THE FTC AND THE NEW COMMON LAW OF PRIVACY

Daniel J. Solove & Woodrow Hartzog***

One of the great ironies about information privacy law is that the primary regulation of privacy in the United States has barely been studied in a scholarly way. Since the late 1990s, the Federal Trade Commission (FTC) has been enforcing companies' privacy policies through its authority to police unfair and deceptive trade practices. Despite over fifteen years of FTC enforcement, there is no meaningful body of judicial decisions to show for it. The cases have nearly all resulted in settlement agreements. Nevertheless, companies look to these agreements to guide their privacy practices. Thus, in practice, FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or any common law tort.

In this Article, we contend that the FTC's privacy jurisprudence is functionally equivalent to a body of common law, and we examine it as such. We explore how and why the FTC, and not contract law, came to dominate the enforcement of privacy policies. A common view of the FTC's privacy jurisprudence is that it is thin, merely focusing on enforcing privacy promises. In contrast, a deeper look at the principles that emerge from FTC privacy "common law" demonstrates that the FTC's privacy jurisprudence is quite thick. The FTC has codified certain norms and best practices and has developed some baseline privacy protections. Standards have become so specific they resemble rules. We contend that the foundations exist to develop this "common law" into a robust privacy regulatory regime, one that focuses on consumer expectations of privacy, extends far beyond privacy policies, and involves a full suite of substantive rules that exist independently from a company's privacy representations.

---

* John Marshall Harlan Research Professor of Law, George Washington University Law School.

** Assistant Professor, Samford University's Cumberland School of Law. The authors would like to thank Derek Bambauer, Julie Brill, Danielle Citron, Brannon Denning, Bob Gellman, Chris Hoofnagle, Toby Levin, Paul Ohm, Gerry Stegmaier, David Vladeck, Joel Winston, Chris Wolf, the participants of the Fifth Annual Privacy Law Scholars Conference and the International Association of Privacy Professionals Privacy Academy, the members of the Federal Trade Commission, and the faculty at the Michigan State University College of Law and the Notre Dame Law School. The authors would also like to thank Andrew Hasty, Dennis Holmes, and Blake Hungerford for their excellent research assistance and the George Washington University Law School Scholarship Grant Program and Samford University's Cumberland School of Law for their financial support.

INTRODUCTION

One of the great ironies about information privacy law is that the primary regulation of privacy in the United States has barely been studied in a scholarly way. Since the late 1990s, the Federal Trade Commission (FTC or "Commission") has been enforcing companies' privacy policies through its authority to police unfair and deceptive trade practices.[1] The FTC has also been enforcing several privacy statutes and the Safe Harbor Agreement that enables companies to transfer data between the United States and the European Union.[2]

Despite over fifteen years of FTC enforcement, there are hardly any judicial decisions to show for it. The cases have nearly all resulted in settlement agreements. Nevertheless, companies look to these agreements to guide their decisions regarding privacy practices. Those involved with helping businesses comply with privacy law—from chief privacy officers to inside counsel to outside counsel—parse and analyze the FTC's settlement agreements, reports, and activities as if they were pronouncements by the Chairman of the Federal Reserve. Thus, in practice, FTC privacy jurisprudence has become the broadest and most influential reg-

1. See, e.g., Marcia Hofmann, Federal Trade Commission Enforcement of Privacy, *in* Proskauer on Privacy § 4:1.2 (Kristen J. Mathews ed., 2012) (discussing FTC's authority to ensure individuals and businesses do not engage in unfair or deceptive acts); Andrew Serwin, The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices, 48 San Diego L. Rev. 809, 811 (2011) (tracing development of FTC's role in consumer protection enforcement).

2. A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, FTC (July 2008) [hereinafter Overview of FTC Authority], http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (on file with the *Columbia Law Review*) (explaining "Commission enforces a variety of specific consumer protection statutes . . . prohibit[ing] specifically-defined trade practices and generally specify[ing] that violations . . . be treated as if they were 'unfair or deceptive' acts or practices under Section 5(a)," including Truth-in-Lending Act, Fair Credit Reporting Act, and Children's Online Privacy Protection Act).

ulating force on information privacy in the United States—more so than nearly any privacy statute or common law tort. It is therefore quite surprising that so little scholarly attention has been devoted to the FTC's privacy jurisprudence.

In this Article, we endeavor to map this uncharted terrain. We explore how and why the FTC, and not contract law, came to dominate the enforcement of privacy policies. We seek to understand why the FTC jurisprudence developed the way that it did and how it might develop in the future. We contend that the FTC's privacy jurisprudence is functionally equivalent to a body of common law, and we examine it as such.

One reason for the scant focus on the FTC might be because of the perception that the FTC's privacy jurisprudence is rather thin, merely focusing on enforcing privacy promises. In contrast, a deeper look at the principles that emerge from FTC privacy "common law" demonstrates that the FTC's privacy jurisprudence is quite thick. The FTC has codified certain norms and best practices and has developed some baseline privacy protections. Standards have become so specific they resemble rules. The FTC has thus developed a surprisingly rich jurisprudence. We contend that the foundations exist to develop this "common law" into a robust privacy regulatory regime, one that focuses on consumer expectations of privacy, extends far beyond privacy policies, and involves a full suite of substantive rules that exist independently from a company's privacy representations.

Comparisons between privacy regulation in the United States and European Union have often pointed out E.U. law's comprehensiveness in contrast with U.S. law's fragmentation and hollow standards, which provide few limits on the collection, use, and disclosure of personal data.[3] But such comparisons are increasingly becoming outdated as FTC privacy jurisprudence develops and thickens.

---

3. See, e.g., Robert Gellman, A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board, 54 Hastings L.J. 1183, 1205 (2003) ("The FTC's endorsement of a diluted version of [Federal Information Processing Standards] is one reason that the Commission is not a good candidate to serve a larger role in privacy policy. The Commission's privacy vision is too limited . . . [and] does not have jurisdiction over many private sector, non-profit, and governmental record keepers."); Allyson W. Haynes, Online Privacy Policies: Contracting Away Control over Personal Information?, 111 Penn St. L. Rev. 587, 606 (2007) (asserting focus of FTC and state enforcement is on "website's adherence to its promises, not a general standard of fairness"); Ryan Moshell, . . . And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection, 37 Tex. Tech L. Rev. 357, 383 (2005) (discussing "FTC's inadequacy and toothlessness in ensuring privacy protection"); James P. Nehf, Recognizing the Societal Value in Information Privacy, 78 Wash. L. Rev. 1, 58 (2003) (discussing "holes in this patchwork of sector-specific privacy laws"); Joel R. Reidenberg, Privacy Wrongs in Search of Remedies, 54 Hastings L.J. 877, 887–88 (2003) (asserting U.S. information privacy "is protected only through an amalgam of narrowly targeted rules . . . [that] leave[] many significant gaps and fewer clear remedies"); Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25

It is fair to say that today FTC privacy jurisprudence is the broadest and most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or common law tort. The statutory law regulating privacy is diffuse and discordant, and common law torts fail to regulate the majority of activities concerning privacy.[4]

Privacy law in the United States has developed in a fragmented fashion and is currently a hodgepodge of various constitutional protections, federal and state statutes, torts, regulatory rules, and treaties. Unlike the privacy laws of many industrialized nations, which protect all personal data in an omnibus fashion, privacy law in the United States is sectoral, with different laws regulating different industries and economic sectors. There is a law for video records and a different law for cable records.[5] The Health Insurance Portability and Accountability Act (HIPAA) protects the privacy of health data,[6] but a different regime governs the privacy of financial data. In fact, there are several laws that regulate financial data depending upon the industry, and health data is not even uniformly protected: Not all health data is covered by HIPAA, and various constitutional and state laws can protect health data more stringently than HIPAA.[7] Although state data security breach notification laws apply broadly across different industries, most state privacy laws are sectoral as well. By and large, it is fair to say that U.S. privacy law regulates only specific types of data when collected and used by specific types of entities.

The sectoral approach also leaves large areas unregulated, especially at the federal level. For example, there is no federal law that directly protects the privacy of data collected and used by merchants such as Macy's and Amazon.com. Nor is there a federal law focused on many of the forms of data collection in use by companies such as Facebook and Google. Most state laws are ineffective at addressing these problems, as are the four privacy torts.[8]

Yale J. Int'l L. 1, 61–62 (2000) (comparing "European scheme of empowering national supervisory authorities" to alleged "decentralized U.S. approach").

4. See, e.g., Daniel J. Solove, Understanding Privacy 8 (2008); Neil M. Richards, The Limits of Tort Privacy, 9 J. on Telecomm. & High Tech. L. 357, 365–74 (2011) ("[A]s a basis for protecting privacy, tort privacy is a very limited remedy.").

5. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified as amended at 18 U.S.C. §§ 2710–2711 (2012)); Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (codified as amended in scattered sections of 47 U.S.C.).

6. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered titles of U.S.C.).

7. See, e.g., Joy L. Pritts, Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule, 2 Yale J. Health Pol'y L. & Ethics 327, 330–48 (2002) (comparing state and federal statutes governing health privacy).

8. See Restatement (Second) of Torts § 652B (1977) (addressing intrusion upon seclusion tort); id. § 652C (addressing appropriation tort); id. § 652D (addressing public disclosure of private facts tort); id. § 652E (addressing false light tort).

Although these enormous areas are for the most part unregulated by any industry-specific statute, they are nevertheless regulated. A substantial number of companies today, and nearly every large company, have privacy policies, and privacy policies are enforced by the FTC. The FTC can bring an action against a company for breaching a promise in its privacy policy—and, even more broadly, for any deceptive or unfair act or practice. This fact has effectively given the FTC a sprawling jurisdiction to enforce privacy in addition to the pockets of statutory jurisdiction Congress has given to it in industry-specific privacy legislation. The FTC reigns over more territory than any other agency that deals with privacy.

Because so many companies fall outside of specific sectoral privacy laws, the FTC is in many cases the primary source of regulation. FTC regulation is thus the largest and arguably the most important component of the U.S. privacy regulatory system.

Despite this fact, there is surprisingly little scholarship about the FTC's privacy regulation.[9] The dearth of scholarship about the FTC stands in stark contrast to the enormous amount of scholarship about information privacy law. Why is the quantity of scholarship so disproportionate to the influence and importance of the FTC?

The most likely reason is that FTC actions have nearly all ended in settlements rather than case law. This, too, is a curiosity in privacy law. Perhaps the single most important and widely applying body of precedent that regulates privacy in the United States is not in the form of any traditional kind of privacy law, such as cases or statutes.

Another curiosity is privacy exceptionalism—privacy policies began as stand-alone documents and are only just recently beginning to be incorporated into a website's terms of use.[10] Why is privacy separate from the rest of the terms? This curiosity becomes even odder when coupled with an additional curiosity—the fact that contract law has barely played a role in governing civil disputes regarding privacy policy violations.

---

9. For notable exceptions, see, e.g., Steven Hetcher, The FTC as Internet Privacy Norm Entrepreneur, 53 Vand. L. Rev. 2041 (2000) [hereinafter Hetcher, Privacy Norm]; James P. Nehf, The FTC's Proposed Framework for Privacy Protection Online: A Move Toward Substantive Controls or Just More Notice and Choice?, 37 Wm. Mitchell L. Rev. 1727 (2011); Ira S. Rubinstein, Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes, 6 I/S: J.L. & Pol'y for Info. Soc'y 355 (2011); Serwin, supra note 1; Jeff Sovern, Protecting Privacy with Deceptive Trade Practices Legislation, 69 Fordham L. Rev. 1305 (2001); Gerard M. Stegmaier & Wendell Bartnick, Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements, 20 Geo. Mason L. Rev. 673 (2013) [hereinafter Stegmaier & Bartnick, Psychics].

10. See, e.g., 2 Ian C. Ballon, E-Commerce and Internet Law 26.14[2] (2d ed. 2013) ("A privacy policy . . . need not be set up like a contract. . . . [S]ince privacy policies typically are enforced *against* a site owner . . . many sites . . . treat Privacy Statements as notices to consumers making clear . . . that it is not a contract. Others incorporate privacy policies by reference in Terms of Service . . . .").

Although privacy policies look like contracts,[11] there are barely a handful of cases attempting to enforce privacy policies as contracts.[12] In contrast, terms of use are clearly the province of contract law. Of course, both the FTC and contract law can regulate simultaneously, but why has privacy become so exclusively the province of the FTC? Moreover, the doctrines developed by the FTC are sometimes parallel with contract law, but not always. This body of doctrines is thus somewhat unique—a body of "law" unto itself. It is a new species that has yet to be classified in the legal taxonomy.

The result of all these oddities is that a large domain of the U.S. privacy regulatory framework primarily consists of a relatively obscure body of doctrines that scholars have not analyzed in depth. Thus, it is often hard to characterize precisely what this large domain of regulation is, to understand precisely what it says when viewed altogether, and to predict where it is heading.

In this Article, we aim to shed light on these issues. Our primary thesis is that through a common law-like process, the FTC's actions have developed into a rich jurisprudence that is effectively the law of the land for businesses that deal in personal information. This jurisprudence has the foundations to grow even more robust. By clarifying its standards and looking beyond a company's privacy promises, the FTC is poised to enforce a holistic and robust privacy regulatory regime that draws upon industry standards and consumer expectations of privacy to remain potent, feasible, and adaptable in the face of technological change.

Our argument has four parts. In Part I we discuss how the FTC rose to its current dominant position in the domain of privacy. In the late 1990s, it was far from clear that the body of law regulating privacy policies would come from the FTC and not from traditional contract and promissory estoppel. We explore how and why the current state of affairs developed.

As a response to claims that the FTC acts arbitrarily and provides little guidance for companies, in Part II we demonstrate how the FTC's settlement agreements are the functional equivalent of privacy common law. Understanding the FTC's privacy jurisprudence as such helps describe the evolutionary nature of this body of law and provides a dif-

---

11. See, e.g., Scott Killingsworth, Minding Your Own Business: Privacy Policies in Principle and in Practice, 7 J. Intell. Prop. L. 57, 91–92 (1999) (explaining ways in which website privacy policies resemble contracts).

12. See, e.g., In re JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 316–18 (E.D.N.Y. 2005) (discussing plaintiff's claim that JetBlue's privacy policy constitutes self-imposed contractual obligation between airline and consumers); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1999–2000 (D.N.D. 2004) (reasoning "broad statements of company policy do not generally give rise to contract claims" and thus dismissing contract claim); In re Nw. Airlines Privacy Litig., No. Civ.04-126(PAM/JSM), 2004 WL 1278459, at *5–*6 (D. Minn. June 6, 2004) (rejecting claim that Northwest Airlines's online privacy statement constitutes unilateral contract).

ferent perspective with which to analyze the perceived lack of guidance from the Commission. We explore the benefits and drawbacks of the fact that so much privacy jurisprudence has developed through FTC settlements rather than through judicial decisions.

Part III examines the principles emerging from this FTC privacy "common law." The principles extend far beyond merely honoring promises. The FTC's jurisprudence reveals four major patterns of development: (1) increasingly specific standards that are becoming more rule-like in nature; (2) the emergence of qualitative standards that essentially codify certain norms and best practices regarding privacy; (3) the development of certain baseline protections or sticky default rules; and (4) a recognition of contributory liability. We contend that these developmental patterns are not unusual or radical; they are classic patterns of common law evolution.

Part IV contends that the foundations exist to develop this "common law" into a robust privacy regulatory regime, one that (1) focuses less on broken promises and more on broken consumer expectations of privacy; (2) extends far beyond privacy policies to a much wider array of statements and practices; and (3) involves a full suite of substantive rules that exist independently from a company's privacy representations.

I. THE FTC'S RISE AS PRIVACY REGULATOR

Today, scholars and practitioners almost take for granted that a privacy policy is a separate document, not a contract or even a set of privately enforceable promises, and that the FTC is the primary enforcer. These things were not always readily apparent. This Part traces how the largest body of privacy regulation developed and why it took the form and structure that it currently has.

A. *The Rise of Privacy Policies*

As the Internet began to blossom in the mid-to-late 1990s and people began to surf the Web and engage in online commercial activity, privacy became an obvious concern because a significant amount of personal data could be gathered. Data security was another major concern, as many people were reluctant to use the Internet out of fear that their data could be improperly accessed.

Few laws directly regulated privacy in many of these contexts. Attempts to use the privacy torts to address problems with data collection and use ended in failure. Indeed, tort law was a poor fit for these sets of problems. For example, the tort of appropriation was rejected by courts as a way to protect against the sale of personal information. The tort occurs when one "appropriates to his own use or benefit the name or likeness of another."[13] In *Dwyer v. American Express Co.*, a court concluded

13. Restatement (Second) of Torts § 652C.

that American Express did not violate the appropriation tort when it sold its cardholders' names to merchants because "defendants' practices do not deprive any of the cardholders of any value their individual names may possess."[14] In *Shibley v. Time, Inc.*, a court rejected an appropriation action against a magazine that sold its subscription lists to direct mail companies.[15]

Other privacy torts were also of little applicability. The tort of public disclosure of private facts, for example, creates a cause of action when one makes public through widespread disclosure "a matter concerning the private life of another" in a way that "(a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[16] Because many uses of data by companies do not involve widespread disclosure and do not involve data that would be highly offensive if disclosed, the tort proved to be of little use. As a result, few cases involving the privacy torts were brought in situations involving problems with the collection and use of personal data.

An attempt was made early on to apply existing statutory law to online data gathering practices. In *In re DoubleClick, Inc. Privacy Litigation*, a group of plaintiffs attempted to challenge the use of cookies by DoubleClick, an online advertising company.[17] DoubleClick used cookies to gather web surfing data about users to create profiles of them to assist websites in delivering targeted banner advertisements. The plaintiffs argued that the DoubleClick cookies violated the Electronic Communication Privacy Act (ECPA) because they intercepted their online communications.[18] The court dismissed the case on the grounds that "DoubleClick-affiliated Web sites consented to DoubleClick's access of plaintiffs' communications to them."[19] The ECPA was indeed a poor fit, as it was designed to regulate wiretapping and electronic snooping rather than commercial data gathering. The records maintained by internet retailers and websites were often held not to be "communications" under the ECPA.

These rare attempts to apply existing law nearly all failed because so few laws regulated the privacy and security of data online. Some early commentators hailed the regulatory void for online activity as essential breathing space to allow the Internet to flourish. For example, John Perry Barlow's famous *A Declaration of the Independence of Cyberspace* began:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You

14. 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995).
15. 341 N.E.2d 337, 339 (Ohio Ct. App. 1975).
16. Restatement (Second) of Torts § 652D.
17. 154 F. Supp. 2d 497 (S.D.N.Y. 2001).
18. Id. at 507.
19. Id. at 511.

> are not welcome among us. You have no sovereignty where we gather.[20]

Industry favored a self-regulatory regime, which consisted largely of what has become known as "notice and choice." For the "notice" part, companies began to include privacy policies on their websites, especially commercial ones.[21] The privacy policy was typically a special page that users could read by clicking a link at the bottom of a website's homepage.[22] These policies described the various ways in which websites collected, used, and shared a visitor's personal information, as well as the various ways that information was protected. For the "choice" part, users were given some kind of choice about how their data would be collected and used, most commonly in the form of an opt-out right, whereby companies could use data in the ways they described in the privacy policy unless users affirmatively indicated they did not consent to these uses.

The use of privacy policies and some dimension of choice emerged from the Fair Information Practice Principles (FIPPs), sometimes known as just the Fair Information Practices (FIPs).[23] The FIPPs were first stated in a 1973 report by the U.S. Department of Health, Education, and Welfare (HEW), and they became extremely influential in shaping privacy law in the United States and around the world.[24] For example, the FIPPs were restated and expanded in the OECD Guidelines of 1980 as well as the APEC Privacy Framework of 2004.[25]

One of the most prominent FIPPs is the individual's right to have notice about the data gathered about herself and the right to know how

---

20. John Perry Barlow, A Declaration of the Independence of Cyberspace, Elec. Frontier Found. (Feb. 8, 1996), https://projects.eff.org/~barlow/Declaration-Final.html (on file with the *Columbia Law Review*).

21. See, e.g., Michael D. Scott, The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60 Admin. L. Rev. 127, 130–31 (2008) ("The main element of self-regulation included FTC enforcement of those privacy policies that companies collecting personal information posted on their websites.").

22. See, e.g., Haynes, supra note 3, at 594 ("Typical privacy policies are accessed via hyperlinks at the bottom of the screen on a website's home page.").

23. See, e.g., Robert Gellman, Fair Information Practices: A Basic History 1–2, 12 (Nov. 11, 2013) (unpublished manuscript), available at http://bobgellman.com/rg-docs/rg-FIPPShistory.pdf (on file with the *Columbia Law Review*) (recounting origin of FIPs).

24. U.S. Dep't of Health, Educ., & Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems 41–42 (1973).

25. Ministerial Council of the Org. for Econ. Cooperation & Dev., Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Doc. C(80)58/FINAL (Sept. 23, 1980), available at http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=114&InstrumentPID=312 (on file with the *Columbia Law Review*), amended by O.E.C.D. Doc. C(2013)79 (July 11, 2013); Asia-Pacific Econ. Cooperation, APEC Privacy Framework 5–19 (2004), available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (on file with the *Columbia Law Review*).

it will be used. Another of the most prominent FIPPs is the individual's right to consent to the collection and use of her personal data.[26] These two FIPPs became the backbone of the U.S. self-regulatory approach, with privacy policies seeking to satisfy the right to notice, and with user choice seeking to satisfy the right to consent.

In the late 1990s, organizations such as TRUSTe began to issue privacy "seals" that certified that a partnered website would conform to certain basic privacy norms, such as having a privacy policy. These seals became valuable for websites to promote consumer trust, and they drove more websites to create privacy policies.[27]

For example, in 1999, America Online (AOL)'s privacy policy stated: "In general, our service automatically gathers certain usage information like the numbers and frequency of visitors to AOL.COM and its areas, very much like television ratings that tell the networks how many people tuned in to a program. We only use such data in the aggregate."[28] The policy went on to assure visitors that AOL "do[es] not use or disclose information about your individual visits to AOL.COM or information that you may give us, such as your name, address, email address or telephone number, to any outside companies."[29] This very early privacy policy included a certification seal from TRUSTe, which certified that the partnered website would notify its users about "[w]hat information is gathered/tracked; [h]ow the information is used; [and] [w]ho information is shared with."[30]

Privacy policies were largely a voluntary measure by companies on the Internet to promote their privacy practices and partially an attempt

---

26. See, e.g., Gellman, supra note 23, at 6–7 (enumerating OECD principles on data protection, including collection limitation and individual participation principles).

27. The FTC even mentioned the presence of these seals in its complaints. E.g., First Amended Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Toysmart.com, LLC, No. 00-11341-RGS (D. Mass. July 21, 2000) [hereinafter Toysmart.com Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/toysmartcomplaint.htm (on file with the *Columbia Law Review*) (noting defendant "became a licensee of . . . an organization that certifies the privacy policies of online businesses and allows such businesses to display a . . . trustmark or seal").

28. Privacy Policy, AOL.com (1999) [hereinafter Archived AOL Privacy Policy], http://web.archive.org/web/19990503010144/http://www.aol.com/info/privacy.html (on file with the *Columbia Law Review*) (accessed through Internet Archive). The first privacy policy to be indexed for the auction website eBay was indexed in January 1999, but has a copyright date of 1995–1998 and was expressly incorporated into the terms of use. eBay Privacy Policy, eBay Inc. (1999), http://web.archive.org/web/19990117033125/http://pages.ebay.com/aw/privacy-policy.html (on file with the *Columbia Law Review*) (accessed through Internet Archive).

29. Archived AOL Privacy Policy, supra note 28.

30. Id. The current AOL.com privacy policy is similar in format to this original version, including its status as a stand-alone document accessible via a link on the homepage. AOL Privacy Policy, AOL.com, http://privacy.aol.com/privacy-policy (last updated June 28, 2013) (on file with the *Columbia Law Review*).

at self-regulation in order to stave off further regulation.[31] The goal was in part to convince policymakers that self-regulation could work and that no additional regulation was needed.

To a significant extent, the approach was successful. Congress crafted a few industry-specific privacy statues, but left a large array of data collection and use unregulated. The Clinton Administration created the Information Infrastructure Task Force to explore the issue, which issued documents in 1995 and 1997 that largely recommended a self-regulatory approach.[32]

Even when statutes were passed, they often embraced the notice-and-choice approach. Privacy laws began to require privacy policies.[33] For example, the Gramm-Leach-Bliley Act of 1999 required financial institutions to provide privacy policies to their customers.[34] Privacy policies began to transcend mere online contexts and soon became the norm for all companies that collected and used data, whether online or offline.

According to Professor Allyson Haynes, "In 1998, only 2% of all websites had some form of privacy notices, and in 1999, eighteen of the top 100 shopping sites did not display a privacy policy. By 2001, virtually all of the most popular commercial websites had privacy notices . . . ."[35] Indeed, today, whether for online or offline activities, most established companies in nearly all industries have a privacy policy.

---

31. See, e.g., Haynes, supra note 3, at 593 ("Online privacy policies have appeared . . . as a voluntary measure by websites . . . ."); Hetcher, Privacy Norm, supra note 9, at 2046–47 (recounting that threat by FTC of recommending further privacy legislation resulted in significant jump in number of sites offering privacy policies); Scott, supra note 21, at 130–31 (explaining rationale behind early emphasis on self-regulation).

32. Info. Policy Comm., Info. Infrastructure Task Force, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information (1995), available at http://aspe.hhs.gov/datacncl/niiprivp.htm (on file with the *Columbia Law Review*); Info. Policy Comm., Nat'l Info. Infrastructure Task Force, Options for Promoting Privacy on the National Information Infrastructure, Draft for Public Comment (1997), available at http://aspe.hhs.gov/datacncl/privacy/promotingprivacy.shtml (on file with the *Columbia Law Review*).

33. See, e.g., Cal. Bus. & Prof. Code § 22575 (West 2008) ("An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site . . . ."); Killingsworth, supra note 11, at 71–81 (describing statutes and legal principles dealing with website privacy).

34. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. § 6803 (2012)).

35. Haynes, supra note 3, at 593–94 (footnotes omitted); see also FTC, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress 10 (2000) [hereinafter FTC, Fair Information Practices], available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (on file with the *Columbia Law Review*) ("This year, the Commission's Survey findings demonstrate continued improvement on this front, with 88% of Web sites in the Random Sample posting at least one privacy disclosure. Of sites in the Random Sample that collect personal identifying information, 90% post at least one privacy disclosure." (footnote omitted)).

Because of the way that they developed, privacy policies typically existed as a separate document or special webpage devoted exclusively to privacy. Websites often had—and continue to have—a terms-of-use page with contractual language addressing a wide variety of other issues. Likewise, privacy policies provided in offline contexts were—and remain—separate documents from other disclosures and contractual terms.

B. *Privacy Policies as Contract?*

As privacy policies emerged, the existence and nature of any binding legal force behind them remained unclear. Initially, it appeared that contract law would play a large role. In one of the rare articles to examine whether privacy policies were enforceable as contracts, Scott Killingsworth argued in 1999 in the affirmative, observing, "As between the website and the user, a privacy policy bears all of the earmarks of a contract, but perhaps one enforceable only at the option of the user."[36] In addition, Killingsworth asserted the following:

> It is no stretch to regard the policy as an offer to treat information in specified ways, inviting the user's acceptance, evidenced by using the site or submitting the information. The website's promise and the user's use of the site and submission of personal data are each sufficient consideration to support a contractual obligation.[37]

Killingsworth concluded that people could enforce privacy policies as contracts. At the time, however, despite great concern over the collection and use of personal data on the Internet, there were no published opinions using a contract theory to remedy a privacy policy violation.[38]

Eventually, in 2004 and 2005, a few litigants brought breach of contract claims for privacy policy violations. These cases arose out of airlines that shared passenger name records with the federal government after the September 11, 2001 terrorist attacks.[39] All failed, mainly because the

---

36. Killingsworth, supra note 11, at 91–92.

37. Id. (emphasis omitted) (citation omitted).

38. The first judicial opinion referencing an online privacy policy appears to be Raley v. Michael, 56 Va. Cir. 87, 88 (2001), which states: "The User Agreement is a legal document that spells out the relationship between you and eBay. It outlines the services, pricing, Privacy Policy, and the buyer and seller relationship for listing and bidding on items in eBay's auction format." However, the first judicial opinion to tackle privacy policies under a contract theory in earnest was *Crowley v. CyberSource Corp.*, which involved allegations of improper interception and storage of customers' information, including credit card numbers. 166 F. Supp. 2d 1263, 1267–68 (N.D. Cal. 2001) (finding since privacy policy was not incorporated by reference, it did not apply in relevant contractual dispute).

39. E.g., In re JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 324–27 (E.D.N.Y. 2005) (dismissing suit against airline for allegedly unlawful sharing of passengers' personal information); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1199–200 (D.N.D. 2004) (same); In re Nw. Airlines Privacy Litig., No. Civ.04-126(PAM/JSM), 2004 WL 1278459, at *5–*6 (D. Minn. June 6, 2004) (same).

plaintiffs were unable to establish damages.[40] In one case, the court even disputed whether a privacy policy should be deemed a contract. The court reasoned that "broad statements of company policy do not generally give rise to contract claims."[41] Moreover, the court noted that plaintiffs failed to allege that they read or relied upon the privacy policy.[42]

Promissory estoppel, the equitable doctrine that protects those who detrimentally rely upon promises, also seemed like it would serve as an effective tool for the enforcement of privacy policies; yet it has been used even less frequently than formal contract. According to the Restatement (Second) of Contracts:

> A promise which the promisor should reasonably expect to induce action or forbearance on the part of the promisee or a third person and which does induce such action or forbearance is binding if injustice can be avoided only by enforcement of the promise. The remedy granted for breach may be limited as justice requires.[43]

In the few cases promissory estoppel has been alleged in privacy-related disputes, it has not been successful, largely based on a lack of evidence of detrimental reliance.[44]

Today, contract law—formal contract and promissory estoppel—plays hardly any role in the protection of information privacy, at least vis-à-vis websites with privacy policies. Contract law litigation theories have barely been attempted, as the number of cases involving these theories has been exceedingly low over the past fifteen to twenty years after the rise of privacy policies.

---

40. E.g., *JetBlue*, 379 F. Supp. 2d at 326 ("[P]laintiffs failed to proffer any . . . form of damages that they would seek if given the opportunity to amend the complaint."); *Dyer*, 334 F. Supp. 2d at 1200 (holding plaintiffs failed to allege contractual damages arising out of alleged breach); *Nw. Airlines Privacy Litig.*, 2004 WL 1278459, at *6 (same).

41. *Dyer*, 334 F. Supp. 2d at 1200.

42. Id. Note that the FTC faces a similar difficulty in establishing that an unread deceptive representation is "material," meaning that it "is likely to affect the consumer's conduct or decision with regard to a product or service." Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce (Oct. 14, 1983) [hereinafter Letter from James C. Miller III to Hon. John D. Dingell] (on file with the *Columbia Law Review*), reprinted in In re Cliffdale Assocs., Inc., 103 F.T.C. 110 app. at 175–84 (1984) (decision & order).

