San Diego Law Review

Volume 48 | Issue 3 Article 4

8-1-2011

The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices

Andrew Serwin

The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices

ANDREW SERWIN*

TABLE OF CONTENTS

---

* Andrew B. Serwin is the founding chair of the Privacy, Security, and Information Management Practice and a partner in the San Diego, Del Mar and Washington, D.C. offices of Foley & Lardner LLP. Mr. Serwin is recognized as one of the nation's leading privacy and information security lawyers. Mr. Serwin was named to *Security Magazine*'s "25 Most Influential Industry Thought Leaders" for 2009 and is the only law firm lawyer to receive this award. He was ranked second in the 2010 *Computerworld* survey of top global privacy advisors and is ranked by *Chambers USA*—2009 through 2011—in the area of National Privacy & Data Security.

Mr. Serwin has written a number of books, including the leading treatise on privacy *Information Security and Privacy: A Guide to Federal and State Law and Compliance*, a 4000 page treatise that examines all aspects of privacy and security laws, published by Thomson-West. The treatise has been cited as authority by the Fourth Circuit in *Ostergren v. Cuccinelli*, 615 F.3d 263, 279 (4th Cir. 2010). He is also the author of *Information Security and Privacy: A Guide to International Law and Compliance*, as well as several leading law review articles: *Privacy 3.0—The Principle of Proportionality* and *Poised on the Precipice: A Critical Examination of Privacy Litigation*, the latter of which was cited by *Hammond v. Bank of New York Mellon Corp.*, No. 08 Civ. 6060, 2010 WL 2643307, at *2 (S.D.N.Y. June 25, 2010), and *Joseph Oat Holdings, Inc. v. RCM Digesters, Inc.*, No. 09-4208, 2010 WL 5065037, at *7 (3d Cir. Dec. 13, 2010).

I. INTRODUCTION

We live in a society that is marked by rapid technological advances. These new technologies present significant benefits to consumers, but these benefits in many cases are predicated on the disclosure and sharing of information. Balancing consumer protection efforts while simultaneously providing the appropriate incentives for innovation is one of the biggest challenges faced by regulators.

The Federal Trade Commission (FTC) sets the agenda for consumer protection in the United States, and privacy is a prominent part of this agenda. Despite its now central role in consumer protection, the FTC started as an entity focused on protecting business competitors that did not have a consumer protection portfolio. The origins of the FTC, including its original jurisdictional scope, required Congress to significantly amend the Federal Trade Commission Act (FTCA) to provide the FTC with authority to address harms to consumers.[1] This was achieved by giving the FTC expanded ability to act to stop "deceptive" and "unfair" acts or practices. Over time, both the courts and the FTC have clarified the FTC's jurisdiction to protect consumers, and the FTC has taken an increased role in privacy enforcement, first through cases alleging deception, and then through cases relying upon the FTC's unfairness authority.[2]

The FTC recently issued guidance, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, which identified the successes the FTC has had in privacy enforcement, including its continuing efforts with international outreach,[3] as well as some continuing issues with current enforcement and data protection regimes. As noted by the opening sentences of the report:

> In today's digital economy, consumer information is more important than ever. Companies are using this information in innovative ways to provide consumers with new and better products and services. Although many of these companies manage consumer information responsibly, some appear to treat it in an irresponsible or even reckless manner. And while recent announcements of privacy

1. *See generally* Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2006).
2. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS 3–6 (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
3. *Id.* at 12 ("In recent years, the Commission has continued to employ a range of tools—including law enforcement, consumer and business education, policymaking, and international outreach—in pursuing its consumer privacy initiatives.").

