Y. TIMES, Jan. 27, 2009, http://www.nytimes.com/2009/01/28/washington/28vets.html.
Fraley v. Facebook, Inc., No. 5:11-cv-0176 (N.D. Cal. Aug. 26, 2013)	Plaintiffs alleged that Facebook used members' pictures in ads without their consent.	$20,000,000	Emily Field, *Facebook's $20M Ad Settlement Kosher, 9th Cir. Says*, LAW360 (Jan. 6, 2016, 5:54 PM), http://www.law360.com/articles/743306/facebook-s-20m-ad-settlement-kosher-9th-circ-says.
Snow v. LensCrafters, Inc., CGC-02-405544 (Cal. Sup. Ct. July 11, 2008)	Plaintiffs alleged that the optometrists and LensCrafters mishandled and misused the patients' medical and prescription information in violation of California's CMIA and other consumer protection laws.	$20,000,000	Pete Brush, *LensCrafters Settles $20 Million Indemnification Battle*, LAW360 (Mar. 31, 2009, 12:00 AM), http://www.law360.com/articles/94630/lenscrafters-settles-20m-indemnification-battle.

Case	**Claims**	**Settlement Amount**	**Case Citation**
Marenco v. Visa, Inc., 2:10-cv-08022 (C.D. Cal. Nov. 30, 2011)	Plaintiff alleged Visa recorded thousands of telephone calls to customer service representatives without permission or disclosure. Plaintiff claimed this violated recording laws in several states.	$18,000,000	Bibeka Shrestha, *Visa Hangs Up Call Recording Class Action For $18M*, LAW360 (Oct. 24, 2011, 5:36 PM), http://www.law360.com/articles/280110/visa-hangs-up-call-recording-class-action-for-18m.
Harris v. ComScore Inc., No. 1:11-cv-05807 (N.D. Ill. May 30, 2014)	Plaintiffs alleged that online data analytics company ComScore installed data harvesting software on users' computers without consent, which allowed them to surveil and sell private information. Plaintiffs claimed violations of the SCA, ECPA, and other causes of action.	$14,000,000	Andrew Scurria, *ComScore Pays $14M To Escape Massive Privacy Class Action*, LAW360 (June 4, 2014, 2:54 PM), http://www.law360.com/articles/544569/comscore-pays-14m-to-escape-massive-privacy-class-action
Perkins v. LinkedIn Corp., 5:13-cv-04303 (N.D. Cal. Sep. 15, 2015), https://casetext.com/case/perkins-v-linkedin-corp-2	Plaintiffs asserted that LinkedIn took users' email addresses and used them to harvest additional email addresses from the users' external accounts. They alleged that LinkedIn used the email addresses to send an initial contact and at least two follow-up emails to those in the users' address books, making it look like the email was sent or endorsed by the user, in an effort to acquire more members, especially premium-paying members. Plaintiffs claimed that they did not agree to allow the emails to be sent.	$13,000,000	Seung Lee, *LinkedIn to pay $13 Million in Suit Settlement for Excessively Spamming Users*, NEWSWEEK (Oct. 5, 2015, 2:59 PM), http://www.newsweek.com/linkedin-13-million-class-action-lawsuit-emails-379975.