43. Restatement (Second) of Contracts § 90(1) (1981).

44. E.g., Smith v. Trusted Universal Standards in Elec. Transactions, Inc., No. 09-4567 (RBK/KMW), 2011 WL 900096, at *10 n.10 (D.N.J. Mar. 15, 2011) ("[T]here is no evidence . . . that Plaintiff relied on a promise . . . . Therefore, no reasonable jury could conclude that a contract existed between the parties based upon a doctrine of promissory estoppel."); Complaint at 19, Strickland-Saffold v. Plain Dealer Publ'g Co., No. CV-10-723512 (Ohio Ct. Com. Pl. Jan. 7, 2011), available at http://www.courthousenews.com/2010/04/08/PlainDealer.pdf (on file with the *Columbia Law Review*) (asserting plaintiffs had justifiably relied on defendants maintaining website registration information based on promise in user agreement).

The few cases that have been brought against organizations for breach of contract for failing to follow their privacy policy have continued to fail.[45] Although a few courts have mentioned that a contract claim could be conceivable,[46] most such claims are dismissed because the privacy policies are not deemed contractual in nature[47] or because the plaintiffs failed to properly allege the harm required to recover for failure to honor privacy promises.[48]

Thus, contract law, which initially seemed to be the most appropriate tool to redress privacy policy violations, has played only a marginally significant role in these disputes. Instead, such violations have predominantly been redressed through the public enforcement of the FTC. Why did this state of affairs develop? How did the FTC reach its position of dominance? Why does the FTC continue to define these issues, with the vast and longstanding body of contract law remaining but a dusty relic in the attic? We will explore these questions in the Parts that follow.

---

45. E.g., Daniels v. JP Morgan Chase Bank, N.A., No. 22575/09, 2011 WL 4443599, at *7–*8 (N.Y. Sup. Ct. Sept. 22, 2001) (finding no breach of contract where bank released confidential documents in response to subpoena).

46. See, e.g., Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 864–65 (N.D. Cal. 2011) (declining to dismiss contractual claim based on damages arising from breach of privacy policy).

47. For a discussion of the relationship among privacy policies, contracts, and claims for invasion of privacy, see Loeffler v. Ritz-Carlton Hotel Co., No. 2:06-CV-0333-ECR-LRL, 2006 WL 1796008, at *2–*3 (D. Nev. June 28, 2006); see also Smith v. Trusted Universal Standards in Elec. Transactions, Inc., No. 09-4567(RBK/KMW), 2010 WL 1799456, at *8–*10 (D.N.J. May 4, 2010) ("Some courts have held that general statements like 'privacy policies' do not suffice to form a contract because they are not sufficiently definite.").

48. E.g., In re LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013) (finding "not receiving the full benefit of the bargain" for premium membership based on breach of privacy "cannot be the 'resulting damages' of this alleged breach [of contract]"); Rudgayzer v. Yahoo! Inc., No. 5:12-CV-01399 EJD, 2012 WL 5471149, at *6 (N.D. Cal. Nov. 9, 2012) (finding "[m]ere disclosure of such information in and of itself, without a showing of actual harm, is insufficient" to support a claim of breach of contract under California law); Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1028 (N.D. Cal. 2012) (rejecting embarrassment and property-based theories of harm as insufficient to state claim for breach of contract under California law); In re Facebook Privacy Litig., No. C 10-02389 JW, 2011 WL 6176208, at *5 (N.D. Cal. Nov. 22, 2011) (rejecting plaintiffs' theory that their personally identifiable information has value and that they suffered "appreciable and actual damage" in breach of contract suit); *Trusted Universal Standards*, 2010 WL 1799456, at *9–*10 ("[E]ven assuming that a contract did exist between Comcast and Plaintiff that incorporated the above terms, and even assuming that Comcast violated those terms, Plaintiff must still plead loss flowing from the breach to sustain a claim. He has not done so." (citations omitted)); Cherny v. Emigrant Bank, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) ("This Court finds that the release of an e-mail address, by itself, does not constitute an injury sufficient to state a claim under any of the legal theories Cherny asserts.").

C. *The Dawn of FTC Privacy Enforcement*

The FTC, which was created in 1914, was originally established to ensure fair competition in commerce.[49] The agency's powers were gradually expanded over a number of years. One of the most significant expansions occurred when Congress passed the Wheeler-Lea Amendment to the Federal Trade Commission Act (FTCA or "FTC Act") to expand the FTC's jurisdiction "to prohibit 'unfair or deceptive acts or practices' in addition to 'unfair methods of competition'—thereby charging the FTC with protecting consumers directly, as well as through its antitrust efforts."[50] Since the passing of section 5 of the FTC Act ("Section 5"), the FTC has pursued violations of various antitrust and consumer protection laws, including claims for false advertising and dangerous products.[51]

At the urging of Congress in 1995, the FTC became involved with consumer privacy issues.[52] The FTC initially encouraged self-regulation, which was justified by a fear that regulation would stifle the growth of online activity.[53] Instead of the FTC creating rules, the companies themselves would create their own rules, and the FTC would enforce them. The FTC thus would serve as the backstop to the self-regulatory regime, providing it with oversight and enforcement—essentially, with enough

---

49. About the Federal Trade Commission, FTC, http://www.ftc.gov/ftc/about.shtm (on file with the *Columbia Law Review*) (last modified Oct. 17, 2013).

50. J. Howard Beales III, Bureau of Consumer Prot., The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection, FTC (May 30, 2003) (quoting Act of Mar. 21, 1938, Pub. L. No. 75-447, 52 Stat. 111, 111 (codified as amended at 15 U.S.C. § 45(a)(1) (2012))), http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection (on file with the *Columbia Law Review*).

51. Cf. 15 U.S.C. § 45 (declaring unfair methods of competition unlawful and setting out means of prevention). See generally Overview of FTC Authority, supra note 2 (discussing investigative, enforcement, and litigation powers of FTC).

52. FTC, Fair Information Practices, supra note 35, at 3–5 ("Since 1995, the Commission has been at the forefront of the public debate on online privacy.").

53. See FTC, Self-Regulation and Privacy Online: A Report to Congress 12–14 (1999) (on file with the *Columbia Law Review*) ("[T]he Commission believes that legislation to address online privacy is not appropriate at this time."); Scott, supra note 21, at 130 (explaining FTC's rationale that "growth of the Internet in general, and electronic commerce in particular, mandated against sweeping regulations that might inhibit the growth of both"); Robert Pitofsky, Chairman, FTC, Prepared Statement of the Federal Trade Commission on "Consumer Privacy on the World Wide Web" (July 21, 1998), available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-consumer-privacy-world-wide-web/privac98.pdf (on file with the *Columbia Law Review*) ("[T]he Commission's goal has been . . . to encourage and facilitate self-regulation as the preferred approach to protecting consumer privacy online."); Robert Pitofsky, Chairman, FTC, Prepared Statement of the Federal Trade Commission on "Self-Regulation and Privacy Online" (July 13, 1999), available at http://www.ftc.gov/public-statements/1999/07/prepared-statement-federal-trade-commission-self-regulation-and-privacy (on file with the *Columbia Law Review)* (describing self-regulation as "least intrusive and most efficient means to ensure fair information practices online").

teeth to give it legitimacy and ensure that people would view privacy policies as meaningful and trustworthy.

The primary source of authority for FTC privacy enforcement was Section 5,[54] which prohibits "unfair or deceptive acts or practices in or affecting commerce."[55] An "unfair or deceptive" act or practice is a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment"[56] or a practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[57] Thus, in its enforcement under Section 5, the FTC had two bases for finding privacy violations—"deceptive" trade practices and "unfair" trade practices.

The FTC began its policing of privacy policies by focusing on deceptive trade practices,[58] though the FTC gradually began to file complaints against companies under an unfairness rationale. Although it could obtain injunctive remedies, the FTC was quite restricted in the severity of penalties it could exact.[59] Because the FTC could only enforce FTC Act violations or infringements of other laws that granted it regulatory authority and because the FTC lacked the ability to enact substantive privacy rules of its own, if a company not regulated by such a jurisdiction-granting statute lacked a privacy policy, then the FTC would have nothing to enforce. Thus, the FTC appeared to be limited to enforcing whatever a company promised, and most companies were under no obligation to make any promises to restrict their collection and use of personal data. It is especially notable, then, that the FTC has become as dominant as it is today.

---

54. E.g., Hofmann, supra note 1.

55. 15 U.S.C. § 45(a)(1).

56. Letter from James C. Miller III to Hon. John D. Dingell, supra note 42, app. at 174–76 (1984); see also Letter from FTC Comm'rs to Wendell H. Ford & John C. Danforth, Senators (Dec. 17, 1980), reprinted in In re Int'l Harvester Co., 104 F.T.C. 949 app. at 1070–76 (1984) [hereinafter FTC Policy Statement on Unfairness], available at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm (on file with the *Columbia Law Review*) (explaining evolution of, and rationale for, FTC's consumer unfairness jurisdiction).

57. 15 U.S.C. § 45(n).

58. Press Release, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case, FTC (Aug. 13, 1998), available at http://www.ftc.gov/news-events/press-releases/1998/08/internet-site-agrees-settle-ftc-charges-deceptively-collecting (on file with the *Columbia Law Review*) (announcing settlement of Agency's first internet privacy case, involving GeoCities' deceptive collection of personal information).

59. See generally Overview of FTC Authority, supra note 2 ("[T]he Commission must still seek the aid of a court to obtain civil penalties or consumer redress for violations of its orders to cease and desist or trade regulation rules.").

D. *The Ascendency of the FTC as the De Facto Data Protection Authority*

Today, the FTC is viewed as the de facto federal data protection authority.[60] A data protection authority is common in the privacy law of most other countries, which designate a particular agency to have the power to enforce privacy laws.[61] Critics of the FTC call it weak and ineffective—"[l]ow-[t]ech, [d]efensive, [and] [t]oothless" in the words of one critic.[62] But many privacy lawyers and companies view the FTC as a formidable enforcement power, and they closely scrutinize FTC actions in order to guide their decisions. This section will discuss why the FTC is viewed as a formidable privacy regulator.

Although steadily increasing each year, the number of FTC enforcement actions has not been particularly voluminous. The FTC has lodged just over 170 privacy-related complaints since 1997, averaging about ten complaints per year.[63] However, that number is slightly misleading given the steady increase in annual complaints. For example, the FTC brought nine privacy-related complaints in 2002, compared to 2012, in which it brought twenty-four complaints for unique privacy-related violations.[64]

The FTC's staff devoted to privacy issues is small. As shown in Table 1 below, the FTC's Bureau of Consumer Protection (BCP) is currently divided into seven divisions.[65]

---

60. See, e.g., Steven Hetcher, The De Facto Federal Privacy Commission, 19 J. Marshall J. Computer & Info. L. 109, 131 (2000) [hereinafter Hetcher, De Facto] ("[T]he FTC is fairly viewed as a nascent, *de facto* federal privacy commission."); James Taylor & Jill Westmoreland, Recent FTC Enforcement Actions Involving Endorsements, Privacy and Data Security, M/E Insights, Winter/Spring 2011, at 28, 29 ("The FTC continues to be the most active regulatory agency when it comes to privacy and data collection."); Richard Santalesa, FTC Issues Final Commission Report on Protecting Consumer Privacy, Info. Law Grp. (Mar. 26, 2012), http://www.infolawgroup.com/2012/03/articles/privacy-law/ftc-issues-final-commission-report-on-protecting-consumer-privacy/ (on file with the *Columbia Law Review*) ("The FTC has a front and center role in data privacy and enforcement.").

61. See, e.g., Daniel J. Solove & Paul M. Schwartz, Information Privacy Law 1127 (4th ed. 2011) (describing privacy commissioners in Canada, New Zealand, and Hong Kong).

62. Peter Maass, Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless, Wired (June 28, 2012, 6:30 AM), http://www.wired.com/threatlevel/2012/06/ftc-fail/all/ (on file with the *Columbia Law Review*).

63. Privacy and Security, FTC, http://business.ftc.gov/privacy-and-security (on file with the *Columbia Law Review)* (last visited Feb. 7, 2014) [hereinafter Bureau of Consumer Protection, Privacy and Security].

64. Legal Resources, FTC, http://business.ftc.gov/legal-resources/8/35 (on file with the *Columbia Law Review)* (last visited Feb. 7, 2014) [hereinafter FTC, Legal Resources] (providing links to recent FTC cases related to privacy and security).

65. The list of divisions comes from the FTC's Organization Directory. FTC, Organization Directory 2, available at http://www.inventions.org/wp-content/uploads/2012/10/FTC-orgdirectory.pdf (on file with the *Columbia Law Review*) (last visited Mar. 8, 2014). The Organization Directory displays an organization code for each organization listed in the directory. The FTC also makes available an Agency Staff Directory, which lists

TABLE 1: DIVISIONS OF THE BUREAU OF CONSUMER PROTECTION

Division Name	Abbreviation	# of Staff
Division of Privacy and Identity Protection	DPIP	46
Division of Financial Practices	DFP	48
Division of Advertising Practices	DAP	51
Division of Marketing Practices	DMP	44
Division of Enforcement	DENF	46
Division of Consumer and Business Education	DCBE	21
Division of Planning and Information	DPI	61

Five of these divisions (DPIP, DFP, DAP, DMP, and DENF) "focus on direct law enforcement and compliance," while the other two divisions (DCBE and DPI) "focus on support for BCP programs."[66] Additionally, there are about 180 FTC staff members located in seven regional offices, many of whom occasionally work on privacy matters.[67] Since 2010, there has also been a team of about five full-time employees dedicated to mobile privacy.[68]

DPIP was created in 2006 by former Chairman Majoras to "address[] cutting-edge consumer privacy matters through aggressive enforcement, as well as rulemaking, policy development, and outreach to consumers and businesses."[69] According to the FTC's current agency and organization directories, there are forty-five FTC staff personnel in DPIP. This represents an increase of about ten staff members since 2006, when DPIP

---

the names and organization codes of each FTC staff member. FTC, FTC Staff Directory (2013), available at http://www.ftc.gov/sites/default/files/attachments/contact-federal-trade-commission/whitepages.pdf (on file with the *Columbia Law Review*). Thus, counting the number of staffers associated with a particular organization code renders the number of FTC staff in a particular division.

66. William E. Kovacic, FTC, The Federal Trade Commission at 100: Into Our 2nd Century 29 (2009), available at http://www.ftc.gov/sites/default/files/documents/public_statements/federal-trade-commission-100-our-second-century/ftc100rpt.pdf (on file with the *Columbia Law Review*).

67. Id.

68. Email from David Vladeck, Dir., Bureau of Consumer Prot., to authors (Oct. 3, 2013, 1:12 PM) [hereinafter Vladeck Interview] (on file with the *Columbia Law Review*).

69. Jon Leibowitz, Comm'r, FTC, Prepared Statement of the Federal Trade Commission on "Social Security Numbers in Commerce: Reconciling Beneficial Uses with Threats to Privacy" 1 (May 11, 2006), available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-social-security-numbers-commerce-reconciling-beneficial/p034302commissiontestimonyconcerningsocialsecuritynumbersincommerce05112006.pdf (on file with the *Columbia Law Review*).

consisted of "more than 30 staff members with expertise in privacy, data security, and identity theft."[70]

DPIP enforces Section 5, and, until recently, it enforced the Fair Credit Reporting Act (FCRA) and Gramm-Leach-Bliley Act (GLBA). It now enforces the Children's Online Privacy Protection Act of 1998 (COPPA).[71] Prior to COPPA's recent transfer to DPIP, DAP was responsible for enforcing the rules. Finally, the DENF is responsible for ensuring compliance with FTC orders, many of which (like the settlement orders with Google, Facebook, Twitter, MySpace, Path, etc.) deal with privacy practices.[72]

In spite of the jurisdictional limitations discussed above, a modest number of enforcement actions, and a relatively small number of personnel devoted to privacy enforcement, the FTC has become the dominant enforcer of privacy. How and why did this happen? There are two key reasons: (1) the FTC's jurisdiction expanded considerably and (2) the FTC's enforcement framework was so uniquely compatible with the self-regulatory approach urged by policymakers.

1. *Expansion of Jurisdiction.* — Part of this story is due to a series of expansions in the FTC's jurisdiction. Like many areas in policy, the FTC's rise to de facto privacy authority can be partially attributed to being in the right place at the right time. The FTC long had the authority (since 1970) to enforce FCRA,[73] which was passed to ensure that consumer reporting agencies respected consumers' privacy. But until the late 1990s, few other privacy laws granted the FTC new enforcement powers.[74] In 1998, Congress gave the FTC rulemaking and enforcement authority under COPPA.[75] In 1999, under GLBA, Congress gave the FTC, among other agencies, the authority to "establish appropriate standards for the financial institutions subject to their jurisdiction" in order to "insure the

---

70. Id.

71. See, e.g., John Eggerton, FTC Moving COPPA Under Privacy Division, Broadcasting & Cable (Feb. 15, 2013, 3:27 AM), http://www.broadcastingcable.com/article/491892-FTC_Moving_COPPA_Under_Privacy_Division.php (on file with the *Columbia Law Review*). The Consumer Financial Protection Bureau (CFPB) is assuming rulemaking responsibility under GLBA and FCRA. See, e.g., M. Maureen Murphy, Cong. Research Serv., RS20185, Privacy Protection for Customer Financial Information 5 (2012), available at http://www.fas.org/sgp/crs/misc/RS20185.pdf (on file with the *Columbia Law Review*) ("On July 21, 2011, the CFPB began operations, assuming, among other things, authority to issue regulations and take enforcement actions under enumerated federal consumer protection laws, including both FCRA and GLBA." (footnotes omitted)).

72. E.g., Division of Enforcement, FTC, http://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-enforcement (on file with the *Columbia Law Review*) (last visited Mar. 8, 2014) (describing DENF role in monitoring compliance with orders entered in FTC consumer protection cases).

73. 15 U.S.C. § 1681s (2012).

74. See generally Statutes Enforced or Administered by the Commission, FTC, http://www.ftc.gov/ogc/stat3.shtm (on file with the *Columbia Law Review*) (last visited Mar. 2, 2014) (listing consumer protection statutes to date).

75. 15 U.S.C. §§ 6501–6506.

security and confidentiality of customer records and information" and "protect against unauthorized access."[76]

Other privacy laws that gave FTC enforcement powers relied heavily upon the same notice-and-choice structure that was already emerging in areas where statutes were not in force. For example, COPPA created a regime requiring notice and parental consent, with the notice being in the form of privacy policies.[77] GLBA created a notice-and-choice regime, with privacy policies and an opt-out right.[78] Beyond general requirements of data security, these regimes largely refrained from dictating what kinds of data would be collected or how it would be used so long as there was adequate notice in the form of a privacy policy.

The FTC was also given enforcement authority against companies failing to comply with the Safe Harbor Agreement between the United States and the European Union.[79] Dissatisfied with the extensively self-regulatory approach in the United States as well as all the gaps in statutory protection, E.U. regulators did not deem the United States to have an adequate level of protection. The E.U. Data Protection Directive of 1996 required that E.U. member nations not transfer personal data to countries that lacked an "adequate level of protection" of privacy. The situation threatened international commerce, which depended upon the smooth flow of data between E.U. member nations and the United

---

76. Id. §§ 6801–6809.

77. Id. § 6502(b)(1)(A) (instructing FTC to promulgate regulations requiring certain websites to post data collection and disclosure practices and obtain parental consent for "collection, use, or disclosure of personal information [obtained] from children").

78. Id. § 6802(a)–(b) (establishing notice requirements and consumer opt-out option). The FTC has identified two different possible privacy protection regimes: the "'notice-and-choice model,' which encourage[s] companies to develop privacy policies describing their information collection and use practices" to consumers, so that consumers can make informed choices, and the "'harm-based model,' which focuse[s] on protecting consumers from specific harms—physical security, economic injury, and unwarranted intrusions into their daily lives." FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 2 (2012) [hereinafter FTC, Protecting Consumer Privacy], available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (on file with the *Columbia Law Review*).

79. See, e.g., Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7, 26–30 (discussing FTC enforcement authority); Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000) (same); Int'l Trade Admin., U.S. Dep't of Commerce, U.S.-EU Safe Harbor Overview, Export.gov, http://www.export.gov/safeharbor/eu/eg_main_018476.asp (on file with the *Columbia Law Review*) (last updated July 1, 2013) ("Under the Federal Trade Commission Act, for example, an organization's failure to abide by commitments to implement the Safe Harbor Privacy Principles might be considered deceptive and actionable by the Federal Trade Commission."); see also Robert R. Schriver, Note, You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission, 70 Fordham L. Rev. 2777, 2792 (2002) ("Assuming these [private sector] measures fail, enforcement then lies with the FTC . . . .").

States. In 2000, the U.S. Department of Commerce and E.U. regulators negotiated the Safe Harbor Agreement to work around these problems. The Safe Harbor Agreement allows companies that agree to follow its seven data-protection principles to be deemed to have adequate privacy protection.[80]

In order for the Safe Harbor Agreement to work, there had to be an enforcement mechanism. In the European Union and in many countries throughout the world, there were data-protection authorities to regulate information privacy. With the United States lacking such an agency, the most obvious agency to turn to for enforcement was the FTC. Under the Safe Harbor Agreement, companies had to agree to be subject to FTC enforcement authority if they violated the principles.[81]

Thus, between 1995 and 2000, the FTC jumped into the privacy regulatory space in a dramatic way, acquiring new power with each passing year. As the FTC began to enforce COPPA and GLBA, it largely followed the same model as the notice-and-choice regime it relied upon to enforce its general Section 5 powers.[82] Although the Safe Harbor Agreement was slightly more restrictive than the notice-and-choice approach, it was not significantly different. Therefore, partly due to the FTC's embrace of the self-regulatory approach, its impeccable timing, a large void in U.S. privacy law, and lack of existing alternatives, the FTC became the go-to agency for privacy.

2. *The Lynchpin Function of FTC Enforcement.* — The FTC solidified its role by lending credibility to the self-regulatory approach. Under self-regulation, businesses essentially determined for themselves the basic rules they will adhere to regarding data collection, use, and disclosure. They stated these rules in their privacy policies. FTC enforcement added some teeth to the promises in privacy policies, most of which lacked any penalty or consequence if a company failed to live up to its promises.

FTC enforcement serves as the lynchpin to the Safe Harbor Agreement, and its Section 5 privacy enforcement serves as the lynchpin that makes the U.S. self-regulatory approach more than hollow. The FTC's dominance in privacy is in part due to its playing this lynchpin function. The FTC has filled a great void, and without the FTC, the U.S. approach to privacy regulation would lose nearly all its legitimacy. The FTC has essentially turned a mostly self-regulatory regime into one with some oversight and enforcement.

As Steven Hetcher posits regarding the website industry, the FTC created "a collective good that the industry would be interested to promote, the avoidance of congressional legislation. The agency threatened to push for legislation unless the industry demonstrated greater respect

---

80. See Int'l Trade Admin., U.S. Dep't of Commerce, supra note 79 (explaining seven Safe Harbor principles).

81. See id.

82. See infra Part III.A (discussing FTC privacy and security cases).

for privacy."[83] The FTC leveraged its very limited powers and fragmented authority to hoist itself into the position of being the dominant regulatory force for data privacy.

The FTC could have become little more than a rubber stamp on a self-regulatory regime. With limited powers and resources, the FTC could have become largely ignored by companies. Indeed, the FTC lacks the general authority to issue civil penalties and rarely fines companies for privacy-related violations under privacy-related statutes or rules that provide for civil penalties. Absent such grounds for issuing a civil penalty, the FTC is limited to fining companies under a contempt action for violating a settlement order.[84] Of the more than 170 privacy-related settlement agreements, only one resulted in civil fines for exclusive violations of Section 5 in violation of a previous consent order.[85]

When the FTC does include fines, they are often quite small in relation to the gravity of the violations and the overall net profit of the violators. This is because any fines issued by the FTC must reflect the amount of consumer loss.[86] For example, in a 2012 case charging Google with bypassing settings on Apple's Safari web browser, the FTC issued a $22.5 million dollar fine, the largest fine for privacy violations in its history. But as at least one news media article noted, the fine "is a small drop in the

---

83. Hetcher, De Facto, supra note 60, at 131; see also Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Books and on the Ground, 63 Stan. L. Rev. 247, 313 (2011) (identifying FTC's importance in "structuring and advancing a collective understanding of privacy").

84. E.g., United States v. Google Inc., No. CV 12-04177 SI, at 7 (N.D. Cal. Nov. 16, 2012) (order), available at http://www.ftc.gov/sites/default/files/documents/cases/2012/11/121120googleorder.pdf (on file with the *Columbia Law Review*) (approving $22.5 million civil penalty for violation of previous consent order).

85. Cf. FTC, Legal Resources, supra note 64 (providing links to recent FTC cases related to privacy and security). This does not include the small number of suspended judgments and disgorgements. E.g., FTC v. ControlScan, Inc., FTC File No. 072 3165, at 6 (N.D. Ga. 2009) (judgment & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2010/02/100225controlscanstip.pdf (on file with the *Columbia Law Review*) (suspending $750,000 monetary judgment pending compliance with other requirements of order); FTC v. Rapp, No. 99-WM-783 (D. Colo. June 27, 2000) (order), available at http://www.ftc.gov/sites/default/files/documents/cases/2000/06/ftc.govtouchtoneorder.htm (on file with the *Columbia Law Review)* (suspending $200,000 in monetary relief pending compliance with other requirements of order); In re Vision I Props., LLC, 139 F.T.C. 296, 305 (2005) (decision & order) (agreeing to pay $9,101.63 to U.S. Treasury as disgorgement); In re Gateway Learning Corp., 138 F.T.C. 443, 470 (2004) [hereinafter Gateway Decision & Order] (decision & order) (agreeing to pay $4,608 to U.S. Treasury as disgorgement).

86. See, e.g., United States' Response to Consumer Watchdog's Amicus Curiae Brief at 9, United States v. Google Inc., No. 3:12-cv-04177-SI (N.D. Cal. Sept. 28, 2012), available at http://www.consumerwatchdog.org/resources/ftcresponse092812.pdf (on file with the *Columbia Law Review*) (arguing "Commission must examine a number of factors, including the benefit obtained by the alleged violator and the harm suffered by consumers" in determining appropriate civil penalty); see also United States v. Danube Carpet Mills, Inc., 737 F.2d 988, 993 (11th Cir. 1984) (indicating "injury to the public" as factor in determining penalty amount).

bucket" because the previous year "Google earned $37.9 billion in revenue."[87]

Beyond fines, cases bring bad press. However, the general public rarely pays attention to FTC privacy actions. Thus, the reputational damage is largely within the community of privacy professionals and the entities that do business with a particular company.

How, then, does the FTC exert influence over companies? One possible method is through fear: Businesses fear the length of the FTC's auditing process—twenty years in more than fifty percent of the cases.[88] The auditing process is exhaustive and demanding. A typical assessment requires the specific detailing of the agreed-upon safeguards to protect consumer information; an explanation of "how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered device functionality or covered information"; an explanation of "how the safeguards that have been implemented meet or exceed the protections" agreed upon in the consent order; and a certification of the effectiveness of the company's protections by "a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession."[89]

The FTC has essentially been inching itself into the role of a de facto federal data protection authority. Perhaps this slow and incremental development is one reason why there has been a dearth of scholarship about the FTC. Over the past fifteen years, the FTC has gradually accumulated territory and power. It developed a body of doctrines one by one in a form that most legal academics do not pay much attention to.

II. FTC SETTLEMENTS AS DE FACTO COMMON LAW

In nearly all of the FTC's Section 5 cases and complaints alleging violations of COPPA, GLBA, and the Safe Harbor Agreement, the final disposition of the matter is a settlement, default judgment, or abandonment of the action by the FTC in the investigatory stage. The result is that there are hardly any judicial decisions in this arena.[90] This Part will

87. Gerry Smith, FTC: Google to Pay Record Fine over Safari Privacy Violation, Huffington Post (Aug. 9, 2012, 1:48 PM), http://www.huffingtonpost.com/2012/08/09/ftc-google-fine-safari-privacy-violation_n_1760281.html (on file with the *Columbia Law Review*).

88. Eighty-six of the FTC's 154 privacy-related settlement orders analyzed had components that lasted for twenty years. See FTC, Legal Resources, supra note 64 (listing recent FTC cases related to privacy and security).

89. In re HTC Am. Inc., FTC File No. 122 3049, No. C-4406, at 5 (F.T.C. July 2, 2013) (consent order) [hereinafter HTC Consent Order], available at http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf (on file with the *Columbia Law Review*).

90. A notable exception here is for the FCRA, due to the fact that the statute offers a privacy right of action where COPPA, GLBA, Section 5, and the Safe Harbor do not. Yet

explore the mechanics of these settlement agreements and describe how and why they have come to function as a de facto body of common law.

Technically, consent orders legally function as contracts rather than as binding precedent.[91] Yet, in practice, the orders function much more broadly than a contract between a company and the FTC. In the world of privacy law practice, everything the FTC says and does is delicately parsed, like the statements of the Chairman of the Federal Reserve. Chris Wolf, director of Hogan Lovells's Privacy and Information Management Practice Group, reads every FTC consent order immediately when it is issued. He explains:

> First, the alleged violations precipitating the consent orders reflect conduct the FTC believes is a violation of Section 5 (or whatever statute within its jurisdiction relied upon) and companies that engage in the same or similar conduct can expect an investigation and an allegation of illegal conduct from the FTC. Second, the orders sometimes reflect what the FTC believes are best practices. . . . Where a comprehensive privacy or security program is required, the outlines of such programs may be instructive for companies to follow.[92]

Critics of the FTC have complained that the FTC acts in an unpredictable fashion and that companies lack guidance about what they ought to do.[93] For example, Michael Scott has critiqued FTC unfairness actions related to data security as "seemingly filed at random, without any guidelines, and without any advance notice to the respondents that their actions might violate § 5 of the FTC Act."[94] Scott notes that "[t]he complaints and consent orders entered into in these cases provide limited guidance as to what a company should do (or not do) to avoid being the

---

even the FTC's actions under FCRA have been limited, with only forty-one privacy-related claims, almost all of which were disposed of by consent decree. See generally FTC, 40 Years of Experience with the Fair Credit Reporting Act (2011), http://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf (on file with the *Columbia Law Review*) (providing staff interpretations of Fair Credit Reporting Act).

91. See United States v. ITT Cont'l Baking Co., 420 U.S. 223, 238 (1975) ("[A] consent decree or order is to be construed for enforcement purposes basically as a contract . . . ."); United States v. Armour & Co., 402 U.S. 673, 681–82 (1971) ("Consent decrees are entered into by parties to a case after careful negotiation has produced agreement on their precise terms."); cf. 1 Stephanie W. Kanwit, Federal Trade Commission § 12:6 (2013) ("[A]ny other interpretation would hamper the consent settlement process.").

92. Email from Chris Wolf, Dir., Privacy & Info. Mgmt. Grp., Hogan Lovells, to author (Mar. 31, 2013, 11:21 AM) [hereinafter Wolf Interview] (on file with the *Columbia Law Review*).

93. See, e.g., Stegmaier & Bartnick, Psychics, supra note 9, at 676 (asserting FTC's use of unclear standard and lack of authoritative guidance may result in lack of constitutionally required fair notice).

94. Scott, supra note 21, at 183 (footnote omitted).

target of an unfairness action by the FTC if it experiences a security breach."[95]

In this Part, we contend that in contrast to these critics' allegations, the FTC has *not* been arbitrary and unpredictable in its enforcement. FTC enforcement has certainly changed over the course of the past fifteen years, but the trajectory of development has followed a predictable set of patterns. These patterns are those of common law development. Indeed, we argue that the body of FTC settlements is the functional equivalent of privacy common law. Understood as such, there is nothing unusual about how the doctrines emerging from the FTC settlements have evolved. We explore what this body of doctrines holds and the directions in which it is developing.