> innovations by a range of companies are encouraging, many companies—both online and offline—do not adequately address consumer privacy interests.[4]

Said differently, although some companies have voluntarily taken steps to improve privacy and adopt best practices, not all companies have. In light of this, the report proposes a new framework for companies in order to further encourage the development of best practices and self-regulation and to guide Congress.[5] It also places the FTC's prior privacy enforcement efforts in two categories—the "notice-and-choice" and "harm-based" models.[6] Although no prior article has attempted to correlate these concepts to the FTC's jurisdiction, as argued below, the notice-and-choice model corresponds to the FTC's deception authority, and the harm-based model corresponds to its unfairness authority. The FTC's recent report also recognized that technological changes in society may call these constructs into question and ultimately suggested a new framework—"privacy-by-design."[7]

The FTC is not the only entity looking at how to solve these issues. Several groups and commentators have made suggestions regarding what model of privacy will help change the path of privacy. These include models based upon accountability, as well as models that focus on restrictions on data processing, also at times known as use-limitations models. Another proposed structure is one I identified in 2008, known as Privacy 3.0, which relies upon proportionality to identify appropriate restrictions on processing and accountability.[8]

This Article will first examine the origins of the FTC, then review the current structure and jurisdiction of the FTC for consumer protection and also track the efforts to define the FTC's authority over deceptive and unfair practices. It will examine the FTC's use of its deception and unfairness authority in privacy enforcement cases, then examine three proposed theoretical models for privacy, and finally propose a framework that would provide guidance for industry and permit privacy issues to be more proactively addressed. The framework will build upon best practices and the privacy-by-design concepts by creating a framework based upon risk of harm, or sensitivity. The framework would be a voluntary program,

---

4. *Id.* at i.

5. *Id.* ("This proposal is intended to inform policymakers, including Congress, as they develop solutions, policies, and potential laws governing privacy, and guide and motivate industry as it develops more robust and effective best practices and self-regulatory guidelines.").

6. *Id.* at iii.

7. *Id.* at v. "In addition, both models have struggled to keep pace with the rapid growth of technologies and business models that enable companies to collect and use consumers' information in ways that often are invisible to consumers." *Id.* at iii.

8. Andrew B. Serwin, *Privacy 3.0—The Principle of Proportionality*, 42 U. MICH. J.L. REFORM 869, 900 (2009).

administered by the FTC, but it would offer those businesses that choose to enter the program a safe harbor from enforcement if the safe harbor requirements are met. The safe harbor proposal in this Article is a new element, but one that would likely further encourage companies to adopt best practices.

II. WHAT ARE THE ISSUES PEOPLE ARE CONCERNED ABOUT?

The FTC's recent report, which was in part based upon a series of roundtables, stated the current privacy issues as follows:

> Stakeholders emphasized the need to improve transparency, simplify the ability of consumers to exercise choices about how their information is collected and used, and ensure that businesses take privacy-protective measures as they develop and implement systems. At the same time, commenters and participants urged regulators to be cautious about restricting the exchange and use of consumer data in order to preserve the substantial consumer benefits made possible through the flow of information. Participants noted, for example, that the acquisition, exchange, and use of consumer data not only helps to fund a variety of personalized content and services, but also allows businesses to innovate and develop new products and services that offer consumers convenience and cost savings.[9]

Thus, the balance that the FTC is trying to strike is to protect consumers in an environment where the FTC perceives notice-and-choice and harm-based models to be failing, while simultaneously not stifling consumer choice or innovation.

Although the United States is clearly the focus for the FTC, it is also equally clear that the FTC recognizes the global nature of these issues and is actively trying to increase coordination and cooperation with foreign governments. As recognized by the report:

> International enforcement and policy cooperation also has become more important with the proliferation of complex cross-border data flows and cloud computing. To protect consumers in this rapidly changing environment, the FTC participates in various international policy initiatives, including those in multilateral organizations such as the OECD and the Asia-Pacific Economic Cooperation forum ("APEC").
>
> Within the OECD, the FTC has participated in the Working Party on Information Security and Privacy, which led the development of the 2007 OECD Council's Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy . . . . In APEC, the FTC has been actively involved in an initiative to establish a self-regulatory framework governing the privacy of data transfers throughout the APEC region.[10]

---

9. FED. TRADE COMM'N, *supra* note 2, at iv.

10. *Id.* at 17 (footnote omitted). The FTC also noted that in 2007 there was a recommendation from the OECD that OECD member countries should foster the