Case	**Claims**	**Settlement Amount**	**Case Citation**
Reed v. 1-800 Contacts, Inc., MDL No. 12-2359 (S.D. Cal. Jan. 2, 2014)	1-800-Contacts allegedly recorded telephone calls made to and received from California residents without their consent in violation of the CIPA.	$11,700,000	Juan Carlos Rodriguez, *1-800 Contacts Agrees To Pay $11.7M In Call-Recording Suit*, LAW360 (Nov. 19, 2013, 5:01 PM), http://www.law360.com/articles/489934/1-800-contacts-agrees-to-pay-11-7m-in-call-recording-suit.
Utility Consumer's Action Network v. Bank of America, N.A., No. CJC-01-004211 (Cal. App. Dep't Super. Ct. Apr. 12, 2007)	Plaintiffs alleged that the Bank of America disclosed nonpublic, personal information belonging to its customers to third-party marketers in exchange for money, without customers' consent or proper notice. They alleged unlawful, unfair and fraudulent business practices, invasion of privacy and unjust enrichment.	$10,750,000	CENTER FOR JUSTICE AND DEMOCRACY AT N.Y. LAW SCHOOL, CLASS ACTIONS ARE CRITICAL TO REMEDY INVASIONS OF PRIVACY (2014), https://centerjd.org/system/files/ClassActionPrivacyF.pdf.
In Re: Webloyalty.com, Inc., Marketing and Sales Practices Litigation, No. 1:07-MD-018-JLT (D. Mass. Jan. 28, 2009)	Plaintiffs alleged that Webloyalty secretly enrolled consumers in a $7-10/month sham discount program if they filled out a discount pop-up on websites such as Priceline and Fandango. Part of this process included obtaining card information from the retailer without the consumer's consent. The class sought relief under the EFTA, ECPA, and Civil Theft.	$10,000,000	Julie Zeveloff, *Webloyalty To Pay Back $10M In Fees In MDL Deal*, LAW360 (Feb. 24, 2009, 12:00 AM), http://www.law360.com/articles/88713/webloyalty-to-pay-back-10m-in-fees-in-mdl-deal.

Case	**Claims**	**Settlement Amount**	**Case Citation**
Lane v. Facebook, Inc., No. C 08-3845 RS (N.D. Cal. Mar. 17, 2010)	Plaintiffs alleged Facebook transmitted personal information obtained from its Beacon program websites back to the Facebook site without the consent of the user. They claimed violations of ECPA, the Video Privacy Protection Act (VPPA), and state law.	$9,500,000	Juan Carlos Perez, *Facebook Will Shut Down Beacon to Settle Lawsuit*, N.Y. TIMES, Sept. 19, 2009, http://www.nytimes.com/external/idg/2009/09/19/19idg-facebook-will-shut-down-beacon-to-settle-lawsuit-53916.html.
Batmanghelich v. Sirius XM Radio Inc., No. 09-cv-09190 (C.D. Cal. Mar. 7, 2011)	Plaintiffs in five states alleged that Sirius XM was illegally recording phone calls in violation of state privacy statutes.	$9,500,000	Richard Vanderford, *Sirius Settles Privacy Suit With 5 States For $9.5M*, LAW360 (Mar. 11, 2011, 11:13 PM), http://www.law360.com/articles/232199/sirius-settles-privacy-suit-with-5-states-for-9-5m.
In re Carrier iQ Inc. Consumer Privacy Litigation, No. 3:12-md-02330 (N.D. Cal. Jan. 22, 2016)	Plaintiffs alleged that Carrier IQ's software, which was designed to help determine the cause of dropped cell phone calls, was transmitting sensitive information from users' phones. The plaintiffs claimed violations of the Federal Wiretap Act and many state privacy acts and consumer protection laws.	$9,000,000	Joe Van Acker, *Carrier IQ, Samsung Ink $9M Deal To End Privacy Suit*, LAW360 (Jan. 25, 2016, 5:18 PM), http://www.law360.com/articles/750372/carrier-iq-samsung-ink-9m-deal-to-end-privacy-suit.