A. *The Anatomy of an FTC Action*

In order to understand the importance of the FTC's body of law, it is important to understand the make-up of the agency and the mechanics of its actions. The FTC is headed by five commissioners, appointed by the President and confirmed by the Senate for staggered seven-year terms.[96] Commissioners may not be removed except for "inefficiency, neglect of duty, or malfeasance in office."[97] No more than three commissioners can be members of the same political party.[98] The President chooses one commissioner to act as chairman.[99] As of April 2014, Edith Ramirez is the Chairwoman.[100] The other commissioners are Julie Brill, Maureen K. Ohlhausen, and Joshua D. Wright, with one commissioner seat vacant.[101]

The FTC has three major categories of authority: investigation, enforcement, and litigation.[102] Within its consumer protection authority,

---

95. Id.

96. 15 U.S.C. § 41 (2012); 16 C.F.R. § 0.1 (2013).

97. 15 U.S.C. § 41; see also Humphrey's Ex'r v. United States, 295 U.S. 602, 631–32 (1935) (holding Commissioner could be removed only for cause, not for partisan political reasons).

98. 15 U.S.C. § 41.

99. Id.

100. Commissioners, FTC, http://www.ftc.gov/commissioners/index.shtml (on file with the *Columbia Law Review*) (last modified Mar. 21, 2013).

101. Id.; see also FTC, Federal Trade Commission Organizational Chart 1, available at http://www.ftc.gov/ftc/ftc-org-chart.pdf (on file with the *Columbia Law Review*) (last visited Feb. 7, 2014) (showing commissioner vacancy). Pursuant to 16 C.F.R. § 4.14(b), part of the Rules of Practice, "[a] majority of the members of the Commission in office and not recused from participating in a matter (by virtue of 18 U.S.C. 208 or otherwise) constitutes a quorum for the transaction of business in that matter." § 4.14(b); see also FTC v. Flotill Prods., Inc., 389 U.S. 179, 188–90 (1967) (holding simple majority of commissioners sufficient for quorum). Further, an "affirmative concurrence of a majority of the participating Commissioners" is required in order for any action to be taken. 16 C.F.R. § 4.14(c).

102. See generally Overview of FTC Authority, supra note 2 (discussing FTC's categories of authority).

the FTC can use both its administrative and judicial enforcement powers.[103] The FTC's administrative enforcement consists of both rulemaking authority as well as adjudicatory authority. Generally, "[t]he Commission may . . . prosecute any inquiry necessary to its duties in any part of the United States"[104] and may "gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce . . . ."[105]

The FTC has stated that "[p]re-complaint investigations are generally non-public and, thus, are not identified on . . . [the agency's] site. On occasion the existence of an investigation may be identified in a press release."[106] The FTC actively monitors for unfair and deceptive trade practices, though due to a relatively small staff and limited budget, the FTC is often forced to rely on informal complaints by consumers and the press, as well as self-reporting, to become aware of potentially wrongful activity.[107]

The FTC "may initiate an enforcement action if it has 'reason to believe' that the law is being or has been violated."[108] If after conducting an investigation the FTC staff determines corrective action is needed, the staff issues a proposed complaint and order setting out the nature of the illegal act and the remedy.[109] After the FTC issues a complaint, the respondent can choose to either settle the FTC's charges or dispute the charges in front of an administrative or federal district court judge.[110]

---

103. Id.

104. 15 U.S.C. § 43.

105. Id. § 46(a).

106. Overview of FTC Authority, supra note 2. The FTC is restricted in its ability to publicize disputes preresolution. See 15 U.S.C § 57b-2 (establishing procedures for document retention and exempting certain items from public disclosure); see also FTC Administrative Staff Manuals, FTC, http://www.ftc.gov/foia/adminstaffmanuals.shtm (on file with the *Columbia Law Review*) (last visited Feb. 7, 2014) (containing links to policies on investigations, confidentiality, and disclosure).

107. FTC, Performance & Accountability Report Fiscal Year 2012, at 6 (2012), available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-performance-and-accountability-report/2012parreport.pdf (on file with the *Columbia Law Review*) (noting "agency's workforce consists of over 1,100 civil service employees dedicated to addressing the major concerns of American consumers," 613 of whom are attorneys).

108. Overview of FTC Authority, supra note 2 (emphasis omitted).

109. 16 C.F.R. § 2.31–.32 (2013).

110. See, e.g., Kovacic, supra note 66, at 42–43 ("When the Commission determines that there is 'reason to believe' that a law violation has occurred, the Commission can vote to issue a complaint setting forth its charges. If the respondent elects to contest the charges, the complaint is adjudicated before an ALJ . . . under the Commission's Rules of Practice."); see also David M. FitzGerald, The Genesis of Consumer Protection Remedies Under Section 13(b) of the FTC Act 4–5 (2004), available at http://www.ftc.gov/sites/default/files/documents/public_events/FTC%2090th%20Anniversary%20Symposium/fit

The FTC negotiates and settles the majority of actions it initiates through prescribed consent order procedures.[111] The FTC Procedures and Rules of Practice allow anyone being investigated to submit a proposed consent order agreement where "time, the nature of the proceeding, and the public interest permit."[112] Generally, however, the FTC initiates the consent order procedure. According to the FTC:

> If the respondent elects to settle the charges, it may sign a consent agreement (without admitting liability), consent to entry of a final order, and waive all right to judicial review. If the Commission accepts such a proposed consent agreement, it places the order on the record for thirty days of public comment (or for such other period as the Commission may specify) before determining whether to make the order final.[113]

One of the main motivations for settling with the FTC is that it allows the company to avoid admitting wrongdoing in exchange for remedial measures. As will be discussed in Part II.B, virtually all the administrative enforcement actions discussed in this Article are settled in this manner.[114]

Companies that violate these settlement orders are liable for a civil penalty of up to $16,000 for each violation.[115] In addition to civil penalties, a district court in a suit brought to enforce the order may also issue injunctions and other equitable relief.[116] However, there is no private cause of action under Section 5 for consumers who are victims of an unfair or deceptive trade practice.[117] Thus, the FTC's complaints and settlement orders constitute most of its privacy activity.[118]

B. *FTC Settlements*

The FTC has issued over 170 privacy-related complaints against companies.[119] Yet virtually every complaint has either been dropped or set-

---

zgeraldremedies.pdf (on file with the *Columbia Law Review*) (describing how FTC uses its 13(b) power to file complaints in federal court).

111. 16 C.F.R. § 2.31–.34.

112. Id. § 2.31.

113. Overview of FTC Authority, supra note 2.

114. See, e.g., 1 Kanwit, supra note 91, § 12:1 (noting majority of actions are settled by negotiations through consent order procedures).

115. Press Release, Commission Approves Federal Register Notice Adjusting Civil Penalty Amounts, FTC (Dec. 23, 2008), http://www.ftc.gov/opa/2008/12/civilpenalty.shtm (on file with the *Columbia Law Review*) (announcing increases in civil penalties).

116. Kanwit, supra note 91, § 12:1.

117. Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2012).

118. As will be discussed below, states look to the FTC's interpretation of the FTCA in their own consumer protection enforcement actions, which creates a ripple effect. Infra note 179 and accompanying text.

119. See, e.g., FTC, Legal Resources, supra note 64 (providing links to privacy-related complaints); Cases and Proceedings, FTC, http://www.ftc.gov/os/caselist/index.shtm (on file with the *Columbia Law Review*) (last modified Feb. 7, 2011) (listing privacy-related

tled.[120] Only one case has yielded a judicial opinion—*FTC v. Accusearch Inc.*, where the Tenth Circuit broadly supported the FTC's authority under Section 5 to bring an action against a company that wrongfully collected and disseminated confidential information.[121] The only other two nondisposed-of cases, *FTC v. Wyndham Worldwide Corp.*[122] and *In re LabMD, Inc.*,[123] currently await resolution in federal district court and the FTC Office of Administrative Law Judges, respectively.

Why do these cases hardly ever make it to court? One reason might be that it is too costly. In most instances, there is no threat of financial penalties for violating Section 5, and thus there is little financial incen-

---

actions issued by FTC); see also Bureau of Consumer Protection, Privacy and Security, supra note 63 (providing compliance resources for companies). While this research has attempted to be exhaustive, for the purpose of this Article's analysis, complaints against multiple parties for the same incident are counted as one complaint and settlement, given the nearly identical overlap in analysis. It is also important to note that in many instances the FTC allegations of a Section 5 violation were based directly on the violation of a statute or other rule. In other instances, the FTC's specific theory of liability was unclear. When the FTC alleged that activity was "false or misleading," the assumption is that the FTC was asserting the activity was deceptive, as opposed to unfair.

120. Of the 154 complaints reviewed for this Article, only six had no accompanying settlement agreement. E.g., Complaint for Permanent Injunction and Other Equitable Relief, FTC v. 77 Investigations, Inc., No. EDCV06-0439 VAP (C.D. Cal. filed May 1, 2006), available at http://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501-77investigcmplt.pdf (on file with the *Columbia Law Review*); Complaint for Injunctive and Other Equitable Relief, FTC v. Corporate Mktg. Solutions, Inc., No. CIV-02 1256 PHX RCB (D. Ariz. filed July 18, 2002) [hereinafter Corporate Mktg. Solutions Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2002/07/cmscmp.pdf (on file with the *Columbia Law Review*). The FTC did not include a settlement agreement in at least one case, though the defendant apparently did agree to settle the complaint with the FTC. Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief, United States v. First Advantage SafeRent, Inc., No. 8:10-cv-00090-PJM (D. Md. filed Jan. 14, 2010), available at http://www.ftc.gov/sites/default/files/documents/cases/2010/02/100202saferentcmpt.pdf (on file with the *Columbia Law Review*); see also Press Release, Tenant Screening Agency Settles FTC Charges: Failed to Respond to Consumers' Requests for Their Files or Investigate Disputes, FTC (Feb. 2, 2010), http://ftc.gov/opa/2010/02/saferent.shtm (on file with the *Columbia Law Review*) (reporting defendant "agreed to settle Federal Trade Commission charges that it violated federal law" in amount of $100,000).

121. 570 F.3d 1187, 1193–95 (10th Cir. 2009) ("[T]he FTCA enables the FTC to take action against unfair practices that have not yet been contemplated by more specific laws.").

122. First Amended Complaint for Injunctive and Other Equitable Relief, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-PGR (D. Ariz. filed Aug. 9, 2012) [hereinafter Wyndham Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (on file with the *Columbia Law Review*); see also Julie Sartain, Analyzing *FTC v. Wyndham*, Int'l Ass'n of Privacy Prof'ls (Oct. 5 2012), https://www.privacyassociation.org/publications/2012_10_11_analyzing_ftc_vs._wyndham (on file with the *Columbia Law Review*) (discussing current FTC claims and Wyndham's motion to dismiss).

123. Complaint, In re LabMD, Inc., FTC File No. 102 3099, No. 9357 (F.T.C. Aug. 29, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf (on file with the *Columbia Law Review*).

tive to spend a great deal of time and resources fighting FTC complaints. The FTC is limited to seeking equitable monetary relief in actions under section 13(b) of the FTCA, which constitute a majority of the FTC's complaints in this area.[124] When the FTC has issued penalties for privacy-related violations, they have ranged from $1,000[125] to $35 million.[126] In most instances (particularly those not involving a separate allegation of a statutory violation), companies pay nothing in response to a violation.[127] In cases where companies might have to pay money in response to a violation, the companies that have settled with the FTC likely pay less than those that do not respond to the complaint and are subjected to a default judgment.[128] Settling with the FTC also allows for companies to "elimi-

---

124. Overview of FTC Authority, supra note 2. The FTC has summarized its authority as follows:

> Section 13(b) of the FTC Act authorizes the Commission to seek preliminary and permanent injunctions . . . . In the early and mid-1980s, . . . the Commission argued that the statutory reference to "permanent injunction" entitled the Commission to obtain an order not only permanently barring deceptive practices, but also imposing various kinds of monetary equitable relief (*i.e.*, restitution and rescission of contracts) to remedy past violations. . . . The courts have uniformly accepted the Commission's construction of Section 13(b), with the result that most consumer protection enforcement is now conducted directly in court under Section 13(b) rather than by means of administrative adjudication.

Id. (citation omitted).

125. E.g., United States v. Godwin (*Skidekids*), No. 1:11-cv-03846-JOF, at 6 (N.D. Ga. Feb. 1, 2012) (consent decree & order) [hereinafter Godwin Consent Decree & Order], available at http://www.ftc.gov/sites/default/files/documents/cases/2011/11/111108skidekidsorder.pdf (on file with the *Columbia Law Review*) (agreeing to total penalty of $100,000 with all but $1,000 suspended). A review of all the FTC's privacy and data-security-related consent orders reveals that the lowest "stand-alone" civil penalty for a privacy-related violation with no suspended amount was $2,000. E.g., FTC v. Garrett, No. H-01-1255, at 5 (S.D. Tex. Mar. 8, 2002) (judgment & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2002/03/discreetdatastip.pdf (on file with the *Columbia Law Review*); FTC v. Guzzetta, No. 01-2335(DGT), at 6 (E.D.N.Y. Feb. 22, 2002) (judgment & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2002/03/guzzettastip.pdf (on file with the *Columbia Law Review*).

126. E.g., FTC v. LifeLock, Inc., No. 072 3069, at 8 (D. Ariz. Mar. 9, 2010) [hereinafter LifeLock Judgment & Order] (judgment & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockstip.pdf (on file with the *Columbia Law Review*).

127. Cf. Overview of FTC Authority, supra note 2 (explaining court can award both prohibitory and monetary equitable relief); supra note 124 and accompanying text (describing FTC's limitation to only equitable monetary relief in actions under section 13(b) of FTC Act).

128. Compare, e.g., FTC v. Action Research Grp., Inc., No. 6:07-cv-00227-Orl-22UAM, at 1, 5 (M.D. Fla. Mar. 18, 2008) (stipulated order & settlement), available at http://www.ftc.gov/sites/default/files/documents/cases/2008/05/080528fo.pdf (on file with the *Columbia Law Review*) (entering $67,000 judgment against several codefendants who settled with FTC), with, e.g., FTC v. Action Research Grp., Inc., No. 6:07-cv-227-ORL-22GJK, at 1, 6 (M.D. Fla. Mar. 18, 2008) (default judgment), available at http://www.ftc.gov/sites/default/files/documents/cases/2008/05/080528judgmentwagner.pdf (on file

nate the uncertainty and expense of lengthy negotiation and pretrial preparation and litigation."[129]

Another reason companies are reluctant to challenge administrative complaints is that, in administrative adjudication, a "reviewing court must also accord substantial deference to Commission interpretation of the FTC Act and other applicable federal laws."[130] Such deference makes a challenger's victory less likely and risks the creation of an adverse precedent. Additionally, the FTC might be willing to settle for less severe provisions in an order than it would demand via litigation due to "the public interest savings in time, money, and uncertainty which the settlement will provide."[131] It appears that given the FTC's limited resources, the Commission also tends to target cases with a high likelihood of success and where companies have no viable defense. David Vladeck, a law professor and former director of the Bureau of Consumer Protection of the FTC, using data security complaints as an example, stated, "[FTC] [s]taff wouldn't bring a close case to the Commission. . . . I think it is fair to say that if there is an argument that a company's security practices are within the bounds of reasonableness the FTC would not bring a security case."[132]

Finally, since settlement agreements do not concede liability, companies are able to move forward without having to admit wrongdoing.[133] Companies may be motivated to avoid the reputational costs of apologizing.[134]

The FTC has virtually unrestrained discretion to define the "access and scope of the consent order process."[135] The common FTC consent

---

with the *Columbia Law Review*) (entering default judgment of $428,085 against codefendant, Wagner, in same action).

129. 1 Kanwit, supra note 91, § 12:4. It should be noted, however, that, "negotiations of a consent in a particularly difficult case may also be lengthy, and the FTC may not accept an order until months (or years) after it is signed." Id. at n.3.

130. Overview of FTC Authority, supra note 2; see also Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842–44 (1984) ("If Congress has explicitly left a gap for the agency to fill, there is an express delegation of authority to the agency . . . . Such legislative regulations are given controlling weight unless they are arbitrary, capricious, or manifestly contrary to the statute."); Jeff Sovern, Private Actions Under the Deceptive Trade Practices Acts: Reconsidering the FTC Act as Rule Model, 52 Ohio St. L.J. 437, 443 & n.41 (1991) (outlining history of judicial deference afforded to FTC).

131. 1 Kanwit, supra note 91, § 12:4 (quoting In re Kraftco Corp., 3 Trade Reg. Rep. (CCH) ¶¶ 21,263, 21,171–21,172 (1977)) (internal quotation marks omitted).

132. Vladeck Interview, supra note 68.

133. Overview of FTC Authority, supra note 2 ("If the respondent elects to settle the charges, it may sign a consent agreement (without admitting liability), consent to entry of a final order, and waive all right to judicial review.").

134. See generally Somini Sengupta, F.T.C. Settles Privacy Issue at Facebook, N.Y. Times (Nov. 29, 2011), http://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html (on file with the *Columbia Law Review*) ("The settlement with the F.T.C., analysts say, could potentially ease investors' concerns about government regulation by holding the company to a clear set of privacy prescriptions.").

135. 1 Kanwit, supra note 91, § 12:1.

order contains financial penalties, bans on certain activities, and requirements for corrective action. It also commonly contains reporting, audit, and compliance requirements for up to twenty years.[136] However, the duration of many requirements in the agreements are varied, even within the order itself. For example, most of the requirements in the *United States v. Godwin* (*Skidekids*) consent order lasted for five years, while the recordkeeping requirement lasted for eight years.[137] In *FTC v. Frostwire, LLC*, the defendant was only required to report to the FTC for three years and engage in recordkeeping for six years.[138] If no termination date in a settlement order is given, the agreement may be perpetual, binding the entity's successors and assigns.[139]

More specifically, there are a number of common substantive aspects in FTC consent orders, in addition to other formalities and procedural requirements.

1. *Prohibitions on Wrongful Activities.* — The heart of a privacy-related FTC consent order is the prohibition on future wrongful activities. Generally speaking, companies that enter into a settlement agreement with the FTC are barred from engaging in the activities that were the subject of the FTC's complaint.[140] The FTC appears to strive for proportionality

136. See, e.g., Press Release, FTC Says Hello to 1996 by Waving Goodbye to Thousands of Administrative Orders that Are at Least 20 Years Old, FTC (Dec. 20, 1995), available at http://www.ftc.gov/news-events/press-releases/1995/12/ftc-says-hello-1996-waving-goodbye-thousands-administrative (on file with the *Columbia Law Review*) (noting both existing and future consent orders would last twenty years). It is important to note that not all obligations in a consent order last the entire length of the order, i.e., twenty years.

137. Godwin Consent Decree & Order, supra note 125, at 14–15.

138. FTC v. Frostwire, LLC, No. 11-cv-23643-CV-GRAHAM, at 13–16 (S.D. Fla. Oct. 12, 2011) [hereinafter Frostwire Final Order] (stipulated final order), available at http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111012frostwirestip.pdf (on file with the *Columbia Law Review*).

139. 1 Kanwit, supra note 91, § 12:4.

140. For examples of prohibitions in decisions and orders that track the activities alleged in the complaint, see, e.g., In re Lookout Servs., Inc., 151 F.T.C. 532, 536–37, 539 (2011) (complaint; decision & order); In re US Search, Inc., 151 F.T.C. 184, 187–88, 190 (2011) (complaint; decision & order). For additional examples of the proportionality between the activities alleged in the complaint and the terms of the final agreements, compare United States v. Teletrack, Inc., No. 1:11-cv-2060, at 5 (N.D. Ga. June 24, 2011) (stipulated final judgment), available at http://www.ftc.gov/sites/default/files/documents/cases/2011/06/110627teletrackstip.pdf (on file with the *Columbia Law Review*), United States v. Am. United Mortg. Co., No. 07C 7064, at 5 (N.D. Ill. Dec. 18, 2007) (stipulated final judgment & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2007/12/071217americanunitedmrtgstipfinal.pdf (on file with the *Columbia Law Review*), In re Twitter, Inc., FTC File No. 092 3093, No. C-4316, at 2 (F.T.C. Mar. 11, 2011) (decision & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf (on file with the *Columbia Law Review*), and In re Directors Desk, LLC, FTC File No. 092 3140, No. C-4281, at 2 (F.T.C. Jan. 19, 2010) (decision & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2010/01/100119directorsdeskdo.pdf (on file with the *Columbia Law Review*), with Complaint for Civil Penalties, Injunctive, and Other Equitable Relief at 6, United States v. Teletrack, Inc., No. 1:11-cv-2060 (N.D. Ga. June 24, 2011), available at http://www.ftc.

between the alleged wrongdoing and the restricted activity.[141] For example, companies accused of violating COPPA rules were prohibited from future COPPA-violating behavior.[142] Companies accused of misrepresenting plans to make certain files publicly accessible were similarly prohibited from making future misrepresentations.[143] Companies accused of unfairly designing software were prohibited from making similar design choices (such as making downloaded files public by default) without sufficient notice to consumers.[144]

2. *Fines and Other Monetary Penalties.* — As previously stated, the penalties have ranged from $1,000[145] to $35 million.[146] But fines in the form of "civil penalties" were not the only monetary loss for companies settling

---

gov/sites/default/files/documents/cases/2011/06/110627teletrackcmpt.pdf (on file with the *Columbia Law Review*), Complaint for Civil Penalties, Injunctive and Other Relief at 4–5, United States v. Am. United Mortg. Co., No. 07C 7064 (N.D. Ill. Dec. 17, 2007), available at http://www.ftc.gov/sites/default/files/documents/cases/2007/12/071217americanunitedmrtgcmplt.pdf (on file with the *Columbia Law Review*), Complaint at 3, In re Twitter, Inc., FTC File No. 092 3093, No. C-4316 (F.T.C. Mar. 11, 2011) [hereinafter Twitter Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf (on file with the *Columbia Law Review*), and Complaint at 3, In re Directors Desk, LLC, FTC File No. 092 3140, No. C-4281 (F.T.C. Jan. 19, 2010), available at http://www.ftc.gov/sites/default/files/documents/cases/2010/01/100119directorsdeskcmpt.pdf (on file with the *Columbia Law Review*).

141. See, e.g., Int'l Outsourcing Grp., Inc., FTC File No. 992 3245 (July 12, 2000) (Swindle, Comm'r, concurring in part and dissenting in part), available at http://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogswin.htm (on file with the *Columbia Law Review*) ("I do not believe that a false claim as to how personal information will be used is sufficient to justify imposing privacy requirements."); id. (statement of Pitofsky, Chairman, & Thompson, Comm'r), available at http://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogchair.htm (on file with the *Columbia Law Review*) ("[W]hile we agree with our colleague that not every case challenging false claims about how personal information is used necessitates the injunctive requirements to protect privacy included here, we think these are reasonably related to the alleged misconduct.").

142. E.g., Godwin Consent Decree & Order, supra note 125, at 1–4 (ordering company to comply with COPPA following violation).

143. E.g., Frostwire Final Order, supra note 138, at 5 (restraining defendants from misrepresenting that consumers' computers are not publicly sharing downloaded files).

144. E.g., id. at 7–8 (ordering compliance with notice and disclosure requirements for software distributions). However, some prohibitions were actually broader than the alleged wrongdoing. See, e.g., In re Chitika, Inc., 151 F.T.C. 494, 501, 504–06 (2011) (decision & order) (requiring extensive notice and disclosure of company's data-use policy after allegations Chitika made false or misleading representations regarding length of targeted advertising opt-out period).

145. Supra note 125 and accompanying text (stating lowest penalty with suspended amount was $1,000 and lowest penalty without any suspended amount was $2,000).

146. LifeLock Judgment & Order, supra note 126 (ordering defendants to pay $35 million in monetary relief).

with the FTC. Companies have also regularly agreed to disgorgement and remuneration to consumers,[147] as well as the freezing of assets.[148]

3. *Consumer Notification and Remediation*. — In many instances, the FTC has required a company to notify customers of its wrongdoing and even offer some form of redress. For example, in *FTC v. Frostwire, LLC*, a company had to deploy patches to previous versions of its software to remedy problematic user interfaces and default settings that rendered many of its consumers' files publicly accessible.[149] Similarly, in *In re Sony BMG Music Entertainment*, Sony had to uninstall problematic software it had installed on users' computers.[150] Other companies agreed to offer refunds to consumers for products associated with misrepresentation, which also effectively notified consumers of misrepresentations.[151] And Choicepoint had to pay more than $5 million for consumer redress.[152]

4. *Deleting Data or Refraining from Using It*. — The FTC has regularly attempted to mitigate the potential harm from wrongfully collected personal information by including in settlement orders requirements to delete or refrain from using that information. The requirement to delete wrongfully collected information is almost always included in settlements involving violations of COPPA.[153] Yet non-COPPA-related defendants, particularly those accused of collecting personal information through

147. E.g., Gateway Decision & Order, supra note 85 (agreeing to pay $4,608 to U.S. Treasury as disgorgement); In re Vision I Props., 139 F.T.C. 296, 311 (2005) (analysis) (agreeing to pay $9,101.63 to U.S. Treasury as disgorgement).

148. E.g., FTC v. GM Funding, Inc., No. SACV 02-1026 DOC (MLGx), at 5–7 (C.D. Cal. Nov. 27, 2002) (judgment & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2002/11/gmfundingstip.pdf (on file with the *Columbia Law Review*) (requiring transfer of all financial documents and assets to United States and freezing such documents and assets).

149. Frostwire Final Order, supra note 138, at 9 (describing transmission of patch "to all computers running" problematic software).

150. In re Sony BMG Music Entm't, FTC File No. 062 3019, No. C-4195, at 6 (F.T.C. June 28, 2007) (decision & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2007/06/0623019do070629.pdf (on file with the *Columbia Law Review*) ("For . . . two years after the date that this order becomes final, [respondent shall] continue to provide free of charge to consumers a program and a patch that uninstalls . . . content protection software and removes the 'privilege escalation vulnerability' associated with any covered product that contains [the] content protection software.").

151. E.g., In re US Search, Inc., 151 F.T.C. 188, 191–92 (2011) (decision & order) (specifying precise refund scheme).

152. United States v. Choicepoint Inc., No. 1:06-CV-0198, at 17–18 (N.D. Ga. Feb. 15, 2006) (stipulated final judgment), available at http://www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf (on file with the *Columbia Law Review*).

153. E.g., United States v. Artist Arena, LLC, No. 1:12-cv-07386-JGK, at 4 (S.D.N.Y. Oct. 3, 2012), available at http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121003artistarenadecree.pdf (on file with the *Columbia Law Review*) (ordering respondent to "delete all personal information collected and maintained" in violation of COPPA).

generally deceptive means or "inducement," have also agreed to delete wrongfully obtained consumer data.[154]

5. *Making Changes in Privacy Policies.* — The FTC often required companies to make modifications to their privacy policies to better notify users that their personal information is being collected, used, and shared.[155] If companies did not have a privacy policy, the FTC might require them to create one, perhaps under its authority to order corrective advertising.[156]

6. *Establishing Comprehensive Programs.* — In several instances, the FTC has required companies to establish a comprehensive security, privacy, or data-integrity program. For example, in *In re HTC America Inc.*, the company had to establish a "comprehensive security program" that was "fully documented in writing" and had to "contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered device functionality or covered information."[157] These particular safeguards may include risk assessments, employee training, and responsibility for security, among other things.[158]

The FTC has also mandated that companies establish a "comprehensive privacy program."[159] For example, in the Google Buzz consent order, Google agreed to establish and implement a "comprehensive privacy

---

154. E.g., In re Aspen Way Enters., Inc., FTC File No. 112 3151, No. C-4392, at 6 (F.T.C. Sept. 25, 2012) (consent order) [hereinafter Aspen Way Agreement & Order], available at http://www.ftc.gov/sites/default/files/documents/cases/2012/09/120925aspenwayagree.pdf (on file with the *Columbia Law Review*) (enjoining respondent from "using, in connection with collecting or attempting to collect a debt, money, or property pursuant to a covered rent-to-own transaction, any information or data obtained" and ordering respondent to "[d]elete or destroy all user data previously gathered using any monitoring or geophysical location tracking technology").

155. E.g., United States v. Sony BMG Music Entm't, No. 08 Civ. 10730 (LAK), at 4–5 (S.D.N.Y. Dec. 15, 2008) (consent decree), available at http://www.ftc.gov/sites/default/files/documents/cases/2008/12/081211consentp0823071.pdf (on file with the *Columbia Law Review*) (ordering "clear and conspicuous notice" of privacy policy in various locations on Sony BMG's website).

156. E.g., Warner-Lambert Co. v. FTC, 562 F.2d 749, 763–64 (D.C. Cir. 1977) (upholding order enjoining company from making certain representations and requiring company, for specific period, to make clarifying statements in future advertisements); see also Lesley Fair, FTC, Federal Trade Commission Advertising Enforcement 66–67 (2008), available at http://www.ftc.gov/sites/default/files/attachments/training-materials/enforcement.pdf (on file with the *Columbia Law Review*) (citing case in which FTC required company to post privacy policy). See generally Michael J. Pelgro, Note, The Authority of the Federal Trade Commission to Order Corrective Advertising, 19 B.C. L. Rev. 899 (1978) (discussing history and reach of FTC's corrective advertising power).

157. HTC Consent Order, supra note 89, at 3.

158. See, e.g., infra Part IV.B (describing FTC's deception jurisprudence as expanding beyond privacy policies and urging greater consumer expansion).

159. E.g., In re Google Inc., FTC File No. 102 3136, No. C-4336, at 4 (F.T.C. Oct. 13, 2011) (consent order), available at http://ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf (on file with the *Columbia Law Review*).

program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers and (2) protect the privacy and confidentiality of covered information."[160] The specifics of the program were similar to those in a comprehensive security program, such as requirements to identify risk, train employees, appoint a responsible coordinator of the program, and engage in regular evaluations of the program. Google also agreed to obtain program assessments from "a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession."[161] Facebook agreed to a similar privacy program in its consent order.[162]

7. *Assessments by Independent Professionals.* — Those accused of unfair or deceptive security practices often agree to biennial assessments by an independent professional to ensure compliance with the order.[163] The auditors' biennial reports must be made available to the FTC for two decades, and companies that fail to do so risk further penalty.[164] For example, as part of their FTC settlement agreements, Google, Facebook, MySpace, and Path created comprehensive privacy programs, which were subject to assessment by independent auditors.[165] The comprehensive programs include "putting employees in charge of privacy, identifying risks and establishing safeguards against violations."[166]

8. *Recordkeeping and Compliance Reports.* — Virtually every company that settled with the FTC agreed to engage in some kind of regular recordkeeping to facilitate the FTC's enforcement of the order.[167] In many instances, the company also agreed to regular reporting requirements.

---

160. Id. at 5.

161. Id.

162. In re Facebook, Inc., FTC File No. 092 3184, No. C-4365, at 5 (F.T.C. Nov. 29, 2011) (consent order), available at http://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf (on file with the *Columbia Law Review*) (parroting language of Google's consent order); see also FTC v. EMC Mortg., No. 4:08-cv-338, at 11 (E.D. Tex. Sept. 9, 2009) (decision & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2008/09/080909emcmortgstipfinljdgmnt.pdf (on file with the *Columbia Law Review*) (requiring "comprehensive data integrity program" similar to comprehensive privacy and security programs).