III. THE FTC—A HISTORICAL PERSPECTIVE

A. The Formation of the FTC

The FTC was originally created in 1914 in order to protect competition among businesses. The original FTCA was enacted concurrently with the Clayton Act, the nation's first antitrust law, which links the FTC's original focus to ensuring a level playing field for businesses rather than the consumer protection focus we see today.[11] The original powers of the agency certainly did not include authority outside the examination of anticompetitive actions and antitrust violations. If one were to view what the FTC was in 1914, it would have primarily consisted of what is now known as the Bureau of Competition.[12]

This stands in stark contrast to the FTC of today, which on its website brands itself as the "nation's consumer protection agency."[13] The FTC's self-professed agenda is "to prevent fraud, deception, and unfair business practices in the marketplace."[14] The change in focus for the FTC to include consumer protection was achieved via amendments to section 5 of the FTCA in 1938 when the FTCA was extended to cover consumers, primarily through the addition of authority to address unfair and deceptive acts or practices.[15] The 1938 amendments also granted the FTC more

---

establishment of an informal network of privacy enforcement authorities and cooperate with each other to address cross-border issues arising from enforcement of privacy laws. *See* ORG. FOR ECON. CO-OPERATION & DEV., OECD RECOMMENDATION ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS PROTECTING PRIVACY 7 (2007), *available at* http://www.oecd.org/dataoecd/43/28/38770483.pdf; *see also* Press Release, Fed. Trade Comm'n, FTC and Internatonal Privacy Enforcement Authorities Launch Global Privacy Cooperation Network and Website (Sept. 21, 2010), *available at* http://www.ftc.gov/opa/2010/09/worldprivacy.shtm.

11. Federal Trade Commission Act of 1914, Pub. L. No. 63-203, 38 Stat. 717 (codified as amended at 15 U.S.C. §§ 41–58 (2006)); Clayton Antitrust Act of 1914, Pub. L. No. 63-212, 38 Stat. 730 (codified as amended at 15 U.S.C. §§ 12–27 (2006) and 29 U.S.C. §§ 52–53 (2006)).

12. *About the Bureau of Competition*, FED. TRADE COMM'N, http://www.ftc.gov/bc/about.shtm (last modified May 20, 2009).

13. *Welcome to the Bureau of Consumer Protection*, FED. TRADE COMM'N, http://www.ftc.gov/bcp/index.shtml (last modified Feb. 1, 2011).

14. *Id.*

15. FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 235, 244 (1972) ("The amendment added the phrase 'unfair or deceptive acts or practices' to the section's original ban on 'unfair methods of competition' and thus made it clear that Congress, through § 5, charged the FTC with protecting consumers as well as competitors. The House Report on the amendment summarized congressional thinking: '[T]his amendment makes the consumer, who may be injured by an unfair trade practice, of equal concern, before the law, with the merchant or manufacturer injured by the unfair methods of a dishonest competitor.'" (quoting H.R. REP. NO. 75-1613, at 2–3 (1937))); *see also* FTC v. Colgate-Palmolive Co., 380 U.S. 374, 384 (1965); Guziak v. FTC, 361 F.2d 700, 703 (8th Cir. 1966); S. REP. NO. 74-1705, at 2–3 (1936).

flexibility in addressing practices before they reached a conclusion and had a significant and long-term effect.[16]

B. The History of Privacy Enforcement

The FTC's first foray into consumer privacy was in the 1970s when it was granted authority to enforce the Fair Credit Reporting Act, or FCRA as it is commonly known.[17] The FTC has subsequently expanded its efforts to protect consumers' privacy through enforcement as well as other initiatives. These efforts have been focused on two models: the notice-and-choice model and the harm-based model.[18]

For the FTC, the notice-and-choice model began in 2000, with the FTC recommending that Congress require businesses to comply with the fair information practice principles, which include notice-and-choice.[19] Congress did not pass this legislation, so the FTC focused initially on raising public awareness, encouraging self-regulation, and also bringing cases under section 5 based upon its deception authority.[20] Deception, as

16. Fashion Originators' Guild of Am. v. FTC, 312 U.S. 457, 466 (1941) ("And as previously pointed out, it was the object of the Federal Trade Commission Act to reach not merely in their fruition but also in their incipiency combinations which could lead to these and other trade restraints and practices deemed undesirable."); Keasbey & Mattison Co. v. FTC, 159 F.2d 940, 946 (6th Cir. 1947); Ford Motor Co. v. FTC, 120 F.2d 175, 182 (6th Cir. 1941).