Case	**Claims**	**Settlement Amount**	**Case Citation**
In re Netflix Privacy Litigation, 5:11-cv--00379 (N.D. Cal. Mar. 18, 2013), http://www.leagle.com/decision/In%20FDCO%2020130319A55/IN%20RE%20NETFLIX%20PRIVACY%20LITIGATION	Plaintiffs alleged that Netflix kept former customers' information long after the users had canceled their accounts. They claimed this practice violated a provision of the VPPA.	$9,000,000	Allison Grande, *Netflix Tells 9th Circ. Its $9M Privacy Deal Passes Muster*, LAW360 (Oct. 31, 2013, 7:56 PM), http://www.law360.com/articles/485252/netflix-tells-9th-circ-its-9m-privacy-deal-passes-muster.
In re Google Buzz Privacy Litigation, 5:10-cv-00672-JW (N.D. Cal. Sep. 3, 2010), https://epic.org/privacy/ftc/googlebuzz/buzz_settlement.pdf	Plaintiffs alleged that Google Buzz, a social networking product, violated their privacy by creating publically-available lists of networking contacts based on an individual's email and chat history. Plaintiffs claimed this practice violated ECPA.	$8,500,000	Ben Parr, *Google Settles Buzz Privacy Lawsuit for $8.5 Million*, MASHABLE (Sept. 3, 2010), http://mashable.com/2010/09/03/google-buzz-lawsuit-settlement/#ePEqKHR5mkqf.
In re Google Referrer Header Privacy Litigation; No. 10-cv-04809 (N.D. Cal. Mar. 31, 2015), https://casetext.com/case/in-re-google-referrer-header-privacy-litig-1	Plaintiffs alleged that Google improperly provided websites with the Google search terms directing a particular user to that website and that the search terms contained personal information. Plaintiffs claimed this violated the SCA.	$8,500,000	*Google Agrees to Pay $8.5 Million to Settle Claims It Disclosed Internet Search Queries*, BLOOMBERG BNA (July 29, 2013), http://www.bna.com/google-agrees-pay-n17179875501/.

Case	**Claims**	**Settlement Amount**	**Case Citation**
Kinder v. Meredith Corp., No. 1:14-cv-11284 (E.D. Mich. Feb. 4, 2016)	Plaintiffs claimed that Meredith Corp. violated Michigan's Video Rental Privacy Act by disclosing subscribers' personal data.	$7,500,000	Allison Grande, *$7.5M Deal In Mich. Magazine Privacy Row Gets Initial Nod*, LAW360 (Feb. 5, 2016, 10:28 PM), http://www.law360.com/articles/755931/7-5m-deal-in-mich-magazine-privacy-row-gets-initial-nod.
Mount v. Wells Fargo Bank, N.A., No. B260585 (Cal. App. Ct. Feb. 9, 2016), http://www.courts.ca.gov/opinions/nonpub/B260585.PDF	Plaintiffs alleged that Wells Fargo secretly recorded customer service phone calls in violation of CalCIPA. The California Court of Appeals affirmed the settlement.	$5,600,000	Joe Van Acker, *Calif. Court Upholds $5.6M Wells Fargo Privacy Settlement*, LAW360 (Feb. 11, 2016, 1:46 PM), http://www.law360.com/articles/758023/calif-court-upholds-5-6m-wells-fargo-privacy-settlement.
Cohorst v. BRE Properties, Inc., No. 3:10-cv-02666 (S.D. Cal. Apr. 29, 2011)	Plaintiffs alleged that BRE properties recorded phone conversations without notice or consent. Their claims included recording laws from 14 states as well as common law invasion of privacy and negligence counts.	$5,500,000	*Cohorst v. BRE Props.*, No. 3:10-CV-2666-JM-BGS, 2011 U.S. Dist. LEXIS 151719 (S.D. Cal. Nov. 9, 2011) (approving $5.5 million settlement for approximately 1,300 people who made calls that were recorded by company without consent).