163. E.g., Verne Kopytoff, Privacy Audits Required of Internet Firms, S.F. Chron. (Mar. 10, 2013), http://www.sfgate.com/technology/article/Privacy-audits-required-of-Internet-firms-4343921.php; see also HTC Consent Order, supra note 89, at 5–6 (setting forth independent assessment requirements).

164. Kopytoff, supra note 163 (explaining failure can result in penalties of $16,000 per violation per day).

165. Id.

166. Id.

167. E.g., Aspen Way Agreement & Order, supra note 154, at 8 (mandating recordkeeping for five years after improper activity).

9. *Notification of Material Changes Affecting Compliance.* — Companies also are usually under the obligation to alert the FTC of any material changes in their organization that might affect compliance obligations, including "a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; [or] the proposed filing of a bankruptcy petition."[168] This notification is important given the privacy interests related to data sets and their commercial treatment as something to be collateralized.[169]

C. *The Privacy "Common Law" of the FTC*

Although the FTC's privacy cases nearly all consist of complaints and settlements, they are in many respects the functional equivalent of common law. While the analogy to traditional common law has its limits, it is nonetheless a useful frame to understand the FTC's privacy jurisprudence. Common law is a form of Anglo-American law that is characterized by incremental development through judicial decisions in a series of concrete cases.[170] The decisions serve as precedent—judges aim to decide cases consistently with previous decisions.[171] In the most traditional form of common law, judges develop the legal rules. Much of Anglo-American tort law, contract law, property law, and criminal law emerged through this process. Many parts of these bodies of law were later codified into statutes, especially criminal law, which today in the United States is almost entirely statutory.

There is also another form of common law that emerges through the interpretation of constitutions and statutes.[172] Although judges do

168. HTC Consent Order, supra note 89, at 7.

169. See, e.g., Xuan-Thao N. Nguyen, Collateralizing Privacy, 78 Tul. L. Rev. 553, 555–57 (2004) (arguing collateralization of databases amounts to collateralization of privacy).

170. Cf., e.g., Joseph Dainow, The Civil Law and the Common Law: Some Points of Comparison, 15 Am. J. Comp. L. 419, 419–20 (1967) (contrasting nature and function of common and civil law); Bernadette Meyler, Towards a Common Law Originalism, 59 Stan. L. Rev. 551, 552–59 (2006) (reviewing various interpretations of common law).

171. Cf., e.g., Frank B. Cross, Identifying the Virtues of the Common Law, 15 Sup. Ct. Econ. Rev. 21, 38 (2007) (discussing stability brought about by reliance on precedent in common law); Cass R. Sunstein, Is Tobacco a Drug? Administrative Agencies as Common Law Courts, 47 Duke L.J. 1013, 1019 (1998) (noting "basic task of common law courts is to specify abstract standards . . . and to adapt legal rules to particular contexts" and agencies like the FTC, operating as common law courts, have "considerable power to adapt statutory language to changing understandings and circumstances").

172. Cf., e.g., Abbe R. Gluck, The Federal Common Law of Statutory Interpretation: *Erie* for the Age of Statutes, 54 Wm. & Mary L. Rev. 753, 757 (2013) ("Exploring this possibility—that statutory interpretation methodology is some kind of judge-made law—allows for some significant doctrinal and theoretical interventions."); Note, Intent, Clear Statements, and the Common Law: Statutory Interpretation in the Supreme Court, 95 Harv. L. Rev. 892, 914 (1982) ("Envisioning statutes as common law would not free the

not create the initial rules, their decisions on the meaning of those rules have precedential effect and become essential to the interpretation of the rules. Indeed, the meaning of many provisions of constitutional and statutory law cannot be understood simply by looking to their text—the body of judicial decisions offering a gloss on those provisions is an essential component that must be consulted. The key factor that makes it imperative to consult these judicial decisions when interpreting constitutional or statutory text is the fact that the decisions have precedential weight.

FTC privacy settlements technically lack precedential force for other companies. The FTC is not strictly required to be consistent, but the FTC has demonstrated a commitment to remaining consistent in practice. As will be discussed, new complaints and settlement orders do not stray far from previous ones. Instead, the FTC incrementally develops this body of law in a stable way. Practitioners look to FTC settlements as though they have precedential weight.[173] The result is that lawyers consult and analyze these settlements in much the same way as they do judicial decisions. This Part will demonstrate how the FTC privacy settlements serve as the functional equivalent to a body of common law.

1. *FTC Settlements.* — Although the FTC has specific rulemaking authority under COPPA and GLBA,[174] for Section 5 enforcement—one of the largest areas of its jurisprudence—the FTC has only Magnuson-Moss rulemaking authority,[175] which is so procedurally burdensome that it is largely ineffective.[176] The FTC must rely heavily on its settlements to

courts from their obligation to implement legislative will; instead, the common law model would free the courts to implement that will.").

173. E.g., Wolf Interview, supra note 92.

174. Overview of FTC Authority, supra note 2, app. c ("Special Statutes that mandate or authorize Commission rulemakings either antitrust and/or consumer protection related . . . include the Graham-Leach-Bliley Act . . . [and] COPPA . . . ."). Note that the Consumer Financial Protection Bureau has transferred rulemaking authority from the FTC for the Fair Credit Reporting Act. Consumer Financial Protection Act of 2010, Pub. L. No. 111-203, § 1100H, 124 Stat. 1955, 2113 (codified as amended at 12 U.S.C. §§ 5481–5603 (2012)) (providing amendments to FCRA "shall become effective on the designated transfer date"); Designated Transfer Date, 75 Fed. Reg. 57,252 (Sept. 20, 2010) (establishing July 21, 2011 as date to transfer functions to CFPB).

175. Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93-637, 88 Stat. 2183 (1975) (codified as amended at 15 U.S.C. §§ 45–46, 49–52, 56–57c, 2301–2312 (2012)).

176. Beth DeSimone and Amy Mudge articulate why the Magnuson-Moss rules are largely ineffective:

> Right now, the FTC is constrained in its rulemaking by the so-called "Magnuson-Moss" rules. These rules require the FTC Staff to engage in an industry-wide investigation, prepare draft staff reports, propose a rule, and engage in a series of public hearings, including cross-examination opportunities prior to issuing a final rule in any area. These processes are so burdensome that the FTC has not engaged in a Magnuson-Moss rule-making in 32 years.

Beth DeSimone & Amy Mudge, Is Congress Putting the FTC on Steroids?, Arnold & Porter: Seller Beware (Apr. 26, 2010), http://www.consumeradvertisinglawblog.com/

signal the basic rules that it wants companies to follow. Indeed, this is how courts create rules in the common law. Because courts cannot legislate, they craft rules in judicial decisions, which remain in effect for future cases by way of precedent. When the FTC issues a settlement, it typically issues a complaint and settlement document simultaneously, and these are publicized on the FTC's website. Among privacy law practitioners, FTC settlements are major news and generate significant attention.[177]

Why are these settlements akin to common law? First, they are publicized, and the FTC follows them. Accordingly, they have a kind of precedential value, and they serve as a useful way to predict future FTC activity. Chris Wolf notes that "consent orders have immediate nationwide impact (to the extent they affect behavior) unlike in the litigation context, where there can be a split of authority on what is or is not prohibited conduct."[178] Additionally, every state has adopted some form of a consumer protection statute, often called "[L]ittle FTC Acts," many of which explicitly look to FTC interpretations of overlapping concepts to guide enforcement.[179]

Second, FTC settlements are viewed by the community of privacy practitioners as having precedential weight. Privacy lawyers routinely use FTC settlements to advise companies about how to avoid triggering FTC enforcement.[180] For example, Wolf notes that when counseling clients, he frequently references activities that triggered FTC actions.[181] Many firms that counsel clients on privacy matters routinely post and dissemi-

---

2010/04/is-congress-putting-the-ftc-on-steroids.html (on file with the *Columbia Law Review*); see also FTC, Rulemaking: Operating Manual, Chapter Seven, available at http://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch07rulemaking.pdf (on file with the *Columbia Law Review*) (last visited Feb. 7, 2014) (delineating rulemaking procedures under Magnuson-Moss Warranty Act).

177. Cf., e.g., infra Part III (providing overview of trends in development of FTC privacy jurisprudence).

178. Wolf Interview, supra note 92.

179. See, e.g., Jean Braucher, Deception, Economic Loss and Mass-Market Customers: Consumer Protection Statutes as Persuasive Authority in the Common Law of Fraud, 48 Ariz. L. Rev. 829, 851 (2006) (noting many state statutes "call upon state courts to interpret them in light of FTC interpretations" and courts often rely on FTC interpretations even when statutes are silent "because of the similarity of language between the FTC Act and the state 'little FTC Acts'"). But see Henry N. Butler & Joshua D. Wright, Are State Consumer Protection Acts Really Little-FTC Acts?, 63 Fla. L. Rev. 163, 182–88 (2011) ("[A] substantial majority of [state consumer protection act] litigation involves claims consistent with behavior that is likely legal under the FTC standard.").

180. See Wolf Interview, supra note 92 (describing practice of informing clients to conform conduct to FTC consent decrees to avoid liability); see also Email from Joel Winston, former Assoc. Dir., Div. of Privacy & Identity Prot., FTC, to authors (Apr. 8, 2013) [hereinafter Winston Interview] (on file with the *Columbia Law Review*) (discussing practice of many law firms of sending clients FTC settlement alerts that include highly detailed analyses of pleadings and predictions for future FTC action).

181. Wolf Interview, supra note 92.

nate information about recent FTC settlements on their blogs.[182] Addressing the precedential value of FTC settlements, David Vladeck states:

> It is not uncommon for lawyers representing respondents in agency proceedings—investigations and then formal complaints—to cite prior complaints or orders (consent or litigated) as "precedent" as to what constitutes an unfair or deceptive trade practice. And I think that practice makes sense. Complaints do signal the agency's view of the applicable law, and do inform regulated parties as to the agency's view of how the law applies to a discrete and identified set of facts. So it seems entirely appropriate that counsel would rely on them to draw inferences about the correctness, or fairness, of the agency's position in an investigation and contested action.[183]

Wolf notes that "[i]t is indeed fair to say that FTC settlements are followed like cases interpreting a statute would be followed."[184]

Indeed, this seems to be the precise intent of the FTC. Toby Levin, a senior attorney with the FTC from 1984 to 2005, states that "[t]he audience for consent orders is very broad—every similarly situated company, whether in that market or engaging in a similar practice."[185] Levin further explains:

> Given its limited resources, the FTC intends for consent orders to send a clear message that the practices identified in the complaint violate the FTC Act. It may wait to bring additional cases involving the same practice to see if the order is receiving the national attention it intends. If not, it may bring additional actions or send "warning letters" to a number of companies engaged in the same practice, putting them on notice that the practice, if continued, will put the company at risk of an FTC action.[186]

According to Levin, "[T]he more responsible companies—the ones that rely on their reputation as industry leaders—will take steps to address the practices outlined in an FTC settlement."[187]

FTC settlements are thus like the common law because they are treated in practice like the common law. The orders are publicized with the intent that practitioners rely upon them, and practitioners do so. The FTC's intent is just part of the equation, for the common law effect of

---

182. E.g., Wendell Bartnick & Edward Holman, RockYou Agrees to FTC Settlement After Data Breach and Alleged COPPA Violations, Wilson Sonsini Goodrich & Rosati: Eye on Privacy (May 2012), http://www.wsgr.com/publications/PDFSearch/eye-on-privacy/May2012/#3 (on file with the *Columbia Law Review*).

183. Vladeck Interview, supra note 68.

184. Wolf Interview, supra note 92.

185. Email from Toby Levin, former Senior Att'y, FTC, to authors (Apr. 3, 2013) [hereinafter Levin Interview] (on file with the *Columbia Law Review*).

186. Id.

187. Id.

FTC settlements rests heavily upon how they are received by the companies they regulate and the community of practitioners that advises these companies.

Of course, settlements are not equal to judicial decisions. Unlike judicial decisions, where other stakeholders are able to be heard through amicus briefs, FTC settlements have no such process. FTC investigations of companies are often secret and only announced when the settlement has been issued. As Wolf observes, "Unlike in litigation, the adversarial process and . . . role of the tribunal is quite limited as companies frequently enter into consent orders to avoid publicity, and thus agree that there has been enough of a case made to settle (even though in litigation, they might be able to prove otherwise)."[188] Nevertheless, the FTC does have a comment period where other stakeholders can be heard before the settlements are finalized. Commissioners vote on settlement orders and often write concurring and dissenting statements to reflect their view on an action.[189] The Commission also sends direct letters to those who comment on the proposed orders addressing their concerns.[190] This is similar in effect to an appellate court's handling of particular issues in a case and the ability of interested parties to voice support and concern, and highlight various interests through amicus briefs.

Settlements need not be as binding on future cases as judicial decisions to reflect aspects of the common law. While there is no well-established doctrine of precedent for settlements, the FTC has been relatively consistent in its privacy jurisprudence. Although the FTC rarely explicitly cites settlement orders in later, separate settlement orders, Levin states that while she was at the FTC, "[i]n a new action, internal memoranda accompanying proposed pleadings would typically cite to the Bureau and the Commission prior complaints or consent orders as precedent for bringing the action against a proposed respondent."[191] The FTC has

---

188. Wolf Interview, supra note 92.

189. E.g., United States v. Google Inc., No. CV 12-04177 SI, at 1 (N.D. Cal. Nov. 6, 2012) (statement of the Commission), available at http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlestatement.pdf (on file with the *Columbia Law Review*); id. (Rosch, Comm'r, dissenting), available at http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googleroschstatement.pdf (on file with the *Columbia Law Review*) (arguing consent decree cannot be in public interest when it contains denial of liability); In re GeoCities, Inc., 127 F.T.C. 94, 133 (1999) (decision & order) (Swindle, Comm'r, concurring), available at http://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015swindlestatement.htm (on file with the *Columbia Law Review*) (emphasizing order remedying violations in particular case does not mean violations should necessarily be found with other commercial internet sites).

190. See, e.g., Equifax Information Services LL [sic], FTC, http://ftc.gov/os/caselist/1023252/index.shtm (on file with the *Columbia Law Review*) (last updated Mar. 15, 2013) (providing links to letters).

191. Levin Interview, supra note 185 ("We generally looked at prior complaints and consent orders as guides to drafting pleadings in new cases.").

referenced previous consent orders in statements that accompany final orders. For example, in a letter to commenter Sidley Austin, LLP as part of *In re Sears Holdings Management Corp.*, the FTC referenced two prior consent orders that were similar to the current one to demonstrate consistency.[192] Indeed, the FTC settlements are rarely inconsistent with each other. There have been hardly any noted instances of inconsistency, despite a sizeable number of practitioner commentators who have analyzed FTC cases.

Precedent is largely a practice that is held together by custom and norms. Of course, appellate courts can reverse lower courts, and this prospect serves to reinforce precedent. The FTC settlements do not appear to be any less consistent than bodies of case law. According to Joel Winston, who served as associate director for DPIP from 2000 to 2011 and whose career at the FTC spanned more than thirty years, although "[a]s a general matter, the Commission doesn't cite consents as legal precedent in formal adjudicatory proceedings," the FTC and its staff "often blur the lines between consents and adjudicated orders in citing cases as precedent. This may come up in consent negotiations, speeches, and other informal communications."[193]

Winston notes that consent decrees are often "designed" to "have a huge impact on other businesses in the same industry or that use similar practices" because the FTC "must be strategic in bringing its cases, since it doesn't have the resources to pursue more than a relatively small fraction of law violators."[194] Thus, "the cases are designed to send a message to others similarly situated."[195]

Winston notes that in his current role as a privacy lawyer in private practice, he has been "surprised at how intense the level of scrutiny is both by the business community and the private bar."[196] He goes on to observe:

> They seem to analyze literally every word of the complaint and order in search of hidden messages; in particular many of the law firms with FTC practices put out client alerts whenever the FTC issues a settlement that include highly detailed analyses of the pleadings and predictions on what they might portend for the future.[197]

In some ways, settlements might have good features that judicial decisions lack. A settlement is mutually agreed upon by both the FTC and the defendant, so it represents a workable compromise. Judicial decisions

---

192. Letter from Donald S. Clark, Sec'y, FTC, to Alan Charles Raul, Sidley Austin, LLP (Aug. 31, 2009), available at http://www.ftc.gov/sites/default/files/documents/cases/2009/09/090909searsletteraustin.pdf (on file with the *Columbia Law Review*).

193. Winston Interview, supra note 180.

194. Id.

195. Id.

196. Id.

197. Id.

need not reach this compromise point. The benefit of reaching a compromise is that the doctrines emerging from these compromises are likely to be workable for at least several key stakeholders, whereas there is no such guarantee with judicial decisions, which can be entirely unworkable or unsatisfactory to any stakeholder.

On the other hand, the company brokering the compromise might not be representative of all stakeholders or even of a majority of stakeholders. The compromise might be workable for that company and others of a similar size and structure, but might not be as workable for other companies. In fact, there is a risk that the FTC could bully small companies with limited resources in order to collaterally attack larger organizations through the consent decree process. While this risk is present, the fact that the FTC has pursued the largest and most popular players in the internet space suggests that the agency has not behaved in this manner.[198]

Regardless of the desirability of a body of doctrines crafted from settlements, this is the body of doctrine that exists in the domain of privacy regulation, and in practice it functions similarly to common law.

The doctrines in the FTC settlements should be studied like a body of common law as adaptive, iterative, and increasingly determinative. Doing so demonstrates that there is order to what might appear chaotic. It shows that there is predictability and clear doctrinal development in this body of regulation. Viewing the FTC settlements as a common law evolutionary process also provides a perspective in the debate over how specific FTC privacy jurisprudence must be. As will be discussed below, standards that might have initially seemed vague are becoming more specific over time.

2. *FTC Reports and Materials.* — In addition to settlement agreements, the FTC has created a form of "soft law"[199] that consists of guidelines, press releases, workshops, and white papers.[200] In the past two years

198. For example, the FTC has brought actions against LinkedIn, Google, Facebook, and Microsoft. See supra note 48 (listing LinkedIn federal actions); supra notes 86–87 and accompanying text (discussing record $22.5 million fine in Google case); infra notes 247–249 and accompanying text (addressing litigation around Facebook's deceptive privacy promises); infra notes 260–261 (describing Microsoft's misrepresented security measures).

199. See, e.g., David M. Trubek & Louise G. Trubek, Hard and Soft Law in the Construction of Social Europe: The Role of the Open Method of Coordination, 11 Eur. L.J. 343, 344 (2005) (describing sanctions and uniform rules as distinguishing factors between hard and soft law); Louise G. Trubek, New Governance and Soft Law in Health Care Reform, 3 Ind. Health L. Rev. 139, 149 (2006) (identifying "soft law" as "informal processes to resolve grievances and disputes, including negotiation and multistepped procedures" and "hard law" as characterized by "command and control, court based dispute resolution, uniform rules, punitive sanctions, and court challenges for noncompliance").

200. The FTC's repository of reports and materials is accessible online. Commission and Staff Reports, FTC, http://www.ftc.gov/policy/reports/policy-reports/commission-and-staff-reports (on file with the *Columbia Law Review*) (last visited Feb. 7, 2014); see also

alone, the FTC has issued reports on the proper use of facial recognition technologies,[201] privacy disclosures on mobile applications,[202] mobile applications for children,[203] and a sweeping report entitled *Protecting Consumer Privacy in an Era of Rapid Change*, which summarizes the FTC's current and future approach to privacy regulation centered on privacy by design, simplified choice for businesses and consumers, and greater transparency.[204]

These materials are purportedly offered by the FTC as guides, yet the FTC has never clearly articulated which parts of its recommendations are mandatory and which parts are simply best practices. Many have criticized this lack of clarity because they feel compelled to be overly cautious to avoid running afoul of opaquely defined boundaries.[205]

Nevertheless, because these materials serve to illuminate the FTC's philosophy and approach, as well as its interpretation of Section 5, these materials have weight. They may not be exactly akin to advisory opinions, but they can come quite close. Companies take the guidance in these materials seriously. In some cases, statements in these materials can become almost like rules.

Perhaps the best analogue to this soft law is dicta in judicial opinions. The FTC materials do not have the same force and effect of a settlement; they are merely statements by the FTC about how it interprets its regulatory authority and Section 5, and how it might choose to enforce in the future. The FTC might change course or not enforce in that manner. The FTC might attempt an enforcement but be challenged by a company in court. Thus, FTC materials do not appear to be as strongly precedential as settlements, but they create incentives for companies to comply, and thus serve as a softer kind of rule.

Vladeck, former director of the Bureau of Consumer Protection, said that there is a key difference between the best practices the FTC

Bamberger & Mulligan, supra note 83, at 313 (describing FTC's use of "soft law techniques to flesh out the meaning" of its substantive rules).

201. FTC, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies (2012), available at http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf (on file with the *Columbia Law Review*).

202. FTC, Mobile Privacy Disclosures: Building Trust Through Transparency (2013), available at http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (on file with the *Columbia Law Review*).

203. FTC, Mobile Apps for Kids: Disclosures Still Not Making the Grade (2012), available at http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf (on file with the *Columbia Law Review*).

204. FTC, Protecting Consumer Privacy, supra note 78.

205. See, e.g., Stegmaier & Bartnick, Psychics, supra note 9, at 719 (calling lack of clarity "Russian Roulette" where companies essentially operate under strict liability framework).

proposes for guidance purposes and the standards it uses "to measure unreasonableness or unfairness in enforcement cases."[206] For the cases it brings, the FTC "look[s] at the company's conduct and see[s] to what extent it measures up to industry standards writ large."[207] When determining best practices for guidance purposes, the FTC arrives at these "through deep and ongoing engagement with all stakeholders, and reference to the statutes the agency enforces."[208]

III. JURISPRUDENCE OF THE NEW COMMON LAW OF PRIVACY

If the FTC's body of doctrines is akin to a body of common law, what does this law hold? And where is it heading?

FTC jurisprudence would not be noteworthy if it merely dealt with obvious broken promises in privacy policies or obvious violations of statutes. With regard to its Section 5 cases, the FTC could have readily stuck to enforcing the most clearly broken promises. But instead, the FTC has advanced doctrines that pushed far beyond this role and that have fleshed out substantive standards that go beyond privacy policies.

Would critics be correct to contend that the FTC has pushed too far? Would they be correct to contend that the FTC has become arbitrary and unpredictable in its enforcement? For example, in an amicus brief, the Chamber of Commerce and others have asserted that the "FTC's enforcement actions in fact harken back to past attempts to extend its authority beyond proper bounds."[209]

We contend that the FTC's privacy jurisprudence has developed along classic common law developmental patterns. These patterns are not arbitrary or surprising—they are quite predictable, almost inevitable. They are the byproduct of the consistent application of rules over time. We begin this Part with an overview of FTC privacy jurisprudence and then demonstrate the key patterns and trajectory of its development.

A. *An Overview of FTC Privacy Jurisprudence*

For the purposes of this discussion, we will divide FTC privacy jurisprudence into three broad areas: (1) deception, (2) unfairness, and (3) statutory and Safe Harbor enforcement. The FTC's jurisprudence in all

---

206. Vladeck Interview, supra note 68.

207. Id.

208. Id.

209. Brief of Chamber of Commerce of the United States of America et al. as Amici Curiae in Support of Defendants at 5, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX PGR (D. Ariz. Mar. 25, 2013); see also Advertising to Kids and the FTC: A Regulatory Retrospective that Advises the Present 5–11, available at http://www.ftc.gov/sites/default/files/documents/public_statements/advertising-kids-and-ftc-regulatory-retrospective-advises-present/040802adstokids.pdf (on file with the *Columbia Law Review*) (last visited Feb. 7, 2014) (describing historical regulatory attempts by FTC that were seen as overreaching).

three of these areas is more developed than what is reflected in the common narrative. The FTC has developed a theory of deception that not only includes broken promises of privacy and security, but also a general theory of deception in obtaining personal information and deception due to insufficient notice of privacy-invasive activities. The FTC's unfairness actions are based on at least five distinct theories: retroactive policy changes, deceitful data collection, improper use of data, unfair design, and unfair information security practices. There has also been a substantial statutory bleed onto Section 5 as the FTC pairs statutory violations with Section 5 violations for the same activity.

1. *Deception.* — The FTC's early privacy cases focused on the deception prong of the FTC's Section 5 authority. A deceptive trade practice is defined as a "misrepresentation, omission or other practice, that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment."[210] This definition can be broken down into three requirements: (1) an act (representation, omission, or practice), (2) the likelihood of a reasonable consumer's deception, and (3) materiality. The FTC primarily relies upon theories of deception when alleging privacy-related violations of Section 5.[211] According to the FTC:

> Practices that have been found . . . misleading or deceptive in specific cases include false oral or written representations, misleading price claims, sales of hazardous or systematically defective products or services without adequate disclosures, failure to disclose information regarding pyramid sales, use of bait and switch techniques, failure to perform promised services, and failure to meet warranty obligations.[212]

As this section demonstrates, although with respect to privacy the FTC initially focused on broken promises, it went on to develop a more holistic and robust theory of privacy-related deception. Today, the FTC considers the entirety of a company's dealings with the consumer, not just the specific promises made in the company's privacy policy.[213]

a. *Broken Promises of Privacy.* — Much of the FTC's privacy jurisprudence is based upon a deception theory of broken promises. Some of these promises are explicit and clear, such as when a company violates its

---

210. Letter from James C. Miller III to Hon. John D. Dingell, supra note 42, app. at 183.

211. Of the 154 privacy-related complaints analyzed for this Article, eighty-seven unambiguously relied upon a theory of deception in alleging a violation of Section 5, whereas there were only forty-six complaints that unambiguously relied upon a theory of unfairness in alleging a violation of Section 5. See FTC, Legal Resources, supra note 64 (listing recent FTC cases related to privacy and security).

212. Letter from James C. Miller III to Hon. John D. Dingell, supra note 42, app. at 175.

213. See id. app. at 178 ("[T]he Commission considers the totality of the practice in determining how reasonable consumers are likely to respond."); see also Hofmann, supra note 1, at 4:1.2 ("The FTC evaluates the entire transaction or course of dealing to determine whether a business's conduct was deceptive.").

own privacy policy, so the determination of a violation requires little interpretation. The types of broken promises cases include:

- Promises to maintain confidentiality or to refrain from disclosing information to third parties;[214]
- Promises to only collect data consistent with the company's privacy policy;[215]
- Promises to provide adequate security for personal data;[216]
- Promises to maintain anonymity;[217] and
- Promises not to disclose personal data to third parties by selling in bankruptcy proceedings.[218]

While many of the broken promises of privacy occurred within the privacy policy, the FTC also looked to implied promises elsewhere on the website. For example, in *In re Google Inc.*, the FTC alleged that not respecting previously established privacy settings such as "blocked" emails and visibility settings constituted a deceptive act based on an implicit promise those settings would be respected.[219] In *In re Stanton*, the FTC found that a company acted deceptively by representing that it had

---

214. E.g., In re Eli Lilly & Co., 133 F.T.C. 763 (2002) (complaint) (charging company with breaking privacy agreement by disclosing customers' personal information).

215. E.g., Complaint at 2, In re HTC Am. Inc., FTC File No. 122 3049, No. C-4406 (F.T.C. June 25, 2013) [hereinafter HTC Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf (on file with the *Columbia Law Review*) (charging company with failing to mitigate security vulnerabilities when providing third parties with sensitive information); In re Microsoft Corp., 134 F.T.C. 709, 715 (2002) (complaint) (charging company with collecting information beyond that provided for in privacy policy).

216. E.g., Complaint at 2, In re Genica Corp., FTC File No. 082 3113, No. C-4252 (F.T.C. Mar. 16, 2009) [hereinafter Genica Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2009/03/090320genicacmpt.pdf (on file with the *Columbia Law Review*); *Microsoft*, 134 F.T.C. at 711–12.

217. E.g., Complaint at 3, 6, In re Compete, Inc., FTC File No. 102 3155, No. C-4384 (F.T.C. Feb. 20, 2013) [hereinafter Compete Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competecmpt.pdf (on file with the *Columbia Law Review*) (charging company with failing to strip personal information before transmission of data to servers).

218. E.g., Toysmart.com Complaint, supra note 27, at 2–3 (describing privacy policy not to disclose personal information to third parties); see also In re Toysmart.com, FTC File No. X00 0075, No. 00-11341 RGS (F.T.C. July 21, 2000) (Swindle, Comm'r, dissenting), available at http://www.ftc.gov/sites/default/files/documents/cases/toysmartswindlestatement_0.htm (on file with the *Columbia Law Review*) ("Toysmart promised its customers that their personal information would *never* be sold to a third party, but the Bankruptcy Order in fact would allow a sale to a third party. In my view, such a sale should not be permitted because 'never' really means never.").

219. Complaint at 4, In re Google Inc., FTC File No. 102 3136, No. C-4336 (F.T.C. Oct. 13, 2011) [hereinafter Google Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf (on file with the *Columbia Law Review*).

taken steps to review the privacy practices of those displaying the company's "privacy seals."[220]

With respect to promises of privacy and security, it is important to note that the FTC does not seem to consider all data breaches, in and of themselves, indicative of broken promises. Rather, the FTC usually faults companies for failures to implement promised procedural protections, such as security protocols and adequate employee training.

For example, in *In re Eli Lilly & Co.*, the defendant violated its privacy policy when it sent out an email to 669 people that "unintentionally disclosed personal information provided to it by consumers in connection with their use of the Prozac.com Web site."[221] The FTC alleged that this disclosure was caused by Eli Lilly's "failure to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information."[222] The FTC alleged that Eli Lilly failed to adequately train its employees regarding consumer privacy and information security; failed to properly oversee and assist the employee who sent out the email "who had no prior experience in creating, testing, or implementing the computer program used;" and failed to have proper procedures to check and control the communications process, "such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the email."[223] The FTC also alleged that Eli Lilly's "failure to implement appropriate measures also violated certain of its own written policies."[224]

b. *General Deception.* — Not all deceptive acts involve a company breaching a promise of privacy. The FTC has also developed a general theory of deception in its complaints based upon a company's deceptive actions taken in order to induce disclosure of personal information. In *FTC v. ReverseAuction.com*, the company ReverseAuction.com was accused of using customer information obtained from eBay to send a deceptive email to eBay users falsely informing them their user ID was about to expire and directing users to ReverseAuction.com.[225] This practice was in violation of eBay's terms of use, which ReverseAuction.com agreed to when it registered as an eBay user. The FTC alleged that the company's misrepresentations regarding how it received customer information from

---

220. Complaint at 4–5, In re Stanton, FTC File No. 072 3165, No. C-4287 (F.T.C. Apr. 5, 2010) (on file with the *Columbia Law Review*).

221. In re Eli Lilly & Co., 133 F.T.C. 763, 767 (2002) (complaint).

222. Id.

223. Id. at 790.

224. Id.

225. Complaint for Permanent Injunction and Other Equitable Relief ¶ 8, FTC v. ReverseAuction.com, No. 00-CV-00032 (D.D.C. Jan. 6, 2000) [hereinafter ReverseAuction.com Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2000/01/www.ftc_.gov-reversecmp.htm (on file with the *Columbia Law Review*).

eBay and the expiration of users' IDs constituted a deceptive trade practice.[226]

The FTC has charged a number of companies with deceptive trade practices for inducing the downloading of spyware through misrepresentations and creating a deceitful software "registration" page to obtain certain information.[227] The deception in these cases stemmed from the fact that only some types of surveillance were disclosed rather than all types.[228] The FTC's theory in these cases was deception by omission.[229]

It is worth noting that if the deception used to induce disclosure of confidential information is egregious enough, the FTC considers the practice unfair. Sometimes the unfairness claim is raised in lieu of deception, but other times it is brought in addition to the deception claim. For example, in *FTC v. Accusearch Inc.*, the FTC alleged that Accusearch "obtained and sold to third parties confidential customer proprietary net-

---

226. Id. ¶¶ 15–16.

227. A number of FTC actions have centered on the creation and use of fake registration spyware software called "Detective Mode." E.g., Complaint at 5, In re DesignerWare, LLC, FTC File No. 112 3151, No. C-4390 (F.T.C. Apr. 11, 2013) [hereinafter DesignerWare Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf (on file with the *Columbia Law Review*) (charging company that created and licensed "Detective Mode"). For examples of companies charged with using Detective Mode to improperly gather personal information on users, see Complaint at 2, In re Aspen Way Enters., Inc., FTC File No. 112 3151, No. C-4392 (F.T.C. Apr. 11, 2013) [hereinafter Aspen Way Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415aspenwaycmpt.pdf (on file with the *Columbia Law Review*); Complaint at 3, In re B. Stamper Enters., Inc., FTC File No. 112 3151, No. C-4393 (F.T.C. Apr. 11, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415bstampercmpt.pdf (on file with the *Columbia Law Review*); Complaint at 3, In re C.A.L.M. Ventures, Inc., FTC File No. 112 3151, No. C-4394 (F.T.C. Apr. 11, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415calmcmpt.pdf (on file with the *Columbia Law Review*); Complaint at 3, In re J.A.G. Rents, LLC, FTC File No. 112 3151, No. C-4395 (F.T.C. Apr. 11, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415jagcmpt.pdf (on file with the *Columbia Law Review*); Complaint at 3, In re Red Zone Inv. Grp., Inc., FTC File No. 112 3151, No. C-4396 (F.T.C. Apr. 11, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415redzonecmpt.pdf (on file with the *Columbia Law Review*); Complaint at 2, In re Watershed Dev. Corp., FTC File No. 112 3151, No. C-4398 (F.T.C. Apr. 11, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415watershedcmpt.pdf (on file with the *Columbia Law Review*); see also Compete Complaint, supra note 217, at 2–3 (charging company for improperly tracking customers' internet use).

228. See, e.g., Complaint at 2, In re Epic Marketplace, Inc., FTC File No. 112 3182, No. C-4389 (F.T.C. Mar. 13, 2013) [hereinafter Epic Marketplace Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2013/03/130315epicmarketplacecmpt.pdf (on file with the *Columbia Law Review*) (charging company for failing to disclose "history sniffing" practice).

229. For an explanation of a deceptive omission, see Letter from James C. Miller III to Hon. John D. Dingell, supra note 42, app. at 175 n.4 ("A misleading omission occurs when qualifying information necessary to prevent a practice, claim, representation, or reasonable expectation or belief from being misleading is not disclosed. Not all omissions are deceptive, even if providing the information would benefit consumers.").

work information without the knowledge or consent of the customer."[230] According to the FTC, Accusearch used "false pretenses, fraudulent statements, fraudulent or stolen documents or other misrepresentations, including posing as a customer of a telecommunications carrier, to induce officers, employees, or agents of telecommunications carriers to disclose confidential customer phone records."[231] The FTC settled with other companies for similar allegations of engaging in misrepresentation to induce the disclosure of personal information.[232]

In *FTC v. Sun Spectrum Communications Organization, Inc.*, the FTC alleged that Sun Spectrum induced people to disclose financial data by falsely representing or implying that Sun Spectrum was calling on behalf of a financial institution or credit card company.[233] According to the FTC, because "Defendants' acts or practices violate Section 521 of the GLB Act, 15 U.S.C. § 6821," the "Defendants' acts or practices are false and misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act."[234]

In *FTC v. Hill*, the FTC alleged two different kinds of general deception or "inducement" theories: "False Affiliation" and "False Claim of Need to Provide Information."[235] *Hill* involved a phishing scam where the

---

230. Complaint for Injunctive and Other Equitable Relief at 5, FTC v. Accusearch Inc., No. 06-CV-0105 (D. Wyo. Sept. 28, 2007) [hereinafter Accusearch Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501accusearchcomplaint.pdf (on file with the *Columbia Law Review*).

231. Id. at 4–5.

232. E.g., FTC v. Action Research Grp., Inc., No. 6:07-CV-00227-Orl-22UAM, at 3–6 (M.D. Fla. Mar. 18, 2008) (order & settlement), available at http://www.ftc.gov/sites/default/files/documents/cases/2008/05/080528fo.pdf (on file with the *Columbia Law Review*) (ordering company to cease deceptive practices and pay fines). Note that somewhat similar activity was alleged only to be "unfair" in other cases. E.g., Complaint for Injunction and Other Equitable Relief at 4–5, FTC v. CEO Grp., Inc., No. 06-CV-60602 (S.D. Fla. Nov. 2, 2007) [hereinafter CEO Grp. Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501ceogroup-cmplt.pdf (on file with the *Columbia Law Review*) (alleging fraudulent obtaining of confidential customer phone records was unfair, rather than deceptive, practice); Complaint for Injunctive and Other Equitable Relief at 5, FTC v. Info. Search, Inc., No. 1:06-CV-01099-AMD (D. Md. Feb. 22, 2007) [hereinafter Info. Search Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501informationsearch-cmplt.pdf (on file with the *Columbia Law Review*) (same); Complaint for Injunctive and Other Equitable Relief at 6, FTC v. Integrity Sec. & Investigation Servs., Inc., No. 2:06-CV-241 (E.D. Va. Oct. 3, 2006) [hereinafter Integrity Sec. & Investigation Servs. Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501-77investigcmplt.pdf (on file with the *Columbia Law Review*) (same).

233. Complaint for Permanent Injunction and Other Equitable Relief at 5–6, FTC v. Sun Spectrum Commc'ns Org., Inc., No. 03-CV-8110 (S.D. Fla. Oct. 3, 2005) [hereinafter Sun Spectrum Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2004/01/031202cmp0323032.pdf (on file with the *Columbia Law Review*).

234. Id. at 10–11.

235. Complaint for Permanent Injunction and Other Equitable Relief at 10–11, FTC v. Hill, No. 03-5537 (S.D. Tex. Mar. 22, 2004) [hereinafter Hill Complaint], available at

defendant created fake websites that masqueraded as websites of popular institutions to trick people into disclosing login credentials and credit card information. Similar allegations of phishing were brought against a minor in *FTC v. [a Minor]*. There, the FTC also alleged theories of false affiliation and misrepresentations in spam emails regarding the need to provide information.[236]

The FTC also views the act of "pretexting" to be a generally deceptive practice used to obtain personal information. According to the FTC, pretexting involves "making various misleading and false statements to financial institutions and others. Such tactics include calling financial institutions and pretending to be the account holder, thereby inducing the financial institution to disclose private financial information," and, upon obtaining this private information, selling it.[237] GLBA is in harmony with the FTC's prohibition on pretexting by using a false identity or affiliation to induce the disclosure of personal information, which is a deceptive act.[238] For example, in *FTC v. Assail, Inc.*, the FTC alleged that the defendants violated section 521 of GLBA by inducing consumers to divulge their personal information by misrepresenting their affiliation with a bank and claiming to be merely "verifying" information.[239] Similar activity was alleged to be independently deceptive in *FTC v. Corporate Marketing Solutions, Inc.*, *FTC v. Hill*, and other such cases.[240]

---

http://www.ftc.gov/sites/default/files/documents/cases/2004/03/040322cmp0323102.pdf (on file with the *Columbia Law Review*).

236. Complaint for Permanent Injunction and Other Equitable Relief at 6–9, FTC v. [a Minor], No. 03-CV-5275 (C.D. Cal. July 23, 2003), available at http://www.ftc.gov/sites/default/files/documents/cases/2003/07/phishingcomp.pdf (on file with the *Columbia Law Review)*.

237. Complaint for Injunction and Other Equitable Relief, FTC v. Rapp, No. 99-WM-783 (D. Colo. Apr. 21, 1999), available at http://www.ftc.gov/sites/default/files/documents/cases/1999/04/ftc.gov-touchtonecomplaint.htm (on file with the *Columbia Law Review*).

238. See, e.g., Touch Tone Info., Inc., FTC File No. 982 3619, No. 99-WM-783 (D. Colo. June 27, 2000) (Swindle, Comm'r, dissenting), available at http://www.ftc.gov/sites/default/files/documents/cases/2000/06/ftc.gov-touchtoneswindle.htm (on file with the *Columbia Law Review*) (discussing consistency between GLBA and FTC personal information rule). For other Commissioners' statements in this case, see Rapp, James J. and Regana L. Rapp d/b/a Touch Tone Info., Inc., FTC, http://www.ftc.gov/os/caselist/jamesrapp.shtm (on file with the *Columbia Law Review*) (last updated June 27, 2000) (providing links to statements relating to Rapp/Touch Tone case).

239. Complaint for Injunctive and Other Equitable Relief at 22–23, FTC v. Assail, Inc., No. W03CA007 (W.D. Tex. Nov. 23, 2004), available at http://www.ftc.gov/sites/default/files/documents/cases/2003/01/assailcmp.pdf (on file with the C*olumbia Law Review*); see also Complaint for Permanent Injunction and Other Equitable Relief at 4–7, FTC v. GM Funding, Inc., No. 02-1026 DOC (MLGx) (C.D. Cal. Nov. 20, 2003) [hereinafter GM Funding Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2002/11/gmfundingcmp.pdf (on file with the *Columbia Law Review)* (alleging acts of misrepresentation).

240. Hill Complaint, supra note 235, at 12–13 (alleging deceptive pretexting of financial information); Corporate Mktg. Solutions Complaint, supra note 120, at 15–16

c. *Insufficient Notice.* — One of the most central aspects of the FTC's privacy jurisprudence is a reliance on "notice and choice."[241] A large part of managing privacy in the United States is providing people with adequate notice about the data collected and used about them and with a choice regarding certain forms of data collection or use. Thus, it is unsurprising that one of the most important features of the FTC's deceptiveness jurisprudence deals with insufficient notice to consumers.[242]

In *In re Sears Holdings Management Corp.*, Sears disseminated a software program that, "when installed, runs in the background at all times on consumers' computers and transmits tracked information, including nearly all of the Internet behavior that occurs on those computers, to servers maintained on behalf of [Sears]."[243] According to the FTC, "Information collected and transmitted include[d]: web browsing, filling shopping baskets, transacting business during secure sessions, completing online application forms, checking online accounts, and, through select header information, use of web-based email and instant messaging services."[244] Although Sears disclosed the tracking in a long licensing agreement, the FTC charged that Sears's disclosure was inadequate and hence deceptive. Specifically, Sears disclosed that the application would track users' "online browsing," but the FTC alleged that, in fact, the application tracked secure online browsing sessions and some computer activi-

---

(enumerating reasons for "deceptive acts" allegation); First Amended Complaint for Injunctive and Other Equitable Relief at 6–7, FTC v. Garrett, No. H-01-1255 (S.D. Tex. Mar. 8, 2002) [hereinafter Garrett Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2002/03/discreetdatacmplnt.pdf (on file with the *Columbia Law Review*) (detailing misrepresentation of privacy measures); Complaint for Injunctive and Other Equitable Relief at 5–6, FTC v. Guzzetta, No. 01-2335(DGT) (E.D.N.Y. Feb. 22, 2002) [hereinafter Guzzetta Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2001/04/pretextingsmartdatacomplaint.pdf (on file with the *Columbia Law Review*) (alleging defendant's false representations); In re Eli Lilly & Co., 133 F.T.C. 763, 764–68 (2002) (complaint) (outlining defendant's alleged misrepresentations for purpose of fraudulently obtaining private information).

241. See, e.g., Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880, 1883–84 (2013) [hereinafter, Solove, Privacy Self-Management] (discussing widespread embrace of notice-and-choice model in United States). But see FTC, Protecting Consumer Privacy, supra note 78, at 2 (referencing shortcomings of notice-and-choice model); Jon Leibowitz, Chairman, FTC, Introductory Remarks at the FTC Privacy Roundtable 3 (Dec. 7, 2009), available at http://www.ftc.gov/sites/default/files/documents/public_statements/introductory-remarks-ftc-privacy-roundtable/091207privacyremarks.pdf (on file with the *Columbia Law Review*) ("We do feel that the approaches we've tried so far—both the notice and choice regime, and later the harm-based approach—haven't worked quite as well as we would like.").

242. See, e.g., In re H&R Block, Inc., 80 F.T.C. 304, 304–09 (1972) (complaint) (discussing notice-related reasons for FTC violation).

243. Complaint at 1, In re Sears Holdings Mgmt. Corp., FTC File No. 082 3099, No. C-4264 (F.T.C. Aug. 31, 2009) [hereinafter Sears Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf (on file with the *Columbia Law Review*).

244. Id. at 1–2.

ties unrelated to the Internet.[245] Susan Gindin has noted that "the Sears Action is a reminder that the FTC will require enhanced notice particularly in regard to the collection and use of 'sensitive' personal information."[246] The consent order is also a clear signal that vague language tucked away in dense boilerplate agreements might not always be an effective method of notice to consumers.

In *In re Facebook, Inc.*, in addition to alleging deceptive promises of privacy inherent in Facebook's privacy settings, the FTC argued that Facebook failed to properly notify users of privacy-related changes in the website.[247] Facebook used a multi-page notice system called a "Privacy Wizard" to notify its users of the changes. The Privacy Wizard consisted of an introductory page, "privacy update pages, which required . . . users to choose, via a series of radio buttons, between new privacy settings that Facebook 'recommended' and the user's 'Old Settings,' for ten types of profile information," and "a confirmation page, which summarized the user's updated Privacy Settings."[248] According to the FTC, the Privacy Wizard failed to disclose the fact that users could no longer limit the visibility of certain parts of their profile to some third parties. The FTC deemed this to be a deceptive trade practice.[249]

In *FTC v. Frostwire, LLC*, the FTC alleged the company misrepresented its privacy practices in its user interface and, in a separate count, found that it failed to notify consumers adequately regarding how its file-sharing software operated, including the fact that downloaded files were shared publicly by default as well as the fact that the software "would publicly share files that consumers previously downloaded from the Gnutella network and stored in 'unshared' folders even after consumers deselected the Share Finished Downloads setting in the Options-Sharing dialog box."[250]

In *FTC v. Echometrix, Inc.*, the FTC alleged that the broad statement contained in the defendant's privacy policy—"[Sentry] uses information

---

245. Id. at 5.

246. Susan E. Gindin, Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears, 8 Nw. J. Tech. & Intell. Prop. 1, 5 (2009).

247. Complaint at 7–9, In re Facebook, Inc., FTC File No. 092 3184, No. C-4365 (F.T.C. July 27, 2012) [hereinafter Facebook Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf (on file with the *Columbia Law Review*).

248. Id. at 7–8.

249. Id. at 9 ("Facebook failed to disclose . . . adequately, that, following the . . . Privacy Changes, users could no longer restrict access to their [personal information] by using privacy settings previously available to them. Facebook also failed to disclose . . . adequately[] that the . . . Privacy Changes overrode existing user privacy settings . . . .").

250. Complaint for Permanent Injunction and Other Equitable Relief at 19, FTC v. Frostwire, LLC, No. 1:11-cv-23643 (S.D. Fla. Oct. 12, 2011) [hereinafter Frostwire Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf (on file with the *Columbia Law Review*).

for the following general purposes: to customize the advertising and content you see[,] . . . improve our services[,] . . . conduct research, and provide anonymous reporting for internal and external clients"—was too vague to adequately disclose that information monitored and collected by the defendant's computer-monitoring software program would be shared with third parties.[251] Thus, according to the FTC, the purchasers of the defendant's computer monitoring software "were unaware that their children's computer activity, obtained in connection with the operation of Sentry, w[as] fed into a database being promoted to marketers."[252]

In *In re Sony BMG Music Entertainment*, the FTC alleged that Sony BMG failed to provide notice to consumers that its software package on defendant's CD would transmit to Sony the albums consumers were playing. The software would retrieve from Sony images and promotional messages to display on consumers' computers.[253] According to the FTC, this insufficient notice constituted a deceptive practice.[254]

d. *Data Security*. — Data security is often a case of broken promises, but it has developed into something more over the years.[255] Even vague promises of security such as providing "reasonable security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of personal information" can be the basis of an FTC action.[256] The FTC has come to rely on industry standards and other norms to identify a particular set of practices that, taken together, constitute adequate security practices for companies collecting personal information.

When the FTC first began to tackle privacy issues, it only dabbled in data security under a theory of deception. One of the first security-related complaints brought by the FTC was *FTC v. Rennert*, in which the FTC accused an online pharmacy of falsely representing "to consumers, expressly or by implication, that the information customers provide to their Web sites is encrypted and that defendants use an SSL secure con-

---

251. Complaint for Permanent Injunction and Other Equitable Relief at 3–4, FTC v. Echometrix, Inc., No. CV10-5516 (E.D.N.Y. Nov. 30, 2010), available at http://www.ftc.gov/sites/default/files/documents/cases/2010/11/101130echometrixcmpt.pdf (on file with the *Columbia Law Review*).

252. Id. at 4.

253. Complaint at 4, In re Sony BMG Music Entm't, FTC File No. 062 3019, No. C-4195 (F.T.C. June 28, 2007) [hereinafter Sony BMG Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2007/01/070130cmp0623019.pdf (on file with the *Columbia Law Review*).

254. Id.

255. See, e.g., infra Part III.A.2, B.3 (showing FTC increasingly both pleads unfairness and develops substantive baseline standards).

256. Compete Complaint, supra note 217, at 4, 6 ("[R]espondent has represented . . . that it employs reasonable and appropriate measures to protect data obtained from consumers from unauthorized access. In truth and in fact . . . respondent did not [do so]. Therefore, the representation . . . was, and is, false or misleading . . . .").

nection when transmitting this information over the Internet."[257] In another early action, the previously referenced *In re Eli Lilly & Co.* case, the FTC charged Eli Lilly with failing to honor a promise of having "security measures in place, including the use of industry standard secure socket layer encryption (SSL), to protect the confidentiality of any of Your Information that you volunteer . . . ."[258] The FTC alleged that Eli Lilly did not implement proper security safeguards.[259]

In the early 2000s, the FTC initiated a flurry of activity around security—nearly overshadowing its privacy cases.[260] One of the most prominent actions was *In re Microsoft Corp.*, where the FTC alleged that Microsoft falsely represented "that it maintained a high level of online security by employing sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers in connection with the Passport and Passport Wallet services."[261]

---

257. Complaint for Permanent Injunction and Other Equitable Relief ¶ 43, FTC v. Rennert, No. CV-S-00-0861-JBR (D. Nev. July 12, 2000), available at http://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogcomp.htm (on file with the *Columbia Law Review*).

258. In re Eli Lilly & Co., 133 F.T.C. 763, 765 (2002) (complaint).

259. Id. at 767 ("For example, respondent failed to provide appropriate training for its employees regarding consumer privacy and information security . . . and failed to implement appropriate checks and controls on the process . . . . Respondent's failure to implement appropriate measures also violated certain of its own written policies.").

260. E.g., Genica Complaint, supra note 216, at 2–3 ("In truth and in fact, respondents did not implement reasonable and appropriate measures to protect consumer information against unauthorized access."); Complaint at 2–3, In re Life Is Good, Inc., FTC File No. 072 3046, No. C-4218 (F.T.C. Apr. 16, 2008) [hereinafter Life Is Good Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2008/04/080418complaint.pdf (on file with the *Columbia Law Review*); Complaint at 2–3, In re Guidance Software, Inc., FTC File No. 062 3057, No. C-4187 (F.T.C. Mar. 30, 2007) [hereinafter Guidance Software Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2007/04/0623057complaint.pdf (on file with the *Columbia Law Review*) ("[R]espondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive personal information stored on its corporate network."); In re Petco Animal Supplies, Inc., 139 F.T.C. 102, 104–05 (2005) (complaint) (alleging defendant did not provide appropriate security); In re MTS, Inc., 137 F.T.C. 444, 448 (2004) (complaint) (same); In re Guess?, Inc., 136 F.T.C. 507, 510–11 (2003) (complaint) ("Since at least October 2000, Respondents' application and website have been vulnerable to commonly known or reasonably foreseeable attacks from third parties attempting to obtain access to customer information stored in Respondents' databases."); In re Microsoft Corp., 134 F.T.C. 709, 712 (2002) (complaint) ("[R]espondent did not maintain a high level of online security by employing sufficient measures reasonable and appropriate under the circumstances . . . .").

261. *Microsoft*, 134 F.T.C. at 711 (noting company represented both "[y]our .NET Passport is protected by powerful online security technology and a strict privacy policy" and "[y]our .NET Passport information is stored on secure .NET Passport servers that are protected in controlled facilities" (emphasis omitted)).

Over time, in its security jurisprudence, the FTC began to include allegations of unfair practices along with claims of deception.[262] One of the most recent examples, *FTC v. Wyndham Worldwide Corp.*,[263] is currently awaiting a judicial decision and is discussed below.

2. *Unfairness.* — In many ways, the FTC's unfairness jurisdiction is quite limited.[264] An "unfair" trade practice is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[265] This test, which has been codified in section 5(n) of the FTC Act,[266] has come to be known as the "three-part test."[267]

The FTC has exercised its unfairness enforcement power judiciously when it comes to privacy and security. Early on, the FTC exercised its unfairness authority quite cautiously and much less frequently than its deception authority. According to Stephen Calkins, writing in the year 2000, "Recent years have seen a very tentative increased focus on consumer unfairness, changed in substantive emphasis and forum of application. In spite of the ease with which a complaint can recite the three-part test, the Commission has shied away from pleading it; but noteworthy exceptions are starting to occur."[268]

This trend of judicious yet increasing pleading of unfairness persists today. The FTC has stated that its understanding of the unfairness doctrine is the result of an "evolutionary process" that refines the standard

---

262. E.g., Complaint at 3, In re Ceridian Corp., FTC File No. 102 3160, No. C-4325 (F.T.C. June 8, 2011) [hereinafter Ceridian Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2011/06/110615ceridiancmpt.pdf (on file with the *Columbia Law Review*) (charging respondent with unfair practices); Complaint at 3, In re Rite Aid Corp., FTC File No. 072 3121, No. C-4308 (F.T.C. Nov. 12, 2010) [hereinafter Rite Aid Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2010/11/101122riteaidcmpt.pdf (on file with the *Columbia Law Review*) (same); Complaint at 3, In re CVS Caremark Corp., FTC File No. 072 3119, No. C-4259 (F.T.C. June 18, 2009) [hereinafter CVS Caremark Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvscmpt.pdf (on file with the *Columbia Law Review*) (same); In re BJ's Wholesale Club, Inc., 140 F.T.C. 465, 468 (2005) (complaint) (same).

263. Wyndham Complaint, supra note 122, at 5.

264. 15 U.S.C. § 45(n) (2012) (limiting severely FTC's authority to declare act or practice unlawful on unfairness grounds).

265. Id.

266. FTC Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (codified as amended at 15 U.S.C. § 45(n)).

267. The three parts are (1) substantial injury, (2) that is not reasonably avoidable, and (3) balancing with countervailing benefits. See, e.g., FTC v. Direct Mktg. Concepts, Inc., 569 F. Supp. 285, 299 (D. Mass. 2008) (describing three-part test to analyze unfair practices).

268. Stephen Calkins, FTC Unfairness: An Essay, 46 Wayne L. Rev. 1935, 1937 (2000).

over time through cases, rules, and Commission statements.[269] In evaluating whether a trade practice is unfair, the FTC focuses largely on substantial injury to consumers.[270] Monetary, health, and safety risks are common injuries considered "substantial," but trivial, speculative, emotional, and "other more subjective types of harm" are usually not considered substantial for unfairness purposes.[271] In determining whether an injury is outweighed by any countervailing benefits to consumers or competition, the FTC considers not only consumers' cost to remedy the alleged injury, but also the cost to society in general.[272] If consumers could have reasonably avoided the alleged injury, the FTC will not consider a trade practice unfair.[273] The FTC has stated that certain trade practices prevent consumers from effective decisionmaking. Indeed, "[m]ost of the Commission's unfairness matters are brought under these circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."[274]

In evaluating unfairness, the FTC also considers whether the trade practice violates established public policy "as it has been established by statute, common law, industry practice, or otherwise."[275] While this factor is usually used to help to determine whether a consumer injury is substantial, the FTC has stated that "[s]ometimes public policy will independently support a Commission action. This occurs when the policy is so clear that it will entirely determine the question of consumer injury, so there is little need for separate analysis by the Commission."[276] While nominally the FTC also considers whether a company's conduct was "immoral, unethical, oppressive, or unscrupulous," the FTC has stated this factor of unfairness is "largely duplicative. Conduct that is truly unethical or unscrupulous will almost always injure consumers or violate

---

269. FTC Policy Statement on Unfairness, supra note 56; see also 15 U.S.C. § 45(n) (authorizing FTC to "consider established public policies as evidence" when making fairness determinations); Hofmann, supra note 1, §§ 4:3 to :4 (articulating evolving nature of FTC's unfairness definition).

270. Hofmann, supra note 1, § 4:4 ("Unjustified consumer injury is the factor that carries the greatest weight in an unfairness analysis. In fact, if the injury to consumers is significant enough, it can be the sole basis for a finding of unfairness.").

271. FTC Policy Statement on Unfairness, supra note 56; see also Hofmann, supra note 1, § 4:4 (citing and discussing FTC's policy).

272. FTC Policy Statement on Unfairness, supra note 56. These societal costs exist "in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters." Id.; see also Hofmann, supra note 1, § 4:4 (discussing FTC's policy).

273. FTC Policy Statement on Unfairness, supra note 56.

274. Id.

275. Id.

276. Id.

public policy as well. The Commission has therefore never relied on [this element] as an independent basis for a finding of unfairness . . . ."[277]

Unfair conduct need not be a violation of any particular law.[278] In *FTC v. Accusearch Inc.*, the Tenth Circuit stated that "the FTCA enables the FTC to take action against unfair practices that have not yet been contemplated by more specific laws."[279] Of course, the FTC may look to other areas of the law in determining what activity is unfair.[280] For example, in *Accusearch*, the FTC looked to the Telecommunications Act, which restricted the disclosure of an individual's phone records,[281] to find that consumers had a reasonable expectation of privacy in their phone records for purposes of Section 5.[282] The FTC filed complaints against, and ultimately settled with, Action Research Group and Information Search on very similar theories.[283]

Although the FTC has yet to summarize its approach in a unified way, its actions reveal that distinct theories of what constitutes an unfair trade practice have emerged: (1) retroactive policy changes, (2) deceitful data collection, (3) improper use of data, (4) unfair design, and (5) unfair information security practices.

a. *Retroactive Changes.* — According to the FTC, it is unfair to change the terms that govern personal information that was collected under a previous, different agreement. In *In re Gateway Learning Corp.*, the company changed its privacy policy to allow the renting of personal data to third parties when previously it had promised that it would not do so.[284] Gateway did not inform customers about this change, despite the fact that it explicitly informed its users that "[i]f at some future time there is a

277. Id.

278. Indeed, the history of the FTC makes it clear that Congress wanted a kind of extrajudicial enforcement function, with the agency generating expertise in commerce. H.R. Rep. No. 63-1142, at 19 (1914) ("It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. . . . If Congress were to adopt the method of definition, it would undertake an endless task.").

279. FTC v. Accusearch Inc., 570 F.3d 1187, 1194 (10th Cir. 2009).

280. See, e.g., id. at 1195 ("[T]he FTC may proceed against unfair practices even if those practices violate some other statute that the FTC lacks authority to administer. Indeed, condemnation of a practice in criminal or civil statutes may well mark that practice as 'unfair.'" (citation omitted)).

281. 47 U.S.C. § 222(c)(1), (c)(2), (h)(l) (2006) (restricting usage and disclosure of "customer proprietary network information").

282. Accusearch Complaint, supra note 230, at 5.

283. See FTC v. Action Research Grp., Inc., No. 6:07-CV-0227-ORL-22JGG, at 1 (M.D. Fla. Mar. 18, 2008) (stipulated final order), available at http://www.ftc.gov/sites/default/files/documents/cases/2008/05/080528fo.pdf (on file with the *Columbia Law Review*) (settling charges of unauthorized access and sale of consumer records). In other cases, similar activity was alleged only to be "unfair." See CEO Grp. Complaint, supra note 232, at 5 (alleging defendant had engaged in "unfair" practices); Info. Search Complaint, supra note 232, at 5 (same); Integrity Sec. & Investigation Servs. Complaint, supra note 232, at 6 (same).

284. Gateway Decision & Order, supra note 85, at 443, 446.

material change to our information usage practices that affect [sic] your personally identifiable information, we will notify you of the relevant changes."[285] The FTC explicitly took issue with Gateway's application of new privacy practices to data collected under its older and different privacy policies.[286] The FTC deemed this retroactive privacy policy change to be an unfair practice. In addition to retroactive changes to policy, the FTC also considers retroactive changes to privacy settings to constitute an unfair practice, as in the *In re Facebook, Inc.* case.[287]

b. *Deceitful Data Collection*. — The FTC has also developed a theory that it is an unfair act to collect personal information in a deceitful manner. In *In re Aspen Way,* the FTC concluded that installing spyware and gathering data without notice was an unfair practice.[288] The FTC did not allege in its complaint that Aspen Way made any privacy-related promises, so use of the spyware presumably did not break a promise of privacy. But the FTC deemed the surreptitious data gathering unfair due to the substantial harm caused to consumers from such invasive surveillance and concerns that "[c]onsumers cannot reasonably avoid these injuries because [the surveillance] is invisible to them."[289] The FTC relied upon a similar theory of unfairness in a complaint against Sony BMG when it alleged that the company causing its spyware to be downloaded without sufficient notice was, by itself, an unfair practice.[290]

In *FTC v. Accusearch, Inc.*, the Tenth Circuit affirmed a summary judgment in favor of the FTC finding that deceitful data collection constituted an unfair trade practice.[291] According to the FTC, the "[d]efendants have used, or caused others to use, false pretenses, fraudulent statements, fraudulent or stolen documents or other misrepresentations, including posing as a customer of a telecommunications carrier, to induce officers, employees, or agents of telecommunications carriers to disclose confidential customer phone records."[292] The act of "pretexting"

---

285. Id. at 445.

286. Id. at 499 ("Respondent posted a revised privacy policy containing material changes to its practices that were inconsistent with Respondent's original promise to consumers. Respondent retroactively applied such changes to personal information it had previously collected from consumers.").

287. Facebook Complaint, supra note 247, at 9 ("[B]y designating certain user profile information publicly available that previously had been subject to privacy settings, Facebook materially changed its promises that users could keep such information private. Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent.").

288. Aspen Way Complaint, supra note 227, at 4.

289. Id. at 2.

290. Sony BMG Complaint, supra note 253, at 4.

291. 570 F.3d 1187, 1201 (10th Cir. 2009) (describing company's practice of soliciting requests for confidential information protected by law and paying researchers likely to use improper methods to find the information).