Case	**Claims**	**Settlement Amount**	**Case Citation**
Coulter-Owens v. Rodale Inc., No. 2:14-cv-12688 (E.D. Mich. May 3, 2016), http://law.justia.com/cases/federal/district-courts/michigan/miedce/2:2014cv12688/292915/44/	Plaintiffs alleged Rodale violated Michigan's Video Rental Privacy Act by disclosing its customers' magazine subscription information and subscription histories to third-party marketing companies without first obtaining the consent of the consumers.	$4,500,000	Anthony Salamone, *Rodale Settles Michigan Lawsuit over Subscriber Privacy for $4.5 Million*, MORNING CALL (June 17, 2016), http://cqrcengage.com/uwmich/app/document/14384322.
Holland v. Yahoo Inc., No. 5:13-cv-04980 (N.D. Cal. Aug. 25, 2016)	Plaintiffs were a class of non-Yahoo users who alleged that Yahoo scanned users' emails before the users had even seen them in an effort to tailor marketing efforts. They claimed this violated CalCIPA.	$4,000,000	Brandon Lowrey, *Yahoo Email Privacy Deal OK'd With $4M In Attys' Fees*, LAW360 (Aug. 26, 2016), http://www.law360.com/articles/833112/yahoo-email-privacy-deal-ok-d-with-4m-in-attys-fees.
In re Quantcast Advertising Cookie Litigation, No. 2:10-cv-05484 (C.D. Cal. Dec. 3, 2010)	Plaintiffs alleged Quantcast and the other websites set up flash cookies on the users' computers to use as local storage within the flash media player to back up browser cookies for purposes of restoring them later. Their claims included violations of the Computer Fraud and Abuse Act, ECPA, the VPPA, and various California state laws.	$2,400,000	Zach Winnick, *ABC, Others Settle Action Over Web Privacy Breaches*, LAW360 (June 13, 2011), http://www.law360.com/articles/251066/abc-others-settle-action-over-web-privacy-breaches.

Case	**Claims**	**Settlement Amount**	**Case Citation**
Curry v. AvMed, Inc., No. 1:10-cv-24513-JLK (S.D. Fla. September 3, 2013)	Plaintiffs brought a breach of contract and privacy class action against a healthcare insurer that had laptops with unencrypted customer information stolen.	$3,000,000	Allison Grande, *AvMed, Customers Reach Settlement In Data Theft Suit*, LAW360 (Sept. 6, 2013, 7:53 PM), http://www.law360.com/articles/470677/avmed-customers-reach-settlement-in-data-theft-suit.
Petersen v. Lowes HIW, Inc., 3:11-cv-01996-RS (N.D. Cal. Aug. 24, 2012)	Plaintiffs alleged that Lowes improperly recorded zip codes and other personal information in order to obtain home addresses for marketing purposes. Plaintiffs claimed this practice violated a California law that prevents a merchant from requesting personal identification information as a condition to accepting credit card payments.	$2,900,000	Brian Mahone, *Lowe's To Pay $3M To Settle ZIP Code Collection Suits*, LAW360 (Apr. 27, 2012, 4:39 PM), http://www.law360.com/articles/334871/lowe-s-to-pay-3m-to-settle-zip-code-collection-suits.
Minnesota v. Accretive Health, Inc., 0:12-cv-00145 (D. Minn. July 30, 2012)	State of Minnesota alleged that a debt collector for two hospital systems violated state privacy laws when a laptop containing patient data was stolen.	$2,490,400	Tony Kennedy & Maura Lerner, *Accretive is Banned from Minnesota*, STAR TRIBUNE, July 21, 2012, http://www.startribune.com/accretive-banned-from-minnesota-for-at-least-2-years-to-pay-2-5m/164313776/.