292. Accusearch Complaint, supra note 230, at 4–5.

is a good example of a practice of data collection that the FTC considers deceitful because the deceit is hidden from consumers.

c. *Improper Use of Data.* — In several cases, the FTC alleged that in addition to the wrongful collection of information, the subsequent misuse of that information was unfair. For example, in *In re Aspen Way Enterprises, Inc.*, the FTC alleged that "respondent has used information improperly gathered from consumers to collect or attempt to collect a debt, money, or property pursuant to a consumer rental contract."[293]

In *FTC v. Hill*, the FTC alleged that defendant used consumers' financial and credit card data to "pay for goods or services without the consumers' consent."[294] The FTC asserted that these actions were unfair. In *FTC v. ReverseAuction.com*, the FTC alleged that the collection of personal information in violation of eBay's terms of use and subsequent use of that information to send deceptive spam emails was an unfair practice.[295]

d. *Unfair Design or Unfair Default Settings.* — In several instances, the FTC has found the design of websites and software to be unfair. In *In re Sony BMG Music Entertainment*, digital rights management (DRM) software was installed on consumers' computers in such a way that consumers were unable to find or remove the software through reasonable effort.[296] If consumers attempted to remove the software, it would render their CD-ROM drive inoperable. The FTC deemed the software design to be unfair.[297]

Related to design are the default settings for data sharing, as these shape consumer behavior. In *FTC v. Frostwire, LLC*, the FTC alleged that failure to notify users that many preexisting files on consumer computers would be designated for public sharing constituted an unfair design.[298] Users who did not wish to share a large number of files had to go through the burdensome process of protecting the files one at a time by unchecking many prechecked boxes designating the files for sharing. The FTC noted that deceitful or obstructionist default settings constitute an unfair design feature.[299]

---

293. Aspen Way Complaint, supra note 227, at 4.

294. Hill Complaint, supra note 235, at 12.

295. ReverseAuction.com Complaint, supra note 225, ¶ 17.

296. The term DRM is generally used to refer to technological measures that allow digital content owners to control how their content is used. E.g., Julie E. Cohen, DRM and Privacy, 18 Berkeley Tech. L.J. 575, 575 (2003) ("In an effort to control the proliferation of unauthorized copies, and to maximize profit from information goods distributed over the Internet, copyright owners and their technology partners are designing digital rights management ('DRM') technologies that will allow more perfect control over access to and use of digital files.").

297. Sony BMG Complaint, supra note 253, at 4.

298. Frostwire Complaint, supra note 250, at 13.

299. Id. at 15–16, 19.

e. *Unfair Data Security Practices.* — As discussed earlier, when companies promise to keep data secure and fail to implement reasonable security safeguards, the FTC deems this a form of broken promise, and it is classified as a deceptive trade practice. What if no promises to safeguard data security are made? In *United States v. Rental Research Services, Inc.*, the FTC alleged that the "[d]efendants have not employed reasonable and appropriate measures to secure the personal information RRS collects for sale to its customers, including reasonable policies and procedures to (1) verify or authenticate the identities and qualifications of prospective subscribers; or (2) monitor or otherwise identify unauthorized subscriber activity."[300] Although there was no promise of security, the FTC deemed the defendants' lack of adequate security measures to be an unfair practice.

3. *Statutory and Safe Harbor Enforcement.* — The FTC also has brought a number of enforcement cases under its statutory authority pursuant to FCRA, COPPA, and GLBA, as well as under its Safe Harbor authority. Many of these cases are quite similar to the FTC's Section 5 cases because the statutes and Safe Harbor have similar requirements to the promises that companies routinely make in their privacy policies. Indeed, the statutes often reference Section 5 and deem a violation of statutory requirements an unfair or deceptive act or practice. In a way, this has resulted in a kind of statutory bleed-over into Section 5, as the same activity results in a dual violation with little indication as to which aspects of the conduct are solely attributable to statutory violations and which aspects of the company's actions are also deceptive or unfair.

For example, data security is a common provision in privacy policies, thus triggering Section 5, but data security also is a requirement in FCRA, GLBA, COPPA, and Safe Harbor. As Joel Winston, the former director of DPIP, observes, the "FTC strives for consistency in its treatment of practices that might violate different laws that it enforces to the extent possible."[301] He notes that "Section 5 often overlaps with the more specific statutes" and that "the Section 5 theory developed in data security cases—that companies that collect personally identifiable information (PII) must have reasonable procedures to protect it—borrows heavily from the GLBA Privacy Rule."[302]

The FTC's "double dipping," in which it considers activity violative of both a statute over which the FTC has jurisdiction and Section 5, is relatively common. For example, almost half of the complaints alleging violations of COPPA also contained an allegation of deceptive trade prac-

300. Complaint for Civil Penalties, Injunctive and Other Equitable Relief at 8, United States v. Rental Research Servs., Inc., FTC File No. 072 3228 (D. Minn. Mar. 5, 2009) [hereinafter Rental Research Servs. Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2009/03/090305rrscmpt.pdf (on file with the *Columbia Law Review*).

301. Winston Interview, supra note 180.

302. Id.

tices.[303] Almost all of the complaints alleging violations of GLBA also contained an allegation of deceptive or unfair trade practices.[304]

303. E.g., Complaint for Civil Penalties, Permanent Injunction, and Other Relief at 9–10, United States v. Path, Inc., No. C-13-0448 (N.D. Cal. Feb. 8, 2013) [hereinafter Path Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathinccmpt.pdf (on file with the *Columbia Law Review*) (alleging deceptive trade practices); Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 13, United States v. Artist Arena LLC, No. 12-CV-7386 (S.D.N.Y. Oct. 3, 2012) [hereinafter Artist Arena Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121003artistarenacmpt.pdf (on file with the *Columbia Law Review*) (same); Complaint for Civil Penalties, Permanent Injunction, and Other Relief at 9–10, United States v. RockYou, Inc., No. CV-12-1487 (N.D. Cal. Mar. 27, 2012) [hereinafter RockYou Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyoucmpt.pdf (on file with the *Columbia Law Review*) (same); Complaint for Civil Penalties, Injunctive, and Other Relief at 9, United States v. Godwin, No. 1:11-cv-03846-JOF (N.D. Ga. Feb. 1, 2012) [hereinafter Godwin Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2011/11/111108skidekidscmpt.pdf (on file with the *Columbia Law Review*) (same); Complaint for Civil Penalties, Injunction and Other Relief at 10, United States v. Playdom, Inc., No. SACV11-0724 (C.D. Cal. May 24, 2011) [hereinafter Playdom Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2011/05/110512playdomcmpt.pdf (on file with the *Columbia Law Review*) (same); Complaint for Civil Penalties, Injunction, and Other Relief at 8, United States v. Iconix Brand Grp., Inc., No. 09-CIV-8864 (S.D.N.Y. Nov. 5, 2009) [hereinafter Iconix Brand Grp. Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2009/10/091020iconixcomplecmpt.pdf (on file with the *Columbia Law Review*) (same); Sony BMG Complaint, supra note 253, at 4–5 (same); Complaint for Civil Penalties, Injunctive, and Other Relief at 6, United States v. Am. Pop Corn Co., No. C02-4008DEO (N.D. Iowa Feb. 14, 2002) [hereinafter American Pop Corn Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2002/02/popcorncmpnt.pdf (on file with the Col*umbia Law Review*) (same); Complaint for Civil Penalties, Injunctive, and Other Relief at 9, United States v. Lisa Frank, Inc., No. 01-1516-A (E.D. Va. Oct. 2, 2001) [hereinafter Lisa Frank Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2001/10/lfcmp.pdf (on file with the *Columbia Law Review*) (same); Complaint for Civil Penalties, Injunctive, and Other Relief at 10–11, United States v. Bigmailbox.com, Inc., No. 01-605-A (E.D. Va. Apr. 19, 2001) [hereinafter Bigmailbox.com Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2001/04/bigmailboxcmp.pdf (on file with the *Columbia Law Review*) (same); Toysmart.com Complaint, supra note 27, at 3 (same). It is not always clear if the FTC is alleging a violation of COPPA, a violation of Section 5, or both. For example, in *United States v. W3 Innovations, LLC*, the FTC initially alleged that a violation of the COPPA rule constitutes an unfair or deceptive trade practice, yet only appeared to bring one count of violating the COPPA rule against the defendant, rather than bringing both a COPPA and Section 5 claim. Complaint for Civil Penalties, Permanent Injunction, and Other Relief at 1–4, 7–8, *W3 Innovations*, No. CV11-03958 (N.D. Cal. Sept. 8, 2011), available at http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110815w3cmpt.pdf (on file with the *Columbia Law Review*); see also Complaint for Civil Penalties, Injunction, and Other Relief at 2–4, 7–8, United States v. Industrious Kid, Inc., No. CV 08 0639 (N.D. Cal. Jan. 30, 2008), available at http://www.ftc.gov/sites/default/files/documents/cases/2008/01/080730comp.pdf (on file with the *Columbia Law Review*); Complaint at 1–4, 8–9, United States v. Xanga.com, Inc., No. 06 CV 6853 (S.D.N.Y. Sep. 7, 2006), available at http://www.ftc.gov/sites/default/files/documents/cases/2006/09/xangacomplaint_image.pdf (on file with the *Columbia Law Review*) ("Pursuant to Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the [COPPA] Rule constitutes an unfair or deceptive act or practice . . . ."). Contrast

a. *FCRA*. — In many complaints, failure to provide the notice and disclosures required under FCRA also constituted either an unfair or deceptive trade practice.[305] Because these cases settled, it was often unclear under which theory the FTC was actually asserting its claims.

The FCRA's "disposal rule" seemed to guide the FTC's general approach to security. For example, in *FTC v. Navone* the FTC brought a claim against the defendant for failing to securely dispose of consumer information under the FCRA disposal rule, as well as a violation of section 5(a) as a deceptive promise of security.[306]

The FCRA's "prescreen rule" has strict requirements for short notices:

> [Notices must] appear on the front side of the first page of the principal promotional document in the solicitation, in a type style that is distinct from the principal type style used on the same page, and in a type size that is larger than the type size of the principal text on the same page, but in no event smaller than 12-point type.[307]

---

this with other FTC complaints where both the COPPA rule and Section 5 were alleged to have been violated. E.g., Playdom Complaint, supra, at 9–10 (alleging separate violations of COPPA and Section 5 independent of COPPA violation).

304. For examples of complaints also alleging deceptive or unfair trade practices, see, e.g., Complaint at 3, In re Franklin's Budget Car Sales, Inc., FTC File No. 102 3094, No. C-4371 (F.T.C. Oct. 3, 2012) [hereinafter Franklin's Budget Car Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026franklinautomallcmpt.pdf (on file with the *Columbia Law Review*); Complaint at 5, In re Premier Capital Lending, Inc., FTC File No. 072 3004, No. C-4241 (F.T.C. Dec. 10, 2008) [hereinafter Premier Capital Lending Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2008/12/081206pclcmpt.pdf (on file with the *Columbia Law Review*); Complaint at 4, Goal Fin., LLC, FTC File No. 072 3013, No. C-4216 (F.T.C. Apr. 9, 2008) [hereinafter In re Goal Fin. Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2008/04/080415complaint_0.pdf (on file with the *Columbia Law Review*); GM Funding Complaint, supra note 239, at 7–9; Complaint at 4, Nations Title Agency, Inc., FTC File No. 052 3117, No. C-4161 (F.T.C. June 19, 2006) [hereinafter Nations Title Agency Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2006/06/0523117nationstitle_complaint.pdf (on file with the *Columbia Law Review*); In re Superior Mortg. Corp., 140 F.T.C. 926, 930 (2005) (complaint); Sun Spectrum Complaint, supra note 233, at 6; Corporate Mktg. Solutions Complaint, supra note 120, at 13–14; Garrett Complaint, supra note 240, at 6; Guzzetta Complaint, supra note 240, at 6.

305. See, e.g., Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 5–6, United States v. Cent. Credit, LLC, No. 2:10-cv-00565 (D. Nev. Apr. 20, 2010), available at http://www.ftc.gov/sites/default/files/documents/cases/2010/04/100422centralcreditcmpt.pdf (on file with the *Columbia Law Review*) (asserting acts in violation of FCRA also constitute unfair or deceptive trade practices).

306. Complaint for Civil Penalties, Injunction, and Other Equitable Relief at 6–8, FTC v. Navone, No. 2:08-cv-01842 (D. Nev. Dec. 20, 2009), available at http://www.ftc.gov/sites/default/files/documents/cases/2009/01/090121navonecmpt.pdf (on file with the *Columbia Law Review*).

307. Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 4, United States v. Metro. Home Mortg., No. CV09-05873 JSL (RZx) (C.D. Cal.

This requirement was relied upon by the FTC to articulate very specific "notice" standards.[308]

Similarly, a company was alleged to have violated FCRA—and also to have engaged in "unfair or deceptive acts or practices" in violation of the FTC Act—for "obtaining information from a consumer reporting agency without having a permissible purpose for which the information was authorized to be furnished."[309] In several other cases, the FTC has charged both FCRA violations as well as FTC Act violations based on the same practice.[310]

It is unclear if the FTC would consider similar activity simply a violation of section 5(a) in other contexts or involving entities not covered by FCRA. No complaints brought by the FTC involve such similar activity, with the exception of using misrepresentations to induce disclosure of information.[311]

b. *COPPA*. — The Children's Online Privacy Protection Rule is the FTC's primary enforcement mechanism under COPPA.[312] According to the FTC, the rule "requires a subject website operator to meet specific requirements prior to collecting online, using, or disclosing personal information from children."[313] COPPA is broad, encompassing meaningful notice, transparency, and parental choice and consent requirements,

---

Oct. 10, 2009) (citing 16 C.F.R. § 642.3(a) (2013)), available at http://www.ftc.gov/sites/default/files/documents/cases/2009/08/090818metromortgagecmpt.pdf (on file with the *Columbia Law Review*).

308. Id.

309. Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 5, United States v. Direct Mktg. Assocs., Corp., No. 2:10-cv-00696-LOA (D. Ariz. Mar. 29, 2010), available at http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100330directmarketingcmpt.pdf (on file with the *Columbia Law Review*) ("Pursuant to section 621(a)(1) of the FCRA, 15 U.S.C. § 1681s(a)(1), the acts and practices alleged herein also constitute unfair or deceptive acts or practices in violation of section 5(a) of the FTC Act, 15 U.S.C. § 45(a).").

310. See, e.g., Plaintiff's Complaint for Civil Penalties at 1, Injunctive and Other Relief, United States v. Credit Bureau Collection Servs., No. 2:10-cv-00169-ALM-NMK (S.D. Ohio Feb. 24, 2010), available at http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100303creditcollectioncmpt.pdf (on file with the *Columbia Law Review*).

311. E.g., id. at 9–10 (discussing various legal requirements violated by material misrepresentations in debt collection practices).

312. For examples of FTC enforcement under COPPA, see Path Complaint, supra note 303, at 9–10; Artist Arena Complaint, supra note 303, at 11–12; RockYou Complaint, supra note 303, at 9–10; Godwin Complaint, supra note 303, at 7–8; Playdom Complaint, supra note 303, at 9; Iconix Brand Grp. Complaint, supra note 303, at 7–8; American Pop Corn Complaint, supra note 303, at 5–6; Lisa Frank Complaint, supra note 303, at 7–8; Bigmailbox.com Complaint, supra note 303, at 8–9; Toysmart.com Complaint, supra note 27, at 3.

313. Iconix Brand Grp. Complaint, supra note 303, at 3.

as well as security and confidentiality safeguards.[314] COPPA violations also tended to draw large fines, ranging from $250,000[315] to $3 million.[316]

c. *GLBA*. — The FTC regularly enforces two major rules under GLBA, the Safeguards Rule and the Privacy Rule. According to the FTC, the Safeguards Rule "requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards."[317] The Privacy Rule, as interpreted by the FTC, "requires financial institutions, *inter alia*, to provide customers with clear and conspicuous notices, both when the customer relationship is formed and annually for the duration of the customer relationship, that accurately reflect the financial institution's privacy policies and practices."[318]

d. *Safe Harbor*. — The U.S.-E.U. Safe Harbor Framework is the mechanism by which U.S. companies transfer data outside of the European Union in a way consistent with the E.U. Data Protection Directive.[319] According to the FTC, the Safe Harbor is a "voluntary frame-

---

314. See id. (listing various COPPA requirements).

315. United States v. Iconix Brand Grp., Inc., No. 09 Civ. 8864 (MGC), at 4 (S.D.N.Y. Nov. 5, 2009) (consent decree & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2009/10/091020iconixsonsentorder.pdf (on file with the *Columbia Law Review*) (imposing civil penalty of $250,000).

316. United States v. Playdom, Inc., No. SACV 11-0724-AG(ANx), at 6 (C.D. Ca. May 24, 2011) (consent decree & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2011/05/110512playdomconsentorder.pdf (on file with the *Columbia Law Review*) (imposing civil penalty of $3 million).

317. In re Nationwide Mortg. Grp., Inc., 139 F.T.C. 245, 246 (2005) (complaint). These safeguards include:

- Designating one or more employees to coordinate the information security program;
- Identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks;
- Designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures;
- Overseeing service providers, and requiring them by contract to protect the security and confidentiality of customer information; and
- Evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

Id. at 246–47.

318. Id. at 248; 16 C.F.R. §§ 313.4(a), 313.5(a)(1), 313.6(a)(8) (2013).

319. According to the FTC:

> The Directive sets forth EU requirements for privacy and the protection of personal data. Among other things, it requires EU Member States to implement legislation that prohibits the transfer of personal data outside the EU, with exceptions, unless the European Commission ("EC") has made a determination

work" that "allows U.S. companies to transfer personal data lawfully from the EU to the U.S. To join the Safe Harbor, a company must self-certify to [the Department of] Commerce that it complies with seven principles and related requirements that have been deemed to meet the EU's adequacy standard."[320] Some of the largest internet companies, including Google, Facebook, and MySpace, were accused by the FTC of failing to adhere to the U.S. Safe Harbor principles of notice and choice.[321] According to the FTC, the failure of these companies to comply with the Safe Harbor rendered their statements to the contrary in their privacy policies deceptive.[322]

B. *Developmental Patterns of FTC Privacy Jurisprudence*

Some commentators have criticized the FTC for acting arbitrarily and providing little guidance to companies, especially in its unfairness authority.[323] But when viewed with the analogy to the common law, the FTC's jurisprudence has evolved in classic patterns of development. Far from being arbitrary, FTC jurisprudence has grown incrementally and predictably.

The FTC's first privacy-related complaints were largely based upon straightforward theories of deception. Companies that made express or implied promises simply had to keep them. This could be thought of as a kind of "thin" jurisprudence in that it did little more than provide ad-

---

> that the recipient jurisdiction's laws ensure the protection of such personal data. This determination is commonly referred to as meeting the EU's "adequacy" standard.

Google Complaint, supra note 219, at 6.

320. Id. at 7.

321. Complaint at 8, In re MySpace LLC, FTC File No. 102 3058, No. C-4369 (F.T.C. Aug. 30, 2012) [hereinafter MySpace Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacecmpt.pdf (on file with the *Columbia Law Review*); Facebook Complaint, supra note 247, at 19; Google Complaint, supra note 219, at 7. Under the notice requirement, a company must disclose "the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure." MySpace Complaint, supra, at 6–7. Under the choice requirement, a company "must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual." Id. at 7. These definitions are consistent across complaints. See, e.g., Facebook Complaint, supra note 247, at 18; Google Complaint, supra note 219, at 7.

322. See, e.g., MySpace Complaint, supra note 321, at 8 (stating, by falsely representing it complied with Safe Harbor principles, MySpace engaged in "false or misleading" behavior constituting deceptive act).

323. See, e.g., Scott, supra note 21, at 165–71 ("No guidelines exist under which the Commission will act or refrain from acting if a data security breach occurs."); Stegmaier & Bartnick, Psychics, supra note 9, at 687–94 ("Th[e] inherent ambiguity [of unfairness authority] can be dangerous for regulated entities . . . .").

ministrative heft behind contract-like promises. But the FTC gradually began developing a body of doctrines that pushed beyond merely punishing broken promises; its privacy jurisprudence began to "thicken." While this development might seem surprising, from a common law perspective it is both natural and predictable.

One classic pattern of common law development is a gradual and incremental evolution of doctrine. The direction is typically from general principles to more specific standards.[324] Interpretations become more expansive over time, as new applications push the boundaries of language. Areas of normative consensus often become adopted as standards. And more kinds of activities that interfere with basic norms, even indirectly, become sources of common law liability or restriction.

The FTC has taken basic and clear violations of the FTC Act and other statutes and has derived a broader regulatory scope and more specific regulatory requirements. Specifically, four developmental patterns have emerged: (1) general standards have evolved into specific ones and become more rule-like in nature; (2) qualitative judgments have been incorporated into the law, often based on norms and best practices; (3) baseline standards have emerged; and (4) contributory liability has developed.

1. *Evolution from General to Specific Standards.* — A clear pattern in FTC privacy jurisprudence has been the evolution from imposing general standards to specific ones. This trend has occurred in Section 5 enforcement despite the fact that privacy policy promises have not progressed toward being more specific. If anything, they have become more vague as lawyers have attempted to avoid language that pins companies down on specifics. Nevertheless, the FTC has found companies in violation of rather general promises because of some very specific problems.

Moreover, Section 5 is vague itself, speaking broadly in terms of "deceptive" and "unfair" trade practices.[325] But as FTC complaints cite in detail the specific wrongful activities that constitute deception or unfairness, these terms start to become fleshed out in the privacy context.

This kind of development is a natural and logical outgrowth of multiple applications of a particular general standard. Much of this tracks the classic "standards versus rules" discussion.[326] The more that standards

---

324. E.g., Russell B. Korobkin, Behavioral Analysis and Legal Form: Rules vs. Standards Revisited, 79 Or. L. Rev. 23, 29 (2000) ("Just as a pure rule can become standard-like through unpredictable exceptions, a pure standard can become rule-like through the judicial reliance on precedent.").

325. 15 U.S.C. § 45(a)(1) (2012) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."). See generally Overview of FTC Authority, supra note 2 (detailing general and specific FTC investigatory powers).

326. For a broad set of scholarship tackling the standards versus rules debate, see generally Colin S. Diver, The Optimal Precision of Administrative Rules, 93 Yale L.J. 65, 65–66 (1983); Louis Kaplow, Rules Versus Standards: An Economic Analysis, 42 Duke L.J.

are applied in particular disputes, the more they adapt to become like rules. With each application, the standard starts to become more specific.[327] For example, the standard of negligence in tort law has developed many rule-like features over time.[328]

A similar dynamic has occurred with the FTC's jurisprudence on security. As previously mentioned, the FTC began very generally by ensuring companies honored their promises of security. But through a multitude of cases, a detailed list of problematic security practices has emerged.

This trajectory led the FTC to a significant challenge to its authority in *FTC v. Wyndham Worldwide Corp.*[329] Defendant Wyndham Worldwide, owner and operator of a series of hotels, was accused of failing "to provide reasonable and appropriate security for the personal information [it] collected and maintained . . . by engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[330] Specifically, the FTC alleged that Wyndham failed to utilize readily available security methods to limit access (such as firewalls), stored information in plain text, failed to implement adequate information security policies before connecting local computers with customer information to the company's larger network of computers, failed to remedy known security vulnerabilities, failed to use adequate identification and password protocols, failed to adequately restrict access to the company's network, and failed to follow proper incident response procedures.[331]

Wyndham is representative of the numerous security-related complaints brought by the FTC. Critics allege that the FTC has given very little guidance regarding which security-related activities or failures constitute an unfair or deceptive trade practice.[332] Yet, when viewed collec-

---

557, 621 (1992); Korobkin, supra note 324, at 56; Eric A. Posner, Standards, Rules, and Social Norms, 21 Harv. J.L. & Pub. Pol'y 101, 116–17 (1997); Kathleen M. Sullivan, The Supreme Court, 1991 Term—Foreword: The Justices of Rules and Standards, 106 Harv. L. Rev. 22, 26–27 (1992); Cass R. Sunstein, Problems with Rules, 83 Calif. L. Rev. 953, 957–58 (1995).

327. See, e.g., Robert L. Rabin, The Pervasive Role of Uncertainty in Tort Law: Rights and Remedies, 60 DePaul L. Rev. 431, 440 (2011) [hereinafter Rabin, Uncertainty] (describing how case-specific decisions constrain general standard of negligence in tort law).

328. See, e.g., Stephen G. Gilles, Rule-Based Negligence and the Regulation of Activity Levels, 21 J. Legal Stud. 319, 321–27 (1992) (arguing courts in negligence cases rely on statutory standards, customs, and reasonable person standard, making negligence law "heavily and pervasively rule based"); Rabin, Uncertainty, supra note 327, at 440 (describing, as example, rule against relief for negligent infliction of emotional distress).

329. Wyndham Complaint, supra note 122, at 1.

330. Id. at 10.

331. Id. at 10–12.

332. See, e.g., Stegmaier & Bartnick, Psychics, supra note 9, at 676 (noting "FTC's declination to use its existing rulemaking authority to clarify its data-security expectations").

tively, the FTC's data security jurisprudence forms a rather detailed list of inadequate security practices:

- Allowing data to be vulnerable to common attacks such as Structured Query Language (SQL) injection attacks and Cross-Site Scripting (XSS) attacks;[333]
- Lack of encryption (storage of data in plain text)/bad encryption;[334]
- Making data easily available (security flaw);[335]

---

333. E.g., RockYou Complaint, supra note 303, at 6; Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 12, 14, United States v. ValueClick, Inc., No. CV08-01711MMM(RZx) (C.D. Cal. filed Mar. 13, 2008) [hereinafter ValueClick Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317complaint.pdf (on file with the *Columbia Law Review*); Complaint at 2, In re CardSystems Solutions, Inc., FTC File No. 052 3148, No. C-4168 (F.T.C. Sept. 5, 2006) [hereinafter CardSystems Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2006/09/0523148cardsystemscomplaint.pdf (on file with the *Columbia Law Review*); In re Petco Animal Supplies, Inc., 139 F.T.C. 102, 104–05 (2005) (complaint); In re Guess?, Inc., 136 F.T.C. 507, 510–11 (2003) (complaint).

334. For examples of FTC enforcement based on plain-text data storage and transmission, see, e.g., Wyndham Complaint, supra note 122, at 10; RockYou Complaint, supra note 303, at 6; Complaint for Permanent Injunction and Other Equitable Relief at 13, FTC v. LifeLock, Inc., No. 2:10-cv-00530-MGM (D. Ariz. filed Mar. 8, 2010) [hereinafter LifeLock Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf (on file with the *Columbia Law Review*); ValueClick Complaint, supra note 333, at 13; Complaint at 3, In re Cbr Sys., Inc., FTC File No. 112 3120, No. C-4400 (F.T.C. Apr. 29, 2013) [hereinafter Cbr Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2013/05/130503cbrcmpt.pdf (on file with the *Columbia Law Review*) ("The Cbr laptop and Cbr external hard drive, both of which were unencrypted, contained enterprise network information, including passwords and protocols, that could have facilitated an intruder's access to Cbr's network . . . ."); Compete Complaint, supra note 217, at 5; Complaint at 4, In re Upromise, Inc., FTC File No. 102 3116, No. C-4351 (F.T.C. Mar. 27, 2012) [hereinafter Upromise Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf (on file with the *Columbia Law Review*); In re Lookout Servs., Inc., 151 F.T.C. 532, 535 (2011) (complaint); Ceridian Complaint, supra note 262, at 2; Twitter Complaint, supra note 140, at 3–4; Genica Complaint, supra note 216, at 2; Complaint at 3, In re TJX Cos., Inc., FTC File No. 072 3055, No. C-4227 (F.T.C. July 29, 2008) [hereinafter TJX Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf (on file with the *Columbia Law Review*); Life Is Good Complaint, supra note 260, at 2; Guidance Software Complaint, supra note 260, at 2; Complaint at 2, In re DSW, Inc., FTC File No. 052 3096, No. C-4157 (F.T.C. Mar. 7, 2006) [hereinafter DSW Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2006/03/0523096c4157dswcomplaint.pdf (on file with the *Columbia Law Review*); In re BJ's Wholesale Club, Inc., 140 F.T.C. 465, 467 (2005) (complaint); *In re Petco*, 139 F.T.C. at 106; *In re Guess?*, 136 F.T.C. at 512.

335. See, e.g., Franklin's Budget Car Complaint, supra note 304, at 3 ("Information for approximately 95,000 consumers, including, but not limited to, names, Social Security numbers, addresses, dates of birth, and drivers' license numbers ('customer files') was made available on a P2P network. Such information can easily be misused to commit identity theft and fraud."); Complaint at 2, In re EPN, Inc., FTC File No. 112 3143, No. C-4370 (F.T.C. June 7, 2012) [hereinafter EPN Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf (on file with the *Columbia Law Review*) ("EPN has engaged in a number of practices that, taken together,

- Failure to test the security of a product or process;[336]
- Failure to implement procedures to find and prevent data vulnerabilities;[337]

---

failed to provide reasonable and appropriate security for personal information on its computers and networks."); *Lookout Servs.*, 151 F.T.C. at 535 ("By typing the precise URL into the browser, [an employee] bypassed the Lookout login page, and was never prompted to provide a valid user credential. The employee then made minimal and easy-to-guess changes to the URL and gained access to the entire I-9 database."); In re MTS, Inc., 137 F.T.C. 444, 448 (2004) (complaint) ("Any visitor to the Tower Web site who entered a valid order number in the Order Status URL could view certain personal information relating to other Tower consumers, specifically, the consumer's name, billing and shipping addresses, email address, phone number . . . and all Tower products purchased online.").

336. These complaints largely stemmed from violations of the Safeguards Rule, section 501 of GLBA. E.g., HTC Complaint, supra note 215, at 6 ("HTC could have detected its failure to deactivate the debug code in its CIQ Interface had it had adequate processes and tools in place for reviewing and testing the security of its software code."); Upromise Complaint, supra note 334, at 4 ("[R]espondent did not test the Targeting Tool before distributing it to consumers or monitor the Targeting Tool's operation thereafter to verify that the information it collected was consistent with respondent's policies . . . ."); Complaint at 4, In re Fajilan & Assocs., FTC File No. 092 3089, No. C-4332 (F.T.C. Aug. 17, 2011) [hereinafter Fajilan Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819statewidecmpt.pdf (on file with the *Columbia Law Review*) (alleging violations of Safeguards Rule because respondent failed "to regularly test or monitor the effectiveness of its existing controls and procedures"); Complaint at 3, In re James B. Nutter & Co., FTC File No. 072 3108, No. C-4258 (F.T.C. May 5, 2009) [hereinafter Nutter Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090616nuttercmpt.pdf (on file with the *Columbia Law Review*) (same); In re Nationwide Mortg. Grp., Inc., 139 F.T.C. 245, 247–48 (2005) (complaint) (same); In re Sunbelt Lending Servs., Inc., 139 F.T.C. 1, 3–4 (2005) (complaint) (same).

337. This includes failure to adequately inventory networked computers and failure to follow incident response procedures by learning from previous attacks. E.g., Wyndham Complaint, supra note 122, at 11 (citing Wyndham's failure "to remedy known security vulnerabilities" which put information at risk). It also includes a failure to "assess risks" to the consumers' personal information a company collects. E.g., Franklin's Budget Car Complaint, supra note 304, at 2 (alleging respondent failed to "[a]ssess risks to the consumer personal information it collected and stored online"); see also HTC Complaint, supra note 215, at 2 (alleging HTC "engaged in a number of practices that, taken together, failed to employ reasonable and appropriate security in the design and customization of the software on its mobile devices"); EPN Complaint, supra note 335, at 2 (asserting several violations including failure to "[a]ssess risks to the consumer personal information it collected and stored online"); Complaint at 2, In re ACRAnet, Inc., FTC File No. 092 3088, No. C-4331 (F.T.C. Aug. 17, 2011) [hereinafter ACRAnet Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110809acranetcmpt.pdf (on file with the *Columbia Law Review*) (alleging failure to provide reasonable and appropriate security for its consumers' personal information); Fajilan Complaint, supra note 336, at 2 (alleging Fajilan failed to provide reasonable and appropriate security for its consumers' personal information including failing to "assess the risks of allowing end users with unverified or inadequate security to access consumer reports"); Ceridian Complaint, supra note 262, at 2 (listing practices failing to protect consumer security such as storing information in "clear, readable text" and failing to "adequately assess the vulnerability of its web applications and network to commonly known or reasonably foreseeable attacks"); Life Is Good Complaint, supra note 260, at 2

- Failure to remedy known security vulnerabilities;[338]
- Failure to implement procedures to detect unauthorized access;[339]
- Failure to implement procedures to control access to information;[340]
- Lack of data minimization (kept data for no reason or after it was needed);[341]
- Failure to implement cheap, easy-to-use, or common industry security practices;[342]

(alleging failure to provide reasonable and appropriate security for its consumers' personal information).

338. For examples of complaints in which the FTC alleged the company failed to remedy known security vulnerabilities, see, e.g., Wyndham Complaint, supra note 122, at 11; ACRAnet Complaint, supra note 337, at 2; Complaint at 3, In re SettlementOne Credit Co., FTC File No. 082 3208, No. C-4330 (F.T.C. Aug. 17, 2011) [hereinafter SettlementOne Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonecmpt.pdf (on file with the *Columbia Law Review*); Nutter Complaint, supra note 336, at 2–3; Nations Title Agency Complaint, supra note 304, at 3.

339. For examples of FTC claims alleging inadequate detection measures, see, e.g., LifeLock Complaint, supra note 334, at 10; ValueClick Complaint, supra note 333, at 14; Cbr Complaint, supra note 334, at 3; Genica Complaint, supra note 216, at 3; Guidance Software Complaint, supra note 260, at 2; DSW Complaint, supra note 334, at 2; *BJ's Wholesale*, 140 F.T.C. at 467.

340. This requirement appears to simply mirror the FCRA requirement in section 604(c) of identity verification. See Fair Credit Reporting Act § 604(c), 15 U.S.C. § 1681b(c) (2012) (defining permissible uses of consumer reports by third parties initiating creditor insurance transactions); id. § 607(a), 15 U.S.C. § 1681e(a) (requiring "[e]very consumer reporting agency [to] make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report"). It appears that, in addition, the FTC considers this an unfair practice. E.g., Complaint at 3, In re Equifax Info. Servs. LLC, FTC File No. 102 3252, No. C-4387 (F.T.C. Mar. 5, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/03/130315equifaxcmpt.pdf (on file with the *Columbia Law Review*) (alleging Equifax violated section 604(c) by furnishing consumer reports to parties without permissible purpose to obtain such reports, which constituted "unfair and deceptive" acts).

341. For examples of the FTC's stance that the unnecessary retention of data constitutes an improper security practice, see, e.g., RockYou Complaint, supra note 303, at 6, 10; Cbr Complaint, supra note 334, at 3; Ceridian Complaint, supra note 262, at 2; Life Is Good Complaint, supra note 260, at 2; DSW Complaint, supra note 334, at 2; *BJ's Wholesale*, 140 F.T.C. at 468.

342. For examples of the FTC's stance that the failure to implement cheap, easy-to-use, or common industry security practices constitutes an improper security practice, see, e.g., Wyndham Complaint, supra note 122, at 10–11; RockYou Complaint, supra note 303, at 6; LifeLock Complaint, supra note 334, at 13; HTC Complaint, supra note 215, at 2–3; Compete Complaint, supra note 217, at 4–5; Upromise Complaint, supra note 334, at 5–6; Ceridian Complaint, supra note 262, at 2; In re Dave & Buster's, Inc., 149 F.T.C. 1450, 1451 (2010) (complaint); Genica Complaint, supra note 216, at 2–3; Complaint at 3–4, In re Reed Elsevier Inc., FTC File No. 052 3094, No. C-4226 (F.T.C. July 29, 2008) [hereinafter Reed Elsevier Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801reedcomplaint.pdf (on file with the *Columbia Law*

- Failure to train employees in proper data security;[343]
- Failure to manage third party access to data;[344]
- Failure to verify and authenticate identity of third party recipient;[345]
- Failure to monitor data recipients' activity;[346]
- Failure to require by contract third party protection of information;[347]
- Failure to securely dispose of data (unsecured dumpsters);[348]

Review); TJX Complaint, supra note 334, at 2–3; Life Is Good Complaint, supra note 260, at 2. Common examples of such practices or measures are firewalls and segmenting servers. See, e.g., RockYou Complaint, supra note 303, at 6–7 (discussing failure to segment servers and take inexpensive measures to protect against hacker attack).

343. For examples of the FTC's articulation of the failure to train employees properly, see, e.g., Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 5–6, United States v. PLS Fin. Servs., Inc., No. 1:12-cv-08334 (N.D. Ill. Oct. 26, 2012) [hereinafter PLS Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2012/11/121107plspaydaycmpt.pdf (on file with the *Columbia Law Review*); HTC Complaint, supra note 215, at 2; EPN Complaint, supra note 335, at 2; Upromise Complaint, supra note 334, at 5; Rite Aid Complaint, supra note 262, at 2–3; CVS Caremark Complaint, supra note 262, at 2; Goal Fin. Complaint, supra note 304, at 2; In re Eli Lilly & Co., 133 F.T.C. 763, 767 (2002) (complaint). Included in this category is a failure to limit employee access to data when such access is not necessary. See, e.g., LifeLock Complaint, supra note 334, at 10 (alleging LifeLock violated Section 5 by, among other acts, "[f]ail[ing] to limit access to personal information . . . only to employees and vendors needing access to the information to perform their jobs").

344. For examples of FTC critiques of inadequate third party access control, see, e.g., Wyndham Complaint, supra note 122, at 12; Rental Research Servs. Complaint, supra note 300, at 7; ValueClick Complaint, supra note 333, at 5; Upromise Complaint, supra note 336, at 4–5; ACRAnet Complaint, supra note 337, at 2; Premier Capital Lending Complaint, supra note 304, at 3–4; Nations Title Agency Complaint, supra note 304, at 2. This includes failure to verify and authenticate the identities of third party recipients as well as failure to monitor or otherwise identify unauthorized recipient activity. See Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 4–6, United States v. ChoicePoint Inc., No. 06-CV-0198 (N.D. Ga. Feb. 15, 2006) [hereinafter ChoicePoint Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2006/01/0523069complaint.pdf (on file with the *Columbia Law Review*) (discussing defective verification policies). It includes general charges of failing to protect information in the hands of third party recipients as well as very specific charges by the FTC such as "[f]ailing to oversee service providers and to require them by contract to implement safeguards to protect respondent's customer information." Nations Title Agency Complaint, supra note 304, at 4.

345. See, e.g., ChoicePoint Complaint, supra note 344, at 4–6 (admonishing company for accepting contradictory verification documentation).

346. E.g., id. at 6–7.

347. This is also a violation of the GLBA Safeguards Rule. See, e.g., Nations Title Agency Complaint, supra note 304, at 3–4 (analyzing violations of Safeguards Rule); In re Sunbelt Lending Servs., Inc., 139 F.T.C. 1, 2–3 (2005) (complaint) (same).

348. See, e.g., PLS Complaint, supra note 343, at 7–8 (alleging inadequate disposal practices); Complaint for Civil Penalties, Injunctive and Other Relief at 4–5, United States v. Am. United Mortg. Co., No. 07C 7064 (N.D. Ill. Dec. 17, 2007), available at http://www.ftc.gov/sites/default/files/documents/cases/2007/12/071217americanunitedmrtgcmplt.

- Failure to set up system of public feedback for vulnerabilities;[349]
- Failure to limit computer connectivity to company's intranet/network; and[350]
- Poor username/password protocol, including the following missteps:[351]
  - Used common/known passwords;
  - Did not require users to change passwords;
  - Failed to suspend users after repeated failed login attempts;
  - Allowed username and password sharing;
  - Permitted users to store passwords in unsafe cookies;
  - Failed to require user information such as passwords to be encrypted in transit; and
  - Allowed new user credentials to be created without checking them against previously obtained legitimate credentials.

This list of inadequate security practices mirrors the HIPAA Security Rule, which is one of the most specific data security laws.[352] For example, the HIPAA Security Rule requires organizations to assess and control risk by implementing security programs,[353] testing the company's data security,[354] ensuring that outside data vendors secure data,[355] training employees in data security,[356] and implementing authentication[357] and access-

---

pdf (on file with the *Columbia Law Review*) (same); Rite Aid Complaint, supra note 262, at 2–3 (same); CVS Caremark Complaint, supra note 262, at 2–3 (same).

349. See HTC Complaint, supra note 215, at 2 (stating company "failed to implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents").

350. See, e.g., In re Dave & Buster's, Inc., 149 F.T.C. 1450, 1451 (2010) (complaint) (asserting defendant "failed to use readily available security measures to limit access between in-store networks, such as by employing firewalls or isolating the payment card system from the rest of the corporate network" and "failed to . . . limit access to its computer networks through wireless access points on the networks").

351. For a detailed exploration of the FTC's interpretation of proper password protocol, see Twitter Complaint, supra note 140, at 3–5; see also Wyndham Complaint, supra note 122, at 10–12 (detailing deficiencies in security measures); LifeLock Complaint, supra note 334, at 9–11 (same); In re Lookout Servs., Inc. 151 F.T.C. 532, 534–35 (2011) (complaint) (same); Reed Elsevier Complaint, supra note 342, at 3–4 (same); TJX Complaint, supra note 334, at 2 (same); Guidance Software Complaint, supra note 260, at 2 (same); CardSystems Complaint, supra note 333, at 2 (same); In re BJ's Wholesale Club, Inc., 140 F.T.C. 465, 467–68 (2005) (complaint) (same).

352. See 45 C.F.R. § 164.308–.312 (2013) (prescribing administrative, physical, and technical safeguards for covered entities).

353. Id. § 164.308(a)(1)(i), (ii)(A)–(B).

354. Id. § 164.308(a)(1)(ii)(B).

355. Id. § 164.308(b)(1).

356. Id. § 164.308(a)(5)(i).

357. Id. § 164.312(d).

control procedures.[358] The Security Rule also requires technical safeguards, such as identification access controls and encryption,[359] and physical safeguards, such as secure data disposal and physical access safeguards.[360]

Many of these requirements were also tethered to the Safeguards Rule of GLBA, particularly when the security promises were vague.[361] It seems that when determining which specific failures amounted, in the aggregate, to a breach of an unspecified promise of security or general standard for unfairness, the FTC has drawn from the particular requirements of other statutes.

Data security provisions in privacy policies often employ vague language such as "reasonable" security measures, so how can such language have led to such a detailed series of security requirements as listed above?

First, the vague language opens the door for the FTC to rely upon industry standards.[362] Vladeck noted that it would be quite rare to "find an FTC data security case where there was a serious argument that the security practice met industry norms. Many of the security lapses were egregious by any measure."[363]

The term "reasonable" in many legal contexts is defined by reference to common practices. For example, the reasonableness inquiry in negligence often draws upon customary practices.[364] In defamation lawsuits brought by nonpublic figures, courts often look to industry customs when determining whether a speaker or publisher acted reasonably.[365]

---

358. Id. § 164.308(a)(3)(ii)(B), (a)(4)(ii)(B)–(C).

359. Id. § 164.312(a), (d).

360. Id. § 164.310.

361. See, e.g., Nations Title Agency Complaint, supra note 304, at 4 (alleging deceptive trade practice where defendant who promised in privacy policy "to maintain the confidentiality and integrity of the personal information in its possession . . . in compliance with federal standards" committed GLBA Safeguards Rule breach by failing to follow specific security procedures).

362. See, e.g., ValueClick Complaint, supra note 333, at 11 (alleging defendants "did not encrypt sensitive information consistent with industry standards"); Compete Complaint, supra note 217, at 5 (alleging respondent "failed to design and implement reasonable information safeguards to control the risks to customer information"); In re Guess?, Inc., 136 F.T.C. 507, 511 (2003) (complaint) ("The risk of web-based application attacks is commonly known in the information technology industry, as are simple, publicly available measures to prevent such attacks. Security experts have been warning the industry about these vulnerabilities since at least 1997 . . . .").

363. Vladeck Interview, supra note 68.

364. See, e.g., Kenneth S. Abraham, Custom, Noncustomary Practice, and Negligence, 109 Colum. L. Rev. 1784, 1785 (2009) ("Admitting custom evidence reflects the idea that recurring patterns of conduct have a bearing on what constitutes reasonable care.").

365. See, e.g., Gobin v. Glove Publ'g Co., 531 P.2d 76, 84 (Kan. 1975) (applying standard based on local "community" or "similar communities under the existing circumstances"); Malson v. Palmer Broad. Grp., 936 P.2d 940, 942 (Okla. 1997) ("[T]he best evidence of ordinary of [sic] care is the degree of care which ordinarily prudent

Second, with regard to data security, there is a consensus that many of the practices listed above are poor security practices.[366] With regard to privacy, what constitutes good practice is more in dispute, although there are certainly some practices about which consensus has developed. Most notably, providing people with notice about data collection and use has become commonplace. The biggest disputes in privacy turn on the way consent should be procured and how data should be used. In these areas, the FTC has not propounded any kind of specific standard.

Returning to the *Wyndham* case, the defendant's arguments against the FTC's detailed security requirements neglect to acknowledge that FTC jurisprudence has progressed in a natural and logical fashion. One would expect over time for a general standard about data security to be refined as that standard is applied in specific cases. This is an almost inevitable progression, and it is exactly how the common law works.

Other general standards have been moving to specific standards for the FTC. Consider the FTC's definition of "clearly and conspicuously," which was defined in Liberty Financial's consent order in 1999 as being "in a type size and location that are not obscured by any distracting elements and are sufficiently noticeable for an ordinary consumer to read and comprehend, and in a typeface that contrasts with the background against which it appears."[367] Compare this to the FTC's more recent interpretation of "clearly and prominently," which contains four different sections and concerns such specifics as: text size, type, and location; the volume and cadence of audible communications; the duration of video communications; and the syntax, complexity, and consistency of any language in any medium.[368]

---

persons, engaged in the same kind of business, customarily have exercised and commonly do exercise under similar circumstances." (emphasis omitted)).

366. See, e.g., Joint Task Force Transformation Initiative, Nat'l Inst. of Standards & Tech., Information Security: Guide for Assessing the Security Controls in Federal Information Systems and Organizations—NIST Special Publication 800-53A, at 1–3 (2010), available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf (on file with the *Columbia Law Review*) (setting out best practices for data security assessment plans within federal government agencies); Joint Task Force Transformation Initiative, Nat'l Inst. of Standards & Tech., Information Security: Guide for Conducting Risk Assessments—NIST Special Publication 800-30, at 4–22 (2012), available at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf (on file with the *Columbia Law Review*) (describing fundamentals of conducting risk management assessments); Microsoft IT Showcase, Information Security at Microsoft Overview: Technical White Paper 19–35 (2007) (discussing Microsoft IT security framework to assist other stakeholders in avoiding poor security practices).

367. In re Liberty Fin. Cos., Inc., FTC File No. 982 3522, No. C-3891, at 2 (F.T.C. Aug. 12, 1999) (decision & order), available at http://www.ftc.gov/sites/default/files/documents/cases/1999/08/libertydo.pdf (on file with the *Columbia Law Review*).

368. In re Scanscout, Inc., File No. 102-3185, No. C-4344, at 2 (F.T.C. Dec. 14, 2011) (decision & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2011/12/111221scanscoutdo.pdf (on file with the *Columbia Law Review*).

The FTC has further bolstered its interpretation of the "clear and conspicuous" requirement by mandating specific text with hyperlinks on webpages, stating, "We collect information about your activities on certain websites to send you targeted ads. To opt out of our targeted advertisements click here."[369] This is a very particular, substantive requirement. The FTC further refined this statement, requiring that opt-out mechanisms "require no more than one action by the user (*e.g.*, one click or one change to a browser setting) after the user is directed to such [opt-out] mechanism."[370]

2. *Incorporation of Qualitative Judgments.* — Although sometimes privacy policies and statutes establish a qualitative standard, such as "adequate" or "reasonable" security, in many cases they do not make any reference to quality. Such is the case with notice. Indeed, many privacy policies do not make explicit promises about notice. They may constitute notice, but they do not make any specific promise that people will be notified. Nevertheless, the FTC has concluded in cases that if notice is provided—regardless of what is promised—it must be of a certain minimum quality. In essence, the FTC is moving toward requiring "complete" or "meaningful" notice.

Recall *In re Sears Holdings Management Corp.*, which involved the ineffectiveness of disclosures regarding the existence and scope of spyware that were buried in a dense, boilerplate terms-of-use agreement.[371] The FTC here looked beyond formalistic notions of notice and consent to examine the substance of the transaction, finding that the full scope of surveillance was not disclosed to consumers due to the vague language used.[372] In addition to the laptop monitoring cases that involved spyware, the FTC indicated in *In re Epic Marketplace* that history sniffing—gathering browser data about whether webpages were previously viewed—is also a practice that "would be material to consumers" in deciding whether to opt out of receiving targeted advertisements.[373] Thus, according to the FTC, in light of the company's other statements describing its privacy and online behavioral targeting practices, its failure to disclose the fact that it engaged in history sniffing was seen as deceptive.

---

369. Id. at 3–4.

370. Id. at 4.

371. Sears Complaint, supra note 243; see also Gindin, supra note 246, at 5 ("In the Sears Matter, the FTC indicated that the crux of the issue was the inadequately disclosed collection of sensitive data . . . ."); Yan Fang, The Death of the Privacy Policy?: Effective Privacy Disclosures After *In re Sears*, 25 Berkeley Tech. L.J. 671, 673 (2010) (supporting conclusion that Sears engaged in deceptive practices).

372. Sears Complaint, supra note 243, at 5 ("[R]espondent has represented, expressly or by implication, that the Application would track consumers' 'online browsing.' Respondent failed to disclose adequately that the software application, when installed, would[] monitor nearly all of the Internet behavior that occurs on consumers' computers . . . .").

373. Epic Marketplace Complaint, supra note 228, at 4.

In *United States v. Path*, a case involving mobile devices and social software, the FTC again rejected vague, slippery language as effective notice to consumers regarding the collection and use of information, particularly in light of user interfaces that seemed to represent more protective practices.[374] In its privacy policy, Path explicitly provided, "We automatically collect *certain information* when you use our site and our services, *such as* your Internet Protocol (IP) address, your operating system, the browser type, the address of a referring site and your activity on our site."[375] Yet the FTC interpreted this statement to mean that "Defendant informed users that it automatically collected *only* certain information, such as IP address, operating system, browser type, address of referring site, and site activity information."[376] According to the FTC, Path collected a lot more personal data, including information about users' mobile device contacts.[377] Although the allegedly wrongfully collected data could technically fall within the language of the privacy policy due to the use of the nonexclusive term "such as" when listing examples of what was collected, the FTC deemed the notice incomplete and the examples inadequately illustrative of the kinds of data gathered.[378] The FTC has thus indicated it will reject as inadequate notices that are technically correct yet not sufficiently complete in explaining a company's practices. In its consent order with Path, the FTC required that the company disclose the categories of information that will be accessed and collected "separate and apart from any 'privacy policy,' 'terms of use,' 'blog,' 'statement of values' page, or other similar document."[379] The FTC also required that Path obtain express affirmative consent to access or collect this information.[380]

These cases involve movement beyond formalities. The FTC required more than a promise being formally honored; it looked to whether it was carried out in an adequate manner. The FTC required more than whether practices technically were consistent with a notice; it looked to how completely the notice described the practices. This kind of inquiry requires qualitative judgments.

The incorporation of qualitative judgments into language that lacks specific qualitative standards or even any qualitative standard is also a natural byproduct of the common law process. By common law process,

---

374. United States v. Path, Inc., No. 13-cv-00448, at 12 (N.D. Cal. Feb. 8, 2013) [hereinafter Path Consent Decree & Order] (consent decree & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf (on file with the *Columbia Law Review*) (requiring clear and prominent disclosure of categories of information being collected from customers).

375. Path Complaint, supra note 303, at 5 (emphases added).

376. Id. (emphasis added).

377. Id. at 4–5.

378. Id. at 5–6, 8.

379. Path Consent Decree & Order, supra note 374, at 12.

380. Id.

this Article is referring not just to judge-made law, but also the body of judicial interpretations of constitutional or statutory language.[381] In any system of precedent, this common law of interpretation will arise.

A notable contrast involves civil law systems, where decisions about statutory provisions are not accorded precedential weight, and each interpretation of the provision need not follow from any previous interpretation.[382] But when statutory or constitutional language is interpreted in the United States, courts are bound to follow the interpretive precedent established by other judicial decisions, and a common law develops as a gloss around this language.[383]

A logical extension of any requirement is that it be carried out in a meaningful way. If the law requires "notice," it would be reasonable to expect courts to imply some kind of qualitative standard, such as "reasonable notice" or "adequate notice." For example, in *In re Aspen Way Enterprises, Inc.*, the FTC required the companies entering into a consent order to abide by very specific procedures to effectuate notice, including the use of icons to notify users when a geolocational tracking feature is operational.[384] In *United States v. ChoicePoint Inc.*, the FTC accused the data broker of failing to adequately verify the identity of third party data recipients because they accepted dubious and often contradictory forms of identification.[385] In *FTC v. ControlScan, Inc.*, the FTC alleged that defendant ControlScan did not take reasonable steps to verify that companies displaying ControlScan's privacy-related certification "seals" were actually providing the appropriate or promised privacy or security protection.[386]

---

381. See Scott Brewer, Exemplary Reasoning: Semantics, Pragmatics, and the Rational Force of Legal Argument by Analogy, 109 Harv. L. Rev. 923, 936 n.30 (1996) (noting term "common law" "can refer to valid legal rules whose principal immediate source of authority is judicial," as well as "*method* of legal decision a court uses, whatever the court takes as its principal source of authority for the decision"); David A. Strauss, Common Law Constitutional Interpretation, 63 U. Chi. L. Rev. 877, 885 (1996) ("[O]ur written constitution has, by now, become part of an evolutionary common law system, and the common law—rather than any model based on the interpretation of codified law—provides the best way to understand the practices of American constitutional law.").

382. See, e.g., Mary Garvey Algero, The Sources of Law and the Value of Precedent: A Comparative and Empirical Study of a Civil Law State in a Common Law Nation, 65 La. L. Rev. 775, 787 (2005) ("[I]n legal systems based on the civil law tradition, cases are not formally recognized as a source of law, and the doctrine of stare decisis is not recognized."); William Tetley, Mixed Jurisdictions: Common Law v. Civil Law, 60 La. L. Rev. 677, 703 (2000) (describing role of statutes as paramount in civil law system).

383. See, e.g., Algero, supra note 382, at 783–86 (explaining under common law, judges must "apply the law as it has been set out in one prior case when the prior decision was made by a court that is higher than, and sometimes equal to, the court rendering the present decision").

384. Aspen Way Agreement & Order, supra note 154, at 5.

385. ChoicePoint Complaint, supra note 344, at 4–6.

386. Complaint for Permanent Injunction and Other Equitable Relief at 8–10, FTC v. ControlScan, Inc., No. 1:10-cv-00532 (N.D. Ga. Mar. 8, 2010) [hereinafter ControlScan

Another qualitative judgment inherent in the FTC jurisprudence is the importance of "opt in" as a consumer preference and a strong disfavoring of default settings that make personal data "publicly accessible." In *FTC v. Frostwire, LLC*, the FTC found that the default setting of "public sharing" for preexisting files on consumer computers was problematic.[387] In *In re Aspen Way*, the companies signing the consent decree were prohibited from using geophysical location tracking technology to track consumers without first obtaining "affirmative express consent."[388] Similarly, in *In re Gateway Learning Corp.*, the FTC required that the company obtain opt-in consent from individuals to material changes in its privacy policy involving data collected prior to the change.[389]

3. *Establishing Baseline Standards.* — Beyond infusing vague standards with more qualitative content, the FTC cases have evolved from enforcing promises to developing more substantive baseline standards that have become nearly independent of the statements made in privacy policies. These baseline standards are based upon industry norms and consumer expectations.[390]

For example, the FTC now appears to require baseline security practices for all companies that deal with personal information and prohibits certain kinds of invasive information collection and use without proper notice regardless of the existence of a privacy policy.[391] In particular, the FTC began to bring complaints against companies engaging in unfair data security practices without any violation of published privacy policies. The FTC asserted that failing to implement "reasonable security measures" to protect personal data constituted an unfair act or practice under Section 5.[392] For example, in *In re Dave & Buster's, Inc.*, the FTC's

---

Complaint], available at http://ftc.gov/sites/default/files/documents/cases/2010/02/100225controlscancmpt.pdf (on file with the *Columbia Law Review*).

387. Frostwire Complaint, supra note 250, at 13.

388. Aspen Way Agreement & Order, supra note 154, at 5.

389. Gateway Decision & Order, supra note 85, at 469.

390. See, e.g., ValueClick Complaint, supra note 333, at 11, 13 (explicitly referencing defendant's failure to follow industry security standards); In re Guess?, Inc., 136 F.T.C. 507, 511 (2003) (complaint) (describing defendant's failure to prevent attacks through simple measures commonly known within industry).

391. See, e.g., Aspen Way Agreement & Order, supra note 154, at 4–5 (outlining notice and consent requirements separate and apart from any existing privacy policy).

392. Compare Franklin's Budget Car Complaint, supra note 304, at 3 (P2P software case based upon deception), with EPN Complaint, supra note 335, at 2–3 (P2P software based upon unfairness). The practices identified as problematic were very similar. In *Franklin's*, the company promised, "We restrict access to non public personal information about you to only those employees who need to know that information to provide products and services to you. We maintain physical, electronic, and procedural safe guards that comply with federal regulations to guard non public personal information," but in fact had allowed the information to be shared on a P2P network. Franklin's Budget Car Complaint, supra note 304, at 2–3. In *EPN*, the FTC made a similar allegation about sharing customers through a P2P network, but did not reference the company's privacy policy. EPN Complaint, supra note 335, at 2–3.

complaint made no reference to any security-related representation by Dave & Buster's. Yet the Commission alleged that the failure of Dave & Buster's "to employ reasonable and appropriate security measures to protect personal information" was an unfair practice.[393] In *In re BJ's Wholesale Club, Inc.*, the FTC brought an unfairness action against a company for inadequate security practices.[394] The FTC's action was not based on any failure to live up to a promise of good security. Nor was there a statute mandating that BJ's Wholesale Club provide good data security. Instead, the FTC concluded that providing inadequate security was an unfair practice. Thus, even without a promise of security or a statutory requirement of security, companies still have an obligation to keep data secure. Essentially, the FTC has mandated adequate data security as a baseline standard.

A progression to baseline standards is part of the common law process. The common law is designed to develop gradually, and it often looks to societal norms when composing a standard.[395] Indeed, in many other areas of law, as industry standards develop, failure to adhere to them makes it increasingly likely that those failing to adhere to them will be deemed negligent.[396]

In the domain of data privacy and security, over the past fifteen years a consensus about certain privacy practices has developed, as the field has become more professionalized and certain privacy practices have become more common. The FTC has begun to look to these standards to establish a baseline standard of care when it comes to personal data. For example, in *United States v. ValueClick, Inc.*, the FTC alleged that the defendant failed to meet its promise of adequate security by, among other things, using a "nonstandard, proprietary form of encryption" instead of "the type of extensively-tested algorithms found in industry-standard systems."[397] The FTC found that this proprietary encryption "utilized a simple alphabetic substitution system that was subject to significant vulnerabilities."[398]

Once standards become well established, there is an expectation that companies follow them, and they may readily become implicit within a broader set of promises. Moreover, people begin to expect that these standards are followed, and a large part of privacy involves managing people's expectations.

---

393. In re Dave & Buster's, Inc., 149 F.T.C. 1450, 1452 (2010) (complaint).

394. In re BJ's Wholesale Club, Inc., 140 F.T.C. 465, 468 (2005) (complaint).

395. E.g., Cross, supra note 171, at 25.

396. See Restatement (Second) of Torts § 295A (1965) ("In determining whether conduct is negligent, the customs of the community, or of others under like circumstances, are factors to be taken into account . . . ."). See generally Richard A. Epstein, The Path to *The T.J. Hooper*: The Theory and History of Custom in the Law of Tort, 21 J. Legal Stud. 1, 16–36 (1992) (discussing custom in American tort law).

397. ValueClick Complaint, supra note 333, at 11.

398. Id.

4. *Recognizing Indirect Liability.* — Another trend in FTC privacy jurisprudence has been to recognize liability arising in part from the promises of others. The FTC has initiated enforcement actions against companies that violate other companies' terms of use or privacy policies rather than any promises these companies make themselves. The FTC has also initiated actions against those who furnish companies with the means to commit unfair or deceptive acts or practices.

In *In re Vision I Properties, LLC*, the FTC contended that a company engaged in an unfair practice by violating the privacy policy of another company.[399] Here, Vision One licensed "shopping cart software and provide[d] related services to thousands of small online retail merchants."[400] Vision One was able to collect personal information when a merchant's consumers used Vision One's "shopping cart" software. The merchants that used Vision One's software often had privacy policies.[401] According to the FTC, the shopping cart and checkout pages generated by Vision One's software looked like they were part of the merchants' sites, but failed to disclose to consumers "that the information entered on them is not subject to the merchant privacy policies or that it will be shared with third parties for marketing purposes."[402] The FTC alleged that "consumers reasonably expect that the merchants' privacy policies cover information consumers provide" on the shopping cart pages, and the collection of consumer information and subsequent sharing of that information with third parties in knowing violation of merchant privacy policies constituted an unfair trade practice.[403]

Facilitating the wrongful conduct of another also triggers FTC condemnation. In *FTC v. Accusearch, LLC*, the FTC claimed that Accusearch facilitated violations of the Telecommunications Act even though Accusearch did not commit the violations itself.[404] In *In re DesignerWare, LLC*, the FTC alleged:

> By furnishing others with the means to engage in the unfair practices . . . respondents have provided the means and instrumentalities for the commission of unfair acts and practices and thus have caused or are likely to cause substantial injury to consumers that cannot be reasonably avoided and is not outweighed by countervailing benefits to consumers or competition.[405]

399. In re Vision I Props., LLC, 139 F.T.C. 296, 297–99 (2005) (complaint).

400. Id. at 297.

401. Id.

402. Id. at 298–99.

403. Id. at 299.

404. Accusearch Complaint, supra note 230, at 3–5.

405. DesignerWare Complaint, supra note 227, at 7.

In *In re MySpace LLC*, the FTC concluded that sharing non-personally identifiable information (PII) with third parties who can use it to obtain PII was constructive sharing of PII.[406] Thus, there was deception.