Case	**Claims**	**Settlement Amount**	**Case Citation**
Fort Hall Landowners Alliance, Inc. v. Department of Interior, No. 4:99-cv-00052-BLW (D. Idaho Dec. 24, 2007)	Group of Native Americans brought suit against the Bureau of Indian Affairs. They claimed the Bureau violated the Privacy Act by disclosing personal information connected to renewals of leases of allotment land.	$2,350,000	Stipulation for Approval of Class Settlement, *Fort Hall Landowners Alliance, Inc. v. Department of Interior*, No. 4:99-cv-00052-BLW, ECF No. 418 (D. Idaho Sept. 19, 2007).
Stone v. Howard Johnson International, Inc., 2:12-cv-01684 (C.D. Cal. Aug. 26, 2015)	Plaintiffs alleged that Howard Johnson and Wyndham hotels were surreptitiously recording customers' phone calls. Plaintiffs claimed violations of California's Privacy Act.	$1,500,000	Linda Chiem, *HoJo, Wyndham Settle Phone Privacy Class Action For $1.5M*, LAW360 (Apr. 27, 2015), http://www.law360.com/articles/648047/hojo-wyndham-settle-phone-privacy-class-action-for-1-5m.
Brown v. Defender Security Company, 2:12-cv-07319 (C.D. Cal. Sept. 12, 2013)	Plaintiffs alleged that a home security company surreptitiously recorded customers' phone calls. Plaintiffs claimed violations of California's Privacy Act.	$1,400,000	Gavin Broady, *Calif. Security Co. Pays $1.4M To Settle Recorded Call Suit*, LAW360 (Sept. 16, 2013, 1:07 PM), http://www.law360.com/articles/472856/calif-security-co-pays-1-4m-to-settle-recorded-call-suit.
In the Matter of Cellco Partnership, d/b/a Verizon Wireless, FCC Rcd DA 16-242 (Mar. 7,	The FCC investigated Verizon to determine whether its "supercookies" that tracked Internet activity broke privacy and data security laws. Verizon settled in order to end the investigation.	$1,300,000	Press Release, FCC, FCC Settles Verizon "Supercookie" Probe, Requires Consumer Opt-In for Third Parties (Mar. 7, 2016), https://apps.fcc.gov/edocs_publi

Case	Claims	Settlement Amount	Case Citation
2016), https://apps.fcc.gov/edocs_public/attachmatch/DA-16-242A1.pdf			c/attachmatch/DOC-338091A1.pdf.
Saunders v. StubHub, Inc., CGC-12-517707 (Cal. App. Dep't Super. Ct. Apr. 9, 2015)	Plaintiffs alleged that StubHub's customer service line recorded customer's calls without notice or consent. They claimed violations of the California Invasion of Privacy Act.	$1,250,000	Beth Winegarner, *StubHub Gets Nod For Deal After Prior Version Didn't 'Add Up'*, LAW360 (July 14, 2015), http://www.law360.com/articles/679170/stubhub-gets-nod-for-deal-after-prior-version-didn-t-add-up.
United States v. Xanga.com, Inc., No. 06 CV 6853 (S.D.N.Y. Sep. 12, 2006), https://www.ftc.gov/sites/default/files/documents/cases/2006/09/xangaconsentdecree_image.pdf	The FTC alleged that a blog hosting website knowingly collected and distributed personal information of children under 13 in violation of COPPA.	$1,000,000	Press Release, FCC, Xanga.com to Pay $1 Million for Violating Children's Online Privacy Protection Rule (Sept. 7, 2006), https://www.ftc.gov/news-events/press-releases/2006/09/xangacom-pay-1-million-violating-childrens-online-privacy.

Case	**Claims**	**Settlement Amount**	**Case Citation**
United States v. Sony BMG Music Entertainment, No. 08 Civ. 10730 (S.D.N.Y. Dec. 15, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/12/081211consentp0823071.pdf	The FTC alleged that Sony allowed tens of thousands of children under age 13 to register on its websites and create personal fan pages where they could interact with other Sony Music fans, including adults, despite knowing the age of the children via the personal information they submitted. The FTC claimed this violated COPPA.	$1,000,000	Press Release, FCC, Sony BMG Music Settles Charges Its Music Fan Websites Violated the Children's Online Privacy Protection Act (Dec. 11, 2008), https://www.ftc.gov/news-events/press-releases/2008/12/sony-bmg-music-settles-charges-its-music-fan-websites-violated.