A related twist arose via the Facebook action, in which the FTC stated that under its consent order, "Facebook will be liable for conduct by apps that contradicts Facebook's promises about the privacy or security practices of these apps."[407]

The cases alleging violations of another company's terms of use are not a very controversial step for the FTC to take. Recognizing a violation for furnishing means for others to violate Section 5 pushes into new territory with respect to privacy jurisprudence—indirect liability that depends upon the actions of others. However, "means and instrumentalities" theories are common in other areas of FTC jurisprudence, such as in the Commission's antifraud complaints against payment processors and purveyors of pyramid schemes.[408] These cases also rest upon a theory of indi-

406. MySpace Complaint, supra note 321, at 4–6 (describing MySpace's undisclosed PII sharing policies as material to consumers in their enrollment and use of the site). For more information on PII, see Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814, 1816 (2011), which states, "PII is one of the most central concepts in privacy regulation. It defines the scope and boundaries of a large range of privacy statutes and regulations."

407. In re Facebook, Inc., FTC File No. 092 3184, No. C-4365, at 1 (F.T.C. Aug. 10, 2012) (statement of the Commission), available at http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookstmtcomm.pdf (on file with the *Columbia Law Review*).

408. See, e.g., FTC v. Mentor Network, Inc., No. SACV 96-1004 LHM (EEx), at 4 (C.D. Cal. Mar. 18, 1997) (stipulated final judgment & order), available at http://www.ftc.gov/sites/default/files/documents/cases/1997/03/mentor.pdf (on file with the *Columbia Law Review*) (enjoining defendants from "advertising, promoting, offering for sale, or sale of any chain or pyramid marketing program"); In re Schmidt, FTC File No. 972 3308, No. C-3834, at 3 (F.T.C. Nov. 3, 1998) (decision & order), available at http://www.ftc.gov/sites/default/files/documents/cases/1998/11/9723308.do_.htm (on file with the *Columbia Law Review*) (ordering respondent to "cease and desist from engaging, participating, or assisting in any manner or capacity whatsoever in any Prohibited Marketing Program"); Complaint for Injunctive and Other Equitable Relief at 17–18, FTC v. Landmark Clearing, Inc., No. 4:11-cv-00826 (E.D. Tex. Dec. 15, 2011), available at http://www.ftc.gov/sites/default/files/documents/cases/2012/01/120105landmarkcmpt.pdf (on file with the *Columbia Law Review*) (alleging defendant's debit transaction service was "unfair or deceptive act[] or practice[]"); Complaint for Injunctive and Other Relief at 6, FTC v. Martinez, No. 00-12701-CAS (C.D. Cal. Dec. 4, 2000), available at http://www.ftc.gov/sites/default/files/documents/cases/2000/12/martinez.pdf (on file with the *Columbia Law Review*) ("By providing false identification templates that are used to facilitate fraudulent activity . . . Defendant has provided the means and instrumentalities for the commission of deceptive acts and practices."); Complaint for Injunctive and Other Equitable Relief at 3–6, FTC v. Five Star Auto Club, Inc., No. 99-CV-1693 (S.D.N.Y. June 12, 2000), available at http://www.ftc.gov/sites/default/files/documents/cases/1999/03/fivestarcmp.pdf (on file with the *Columbia Law Review*) (describing defendants' pyramid scheme); Complaint for Permanent Injunction and Other Equitable Relief at 5, FTC v. Martinelli, No. 399-CV-1272 (D. Conn. July 7, 1999), available at http://www.ftc.gov/sites/default/files/documents/cases/1999/07/dpmarketingcmp.pdf (on file with the *Columbia Law Review*) (alleging pyramid scheme).

rect liability that is relatively common in the law.[409] For example, tort law recognizes the liability of negligent risk-generating behavior that leads to "harms caused by third-party intervening conduct."[410] As Danielle Citron notes, "Courts permit recovery in such cases because the defendant paved the way for the third party to injure another. They justify imposing liability on the enabling actor due to the deterrence gaps—the difficulty of finding and punishing the criminal in order to deter would-be tortfeasors."[411] Citron continues, "Courts have also recognized theories of liability against those who gather or communicate information on the theory that their actions negligently, recklessly, knowingly, or purposefully facilitated criminal conduct."[412]

This theory is also analogous to theories of contributory copyright infringement. In copyright law, companies can be held secondarily liable under two different theories, contributory liability and vicarious infringement.[413] The Supreme Court has stated that "[o]ne infringes contributorily by intentionally inducing or encouraging direct infringement, and infringes vicariously by profiting from direct infringement while declining to exercise the right to stop or limit it."[414] Secondary liability is not provided for by statute, but rather, is a well-established common law principle.[415] Software companies have been found secondarily liable for

---

409. See Robert L. Rabin, Enabling Torts, 49 DePaul L. Rev. 435, 441–42 (1999) ("[T]he erosion of the proximate cause limitation for intervening acts can be regarded as a temporal shift in moral sensibilities from a more individualistic era to one in which tort law . . . increasingly reflects more expansive notions of responsibility for the conduct of others.").

410. Id. at 437 n.14.

411. Danielle Keats Citron, Mainstreaming Privacy Torts, 98 Calif. L. Rev. 1805, 1836–37 (2010).

412. Id. at 1838 ("Thus, in *Remsburg v. Docusearch*, a stalker killed a woman after obtaining the woman's work address from the defendant, a data broker. The court found that the broker had a duty to exercise reasonable care in releasing information to third parties, due to the risk of criminal misconduct." (citing Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003))).

413. See, e.g., Jay Dratler, Jr., Common-Sense (Federal) Common Law Adrift in a Statutory Sea, or Why *Grokster* Was a Unanimous Decision, 22 Santa Clara Computer & High Tech. L.J. 413, 434 (2006) ("[S]econdary liability in copyright is federal common law . . . .").

414. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 914 (2005).

415. See, e.g., id. ("Although '[t]he Copyright Act does not expressly render anyone liable for [another's] infringement,' these secondary liability doctrines emerged from common law principles and are well established in the law." (quoting Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 434 (1984))); see also Kalem Co. v. Harper Bros., 222 U.S. 55, 62–63 (1911) (explaining basis for defendant's indirect liability); Gershwin Publ'g Corp., v. Columbia Artists Mgmt., 443 F.2d 1159, 1161–62 (2d Cir. 1971) ("Although the Act does not specifically delineate what kind of degree of participation in an infringement is actionable, it has long been held that one may be liable for copyright infringement even though he has not himself performed the protected composition."); 3 Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 12.04[A] (2005) ("[A] long

providing the means for copyright infringement under these theories.[416] The most popular examples are the peer-to-peer file-sharing software companies Grokster and Napster.[417] In *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, the Court indicated that contributory liability should be analyzed in light of "rules of fault-based liability derived from the common law."[418]

The FTC appears to be using similar theories of responsibility and culpability. While some of the FTC's indirect-liability complaints do not specifically allege a wrongful "intent" for others to engage in deceptive or unfair acts, basic common law principles provide for imputed intent.[419] The FTC has thus followed the common law to push beyond direct theories of liability toward more indirect ones.

IV. TOWARD A MORE COMPLETE PRIVACY REGULATORY REGIME

The FTC has not fully exerted its powers or pushed the logical extensions of its theories. Until recently, the FTC has largely limited itself to the four corners of privacy policies, but it could readily expand beyond privacy policies, which have increasingly become less relevant in how consumers form their privacy expectations and manage their privacy across websites, apps, and other services.

The implications of the FTC's expansion of enforcement and shift to consumer expectations over company representations are profound. For example, regarding deception, given the FTC's refusal to allow companies to exploit consumer ignorance and create a false sense of trust through language and architecture, is it possible that the FTC could establish an affirmative duty on the part of companies to combat the ignorance and false assumptions of consumers? The FTC's actions certainly seem to be the stirrings of a much more complete and substantive regime than simply requiring companies to follow their promises.

---

series of cases under both the 1909 Act and the current Act imposes liability . . . for acts of infringement committed by others.").

416. E.g., A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1022, 1024 (9th Cir. 2001) (finding likelihood of successful copyright infringement claim against file-sharing software provider based on both contributory and vicarious liability).

417. *Grokster*, 545 U.S. at 919–20; *Napster*, 239 F.3d at 1011.

418. *Grokster*, 545 U.S. at 934–35.

419. See, e.g., id. (discussing jurisprudence of common law imputed intent); DeVoto v. Pac. Fid. Life Ins. Co., 618 F.2d 1340, 1347 (9th Cir. 1980) ("Tort law ordinarily imputes to an actor the intention to cause the natural and probable consequences of his conduct."); Restatement (Second) of Torts § 8A cmt. b (1965) ("If the actor knows that the consequences are certain, or substantially certain, to result from his act, and still goes ahead, he is treated by the law as if he had in fact desired to produce the result.").

A. *From Broken Promises to Broken Expectations*

Although the FTC began enforcing broken *promises* of privacy, its focus seems to have shifted to broken *expectations* of consumer privacy. The shift might seem subtle, but it is dramatic in effect. Instead of the core question being what was promised, which largely focuses on a company's language, the core question has become what was expected, which incorporates the universe of preexisting consumer backgrounds, norms, and dispositions, as well as elements of design, functionality, and other nonlinguistic factors besides privacy-related statements that shape a consumer's expectations.

The FTC could simply look at what a company's polices and design/architecture are and compare that with the company's actions. But it is not doing that. Instead, it seems to be taking consumers as it finds them, full of preexisting expectations, contextual norms, and cognitive limitations, and prohibiting companies from exploiting these assumptions and rational ignorance.

Social science research reveals that consumers do not read or understand privacy policies, are heavily influenced by the way choices are framed, and harbor many preexisting assumptions that are incorrect.[420] For example, according to one study, "64% [of the people surveyed] do not know that a supermarket is allowed to sell other companies information about what they buy" and 75% falsely believe that when "a website has a privacy policy, it means the site will not share my information with other websites and companies."[421]

If the FTC takes into account the growing evidence about how consumers form their expectations, then it could increasingly demand that companies engage in practices that will correct mistaken consumer assumptions, or at the very least not exploit such assumptions. Existing forms of notice might not be deemed sufficient because the empirical evidence shows that consumers are not really being notified.

The FTC has thus far pushed lightly into this territory. *In re Sears Holdings Management Corp.* involved a notice deemed inadequate because consumers were likely not to be aware of it. But the empirical evidence shows that traditional privacy policies are also not being read or under-

420. See, e.g., Solove, Privacy Self-Management, supra note 241, at 1883–88 (describing problems uninformed consumers have reading and comprehending privacy policies).

421. Joseph Turow et al., Open to Exploitation: American Shoppers Online and Offline 3 (June 2005) (unpublished manuscript), available at http://repository.upenn.edu/asc_papers/35 (on file with the *Columbia Law Review*); see also Joseph Turow et al., Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It 21 (Sept. 29, 2009) (unpublished manuscript), available at http://ssrn.com/abstract=1478214 (on file with the *Columbia Law Review*) (finding 62% of respondents think following statement is true and 16% "don't know": "If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission").

stood.[422] The FTC has not followed the empirical evidence to the fullest extent. But the foundation and rationale certainly exist for the FTC to do so. And if it were to do so, many common practices with regard to notice and choice might be deemed deceptive.

Under this view of deception, the deception would not stem from any malice on the part of companies. The deception would simply be the effect of particular practices on consumers with flawed assumptions and cognitive biases.

One of the issues with the FTC's gradual embrace of "deceptive effect" is that it somewhat conflicts with portions of the FTC's formal policy statement on deception.[423] In discussing the materiality of representations, the FTC stated the following:

> Where the seller knew, or should have known, that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false, materiality will be presumed because the manufacturer intended the information or omission to have an effect. Similarly, when evidence exists that a seller intended to make an implied claim, the Commission will infer materiality.[424]

This statement seems to focus on the intent of the company. Yet elsewhere in the FTC's statements on deception, and in its jurisprudence, the FTC focuses almost squarely on the effect of a company's act on a consumer.[425] This focus would seem to provide that a company's practice could be deceptive regardless of whether the company intended to mislead the consumer.

The FTC should clarify its deceptive trade practices jurisprudence by clearly defining the role that a company's knowledge of deception or intent to deceive plays in liability under Section 5. Given the theories articulated in the FTC's complaints, it would be reasonable for the FTC to explicitly create two different categories of deception: (1) deceptive intent and (2) deceptive effect. Deceptive intent could require that the company knew or should have known that its actions would likely deceive the consumer. A theory of "deceptive effect" would not require intent to deceive or knowledge of deception, but would involve cases where common consumer mistaken assumptions and cognitive biases lead to incorrect understandings about a company's privacy practices. Companies would have an obligation to use reasonable means to correct wrong consumer assumptions and account for the cognitive issues. Companies

---

422. See, e.g., Solove, Privacy Self-Management, supra note 241, at 1886 (noting "people operate under woefully incorrect assumptions" about their privacy).

423. Letter from James C. Miller III to Hon. John D. Dingell, supra note 42, app. at 176.

424. Id. app. at 182.

425. E.g., id. app. at 177 ("The Commission believes that to be deceptive the representation, omission or practice must be likely to mislead reasonable consumers under the circumstances.").

would not be required to correct all misnomers and fix all cognitive difficulties, but they would no longer be able to ignore them and gain an advantage through their existence.

B. *Beyond the Four Corners of Privacy Policies*

The FTC could push more boldly beyond the four corners of privacy policies to examine holistically the context of a consumer's experience with a company. The FTC has already moved in this direction, consistent with its other decades-old advertising cases that do not limit deception to specific forms. The FTC has made it clear that it looks beyond privacy policies to find promises and representations in any context that would be relevant to consumers. A review of the boilerplate language is no longer the end of the inquiry, as actions for deception have been based on expectations created by marketing materials, user manuals,[426] pop-up windows,[427] emails,[428] privacy settings,[429] icons,[430] and various other aspects of a website's or software program's design.[431] The actions also demonstrate that the FTC looks at design, architecture, contextual norms, and the preexisting knowledge likely held by consumers to determine consumer expectations.

The FTC has further clarified its deception jurisprudence, stating that while express representations by themselves can be deceptive, implied representations can also be found deceptive by determining mean-

426. E.g., HTC Complaint, supra note 215, at 8 (asserting HTC user manuals created false expectation that users would be notified when third party application required access to personal information).

427. E.g., Aspen Way Complaint, supra note 227, at 4 (alleging pop-up notices deceptively led consumers to believe they were from trusted software providers).

428. E.g., Artist Arena Complaint, supra note 303, at 13 (alleging defendant falsely represented through emails that it would not collect personal information from children without parental consent).

429. E.g., Facebook Complaint, supra note 247, at 9 (alleging Facebook failed to adequately disclose changes to privacy settings, which constituted deceptive act).

430. E.g., ControlScan Complaint, supra note 386, at 8–9 (alleging ControlScan failed to ensure companies receiving verification seals qualified for them and dates displayed on seals falsely suggested daily review of company practices).

431. E.g., Path Complaint, supra note 303, at 7–8 (alleging defendant misrepresented privacy policy and improperly gathered personal information of minors); Complaint for Civil Penalties and Other Relief at 9–10, United States v. Google, Inc., No. CV 12-04177 HRL (N.D. Cal. Nov. 20, 2012) [hereinafter Google II Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmpt exhibits.pdf (on file with the *Columbia Law Review*) (alleging violation of FTC Act through overriding Safari browser's opt-out policy for online data collection through cookies); Complaint at 3, In re Scanscout, Inc., FTC File No. 102 3185, No. C-4344 (F.T.C. Dec. 14, 2011), available at http://www.ftc.gov/sites/default/files/documents/cases/2011/12/111 221scanscoutcmpt.pdf (on file with the *Columbia Law Review*) (alleging violation of FTC Act by misrepresenting users' choice to opt out of online data collection); In re Chitika, Inc., 151 F.T.C. 494, 497–98 (2011) (complaint) (alleging defendant violated FTC Act by collecting user data without consent).

ing "through an examination of the representation itself, including an evaluation of such factors as the entire document, the juxtaposition of various phrases in the document, the nature of the claim, and the nature of the transaction."[432] The FTC also stated that it might "require extrinsic evidence that reasonable consumers reach the implied claims. In all instances, the Commission will carefully consider any extrinsic evidence that is introduced."[433]

A recent example of the FTC's move beyond privacy policies is *In re HTC America, Inc.*[434] There, the FTC considered privacy and security representations made in a user manual for mobile devices regarding the installation of software, as well as representations made via the mobile device's user interface.[435] Specifically, the user interface that allows users to report a software error to HTC also allows users to "add location data" to the submission by checking a button. According to the FTC, "Through this user interface, HTC represents that the user's location data will not be sent to HTC if the user does not check the button marked 'Add location data.'"[436]

The FTC filed a complaint against Path, a social networking service, under a similar theory of deceptive user interfaces. Specifically, the FTC alleged that, in its social network application for a mobile operating system, a site user was given three options upon clicking into the newly added "Add Friends" interface: "'Find friends from your contacts;' 'Find friends from Facebook;' and 'Invite friends to join Path by email or SMS.' . . . The new feature allowed the user to search for friends to add to the user's network."[437] According to the FTC, the user interface served as a representation that the user's contacts would not be collected and stored unless the user selected the "Find friends from your contacts" option.[438]

In *United States v. Google, Inc.*, the FTC charged Google with wrongfully delivering targeted advertisements based upon data gathered in violation of a user's privacy settings.[439] In that case, the FTC looked to privacy settings and instructions on how to use those settings, which were outside of the privacy policy. Specifically, the FTC alleged that in its "browser instructions," Google represented to users of the Safari web

---

432. Letter from James C. Miller III to Hon. John D. Dingell, supra note 42, app. at 176.

433. Id.

434. HTC Complaint, supra note 215, at 7–8.

435. Id.

436. Id. at 7.

437. Path Complaint, supra note 303, at 4.

438. Id. ("Contrary to the representation made by the Path App's user interface . . . , Defendant automatically collected and stored personal information from the user's mobile device contacts even if the user had never selected the 'Find friends from your contacts' option.").

439. Google II Complaint, supra note 431, at 11.

browser that "if they did not change the default [privacy-related cookie] setting, Google would not place DoubleClick Advertising Cookies on a user's browser, collect interest category information from or about the user, or serve targeted advertisements to the user."[440]

In *In re Facebook, Inc.*, the FTC alleged that the company's privacy settings were deceptive because they gave users the impression, which was supported by language elsewhere on the site such as the privacy homepage, that users could utilize the settings to control who saw their profile information.[441] The FTC further alleged that changes to the privacy settings were deceptive because they no longer functioned in the way that they appeared to.[442]

Marketing and other "external" representations have also been important in the FTC's privacy jurisprudence. Notably, in determining the relevant privacy-related promises made by Facebook, the FTC considered statements the company made on its official blog.[443]

In *In re US Search, Inc.*, the FTC looked to standard individual communications with consumers who inquired about a "PrivacyLock" service to find deceptive communications.[444] In *In re Rite Aid Corp.*, the FTC considered general statements made in a marketing brochure seeking consumers' medical history a deceptive privacy statement.[445]

These cases have made it clear that the question of what constitutes a deceptive trade practice is holistic. Not only does the FTC consider representations beyond what exists in a privacy policy, but it considers consumer expectations as well. This raises a number of interesting questions. The first is the extent to which other representations can contradict explicit representations in the privacy policy. While contract law tends to give great weight to the boilerplate terms of a contract, the FTC does not appear to recognize any kind of significant presumption to exculpatory representations buried in dense legalese that run contrary to

---

440. Id. at 8–9.

441. Facebook Complaint, supra note 247, at 6 ("Facebook has represented, expressly or by implication, that, through their Profile Privacy Settings, users can restrict access to their profile information to specific groups . . . . In truth . . . users could not restrict access to their profile information to specific groups, such as 'Only Friends' . . . through their Profile Privacy Settings.").

442. Id. at 9 ("Facebook failed to disclose . . . that . . . users could no longer restrict access to their [profile information] by using privacy settings previously available to them. Facebook also failed to disclose . . . that the December Privacy Changes overrode existing user privacy settings that restricted access to a user's [profile information].").

443. Id. at 12.

444. Complaint at 2–3, In re US Search, Inc., FTC File No. 102 3131, No. C-4317 (F.T.C. Mar. 14, 2011), available at http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110325ussearchcmpt.pdf (on file with the *Columbia Law Review*) (alleging company violated FTC Act by deceiving buyers of privacy product).

445. Rite Aid Complaint, supra note 262, at 2 ("Although you have the right not to disclose your medical history, Rite Aid would like to assure you that we respect and protect your privacy.").

other representations or consumer expectations.[446] Additionally, given the predominance of privacy policies for both websites and applications, do consumers expect companies that collect personal information to have some form of a privacy policy? If so, is an application's failure to have a privacy policy a deceptive practice? That would seem to create a baseline protection for consumers.

Finally, given the universe of potential privacy-related statements the FTC could have (and has) drawn from to find deception, has there been a shift from explicit, insular representations to larger framing effects that create consumer trust? In other words, it appears that what a company has promised is simply one factor in a larger approach to determining whether a company has been deceptive. The FTC looks at architecture, shared norms, and cultural assumptions likely held by consumers to determine consumer expectations. This framework developed by the FTC logically would also consider any statement made by the company that would materially contribute to the creation of trust on the part of the consumer, including press releases, advertising, and perhaps even off-the-cuff remarks in interviews, such as when Mark Zuckerberg assured Facebook users that "[p]rivacy is very important to us."[447] Such an approach looks far beyond simple broken promises to a potentially substantive regime where industry standards that have an effect on consumer expectations are now incorporated into the deceptive contexts.

C. *Developing Substantive Rules*

The FTC has moved beyond promises to substantive privacy protections, evolving from an almost entirely self-regulatory regime to something that resembles more of an actual regulatory regime. In the areas of data security and notice, the FTC has already set forth a series of rather detailed requirements. As this Article discussed above, these requirements are based in common industry practices.

The past fifteen years have witnessed a profound development within industry regarding privacy. A set of basic practices has emerged. This set has been spurred by several factors. The first factor is the peer pressure effect. Many companies implemented privacy practices because other companies were doing so. The widespread use of privacy policies developed this way.

---

446. See, e.g., Sears Complaint, supra note 243, at 5 (alleging company's failure to adequately disclose extent of data collection constituted deceptive practice).

447. John Paczkowski, Facebook CEO Mark Zuckerberg in the Privacy Hot Seat at D8, All Things D (June 2, 2010, 4:48 PM), http://allthingsd.com/20100602/mark-zuckerberg-session/ (on file with the *Columbia Law Review*); see also Privacy a Facebook Priority, Dawn.com (Oct. 18, 2010, 12:00 AM), http://dawn.com/2010/10/18/privacy-a-facebook-priority/ (on file with the *Columbia Law Review*) ("'Privacy, I would say, is the number one most important thing for our company, and we're always listening to feedback,' Randi Zuckerberg, the sister of Facebook co-founder Mark Zuckerberg, said on the first day of the GITEX information and communication technology exhibition.").

Second, regulation in certain industries prompted the practices to develop more broadly. Regarding privacy policies, GLBA and other statutes have made privacy policies more common by forcing a wide array of companies to have them. This, in tandem with the peer pressure effect, worked to make more companies adopt privacy policies. The substance of the standards was influenced by regulation. The HIPAA Security Rule and some state laws helped define specific security practices that became the norm.

Third, the Safe Harbor Agreement and the need to comply with the privacy laws of other countries pushed companies to develop standards.

Fourth, the rise of the Chief Privacy Officer and Chief Security Officer positions have led to the development of standards. These professionals read common bodies of literature, share information in conferences, and bring back consensus knowledge to their institutions.

Fifth, the rise of lawyers and consultants specializing in privacy and data security has contributed to the development of industry norms, as these practitioners advise companies about the practices of other companies.

All of these factors, and more, have resulted in a sharing and pooling of knowledge, and consensus has developed around certain practices. Norms and customs are emerging.

As these norms and customs develop, the FTC can readily draw from them and enforce them as substantive rules. There are at least two ways this can be justified. First, the FTC can view them as implied terms in privacy policies. Even if not stated, these common practices could become implied because what is "reasonable" is often benchmarked by such practices.

Second, the FTC can view them as expected by consumers because such practices are common, and consumers usually assume that companies generally follow common practices. If the FTC takes consumers as they are—with flawed assumptions—then the onus shifts to companies to make sure that such assumptions are corrected. Companies can deviate from common practices only by issuing a much more salient notice.

In this way, the FTC could gradually impose a set of sticky default practices that companies can only deviate from if they very explicitly notify consumers. As the privacy law field develops, so will industry standards and practices, and this development in turn will justify the FTC's enforcement of these standards and practices.

The FTC could see its role in addressing these issues by nudging—and sometimes pushing—companies to avoid exploiting the fact that people have misconceptions and that people do not read policies.[448]

---

448. Cf. Path Consent Decree & Order, supra note 374, at 12 (ordering company to provide more detailed disclosure of categories of information collected).

Increasingly, privacy policies are shorter and much less detailed in an effort to make them quick to read and simple to understand. The problem is that these policies really do not say much. The FTC can readily add flesh and sinew to these simple, barebones claims. Essentially, the FTC could push industries toward adopting more uniform privacy policies. Despite variations in language, the FTC could impose a standard set of meanings for key components, such as access and correction rights, data collection, data sharing, data security, and so on.

In some cases, the FTC could simply require companies to conform to industry norms. For example, a number of apps lack privacy policies. The FTC could conceivably conclude that the failure to have a privacy policy is either deceptive or unfair because consumers now expect a privacy policy. Unless consumers are explicitly notified that there is no privacy policy, the FTC could conclude that consumers are misled because they are operating under the assumption that the apps have privacy policies roughly akin to those of other companies.

For example, outside the privacy context, the FTC has been very active in articulating standards for "clear and conspicuous" disclosures to protect consumers and ensure the integrity of online relationships. Yet, save a few egregious exceptions,[449] it has surprisingly failed to explicitly include privacy notices within this requirement. For example, the FTC recently released a comprehensive guide to effective digital advertising disclosures.[450] The report states:

> Required disclosures must be clear and conspicuous. In evaluating whether a disclosure is likely to be clear and conspicuous, advertisers should consider its placement in the ad and its proximity to the relevant claim. The closer the disclosure is to the claim to which it relates, the better. Additional considerations include: the prominence of the disclosure; whether it is unavoidable; whether other parts of the ad distract attention from the disclosure; whether the disclosure needs to be repeated at different places on a website; whether disclosures in audio messages are presented in an adequate volume and cadence; whether visual disclosures appear for a sufficient duration; and whether the language of the disclosure is understandable to the intended audience.[451]

The report makes no mention of privacy policies as disclosures, despite the commonly argued notion that privacy policies are simply notices.

---

449. See, e.g., DesignerWare Complaint, supra note 227, at 6 (alleging company's failure to disclose installation of geophysical tracking software constitutes deceptive practice); Sears Complaint, supra note 243, at 5 (alleging failure to adequately disclose extent of data collection constitutes deceptive practice).

450. FTC, .Com Disclosures: How to Make Effective Disclosures in Digital Advertising (2013), available at http://www.ftc.gov/os/2013/03/130312dotcomdisclosures.pdf (on file with the *Columbia Law Review*).

451. Id. at i–ii.

The FTC could be particularly effective with its "clear and conspicuous" requirement in areas where privacy is threatened by promises or representations in the design of a technology, form, or communication, or lack of information. The report goes on to counsel:

> If a disclosure is necessary to prevent an advertisement from being deceptive, unfair, or otherwise violative of a Commission rule, and it is not possible to make the disclosure clearly and conspicuously, then that ad should not be disseminated. This means that if a particular platform does not provide an opportunity to make clear and conspicuous disclosures, then that platform should not be used to disseminate advertisements that require disclosures.[452]

The FTC already requires disclosures to remedy a number of different omissions or misrepresentations, including connections between endorsers and sellers of products that might affect the credibility of the endorsement and whether bloggers are receiving material benefits in exchange for reviewing a product or service.[453] The FTC might even consider requiring companies to "substantiate" their privacy promises in the same way that it does for statements in advertising regarding "objective assertions about the item or service advertised."[454] If a company promises that users can use privacy settings to control who sees their information, the FTC would have some precedent for requiring that the company "substantiate" that it is keeping this promise.

Indeed, a privacy substantiation requirement could be an important aspect of the FTC's new "privacy by design" approach,[455] which would require companies to engage in ex ante procedures designed to ensure that promises are valid at the time they are made, rather than after-the-fact enforcement of broken promises. In this sense, privacy substantiation would be entirely consistent with a privacy-by-design approach. These are just examples of how the FTC could justify developing a more substantive requirement for notice. More broadly, the FTC could start imposing the basic Fair Information Practices against companies, since these have become rather common and expected by consumers. The more the FTC focuses on consumer expectations, the more it can justify

---

452. Id. at iii.

453. E.g., 16 C.F.R. § 255.5 (2013); Press Release, FTC Publishes Final Guides Governing Endorsements, Testimonials, FTC (Oct. 5, 2009), http://www.ftc.gov/opa/2009/10/endortest.shtm (on file with the *Columbia Law Review*); Tom Gara, Paid Tweeters Beware: The FTC Is Watching, Wall St. J.: Corp. Intelligence (Mar. 12, 2013, 5:37 PM), http://blogs.wsj.com/corporate-intelligence/2013/03/12/paid-tweeters-beware-the-ftc-is-watching/ (on file with the *Columbia Law Review*).

454. In re Thompson Med. Co., 104 F.T.C. 648 app. at 839 (1984) (FTC Policy Statement Regarding Advertising Substantiation), aff'd, 791 F.2d 189 (D.C. Cir. 1986).

455. FTC, Protecting Consumer Privacy, supra note 78, at vii ("Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.").

rejecting various privacy practices that are likely to take consumers by surprise or that consumers might find confusing.

With a focus on consumer privacy expectations; an embrace of empirical evidence about consumer assumptions and behavior; a willingness to look beyond privacy policies to the entire architecture and design of websites, software, and devices; and a receptivity to imposing consensus norms, practices, and standards, the FTC is poised to take even bolder steps toward developing a thick, meaningful, and broad approach to regulating privacy in the United States.

CONCLUSION

The landscape of United States privacy law has been gap riddled and often confounding. Self-regulation has reigned supreme over many industries. And yet, the FTC has risen to act as a kind of data protection authority in the United States. Despite having limited jurisdiction and limited resources, the FTC has created a body of common law doctrines through complaints, consent decrees, and various reports and other materials. The FTC's jurisprudence has developed in some classic common law patterns, evolving from general to more specific standards, gradually incorporating more qualitative judgments, imposing certain default standards, and broadening liability by recognizing contributory liability.

In the future, the FTC can be even bolder. The FTC has built a foundation from which it can push more toward focusing on consumer expectations than on broken promises, move beyond the four corners of privacy policies into design elements and other facets of a company's relationship with consumers, and develop and establish even more substantive standards.

Through a gradual process akin to that of common law, the FTC has developed a federal body of privacy law, the closest thing the United States has to omnibus privacy regulation. Unlike the top-down approach of the European Union and many countries around the world, the FTC's approach has been bottom up—a series of small steps. Because of these modest movements, and the fact that the FTC's privacy doctrines have not been developed in judicial decisions, they have been largely ignored by the legal academy and are also often underappreciated in the United States and abroad.

Taking stock of what the FTC has been doing, the doctrines it is developing, and the potential future directions it can take reveals that the FTC at least deserves greater study and appreciation. The FTC is far more than a rubber stamp on self-regulation and far more than a mere enforcer of broken promises. This Article is hopefully the start of a more sustained examination of the FTC, the body of law it has developed, and the future directions that law can take.