17. FED. TRADE COMM'N, *supra* note 2, at ii.

18. *Id.* at iii.

19. *Id.* at D-1.

20. The FTC noted:

> In 2000, the Commission reported to Congress that, although there had been improvement in industry self-regulatory efforts to develop and post privacy policies online, only about one-quarter of the privacy policies surveyed addressed the four fair information practice principles of notice, choice, access, and security. Accordingly, a majority of the Commission concluded that legislation requiring online businesses to comply with these principles, in conjunction with self-regulation, would allow the electronic marketplace to reach its full potential and give consumers the confidence they need to participate fully in that marketplace. Although Congress did not enact the recommended legislation, the Commission's work during this time—particularly its surveys, reports, and workshops—raised public awareness about consumer privacy and led companies to examine their information collection practices and to post privacy policies. It also encouraged self-regulatory efforts designed to benefit consumers, improvements in privacy-enhancing technologies, and the creation of online privacy certification programs.
>
> During this period, the Commission also used its Section 5 authority to bring actions against companies that engaged in unfair or deceptive information practices. Most of these early cases involved deceptive statements in companies'

noted below, focuses on what "material" information the consumer was or was not told, particularly where the deception impacts a consumer's choice regarding goods or services. Moreover, although injury is a factor that is considered in deception cases, the analysis of injury is part of an examination of whether the allegedly misleading information was material, and actual injury is not required. Instead, the FTC must simply show that consumers are "likely to suffer injury from a material misrepresentation."[21]

The second enforcement model, the harm-based approach, represented a departure from the notice-and-choice model. Although the FTC continued to use deception in its cases, later cases focused more on actual consumer injury—typically resulting from an alleged breach—and the FTC began instead to rely more on its unfairness authority. As discussed below, the FTC's unfairness authority does not focus on what was told to the consumer but rather whether the consumer suffered "substantial" injury.[22]

Both models have faced criticism, including that the notice-and-choice model has led to lengthy and incomprehensible privacy statements and that the harm-based model does not adequately reflect all potential harms from privacy concerns. In addition, both models suffer shortcomings in adapting to rapid changes in technology.[23] However, these models, despite their criticisms, are key to understanding the FTC's pattern of enforcement and beginning the discussion on the appropriate theoretical model for the future.

IV. THE FTC'S JURISDICTION

Understanding the main grounds for FTC actions, including those that are not regularly at issue in privacy matters, is helpful in understanding the overall basis of FTC actions. There are a number of statutes that the FTC has been charged with enforcing, but the main source of FTC jurisdiction is based upon "unlawful" practices under the FTCA, and the two main bases for finding a practice to be unlawful are sections 5 and

> privacy notices about their collection and use of consumers' data. The legal theories in these early enforcement actions highlighted, in particular, the fair information practice principles of notice and choice (the "notice-and-choice approach"). Collectively, the Commission's policy and enforcement efforts underscored its emphasis on the concepts of transparency and accountability for information practices.

Id. at 8–9 (footnotes omitted).

21. Cliffdale Assocs., Inc., 103 F.T.C. 110, 166 (1984).

22. *See, e.g.*, FTC v. Accusearch Inc., 570 F.3d 1187, 1193 (10th Cir. 2009) (quoting 15 U.S.C. § 45(n) (2006)).

23. FED. TRADE COMM'N, *supra* note 2, at iii.

12 of the FTCA, also known as 15 U.S.C. §§ 45 and 52, respectively.[24] Section 5 prohibits deceptive and unfair acts or practices, and section 12 prohibits false advertisements.[25] The FTC also has responsibility for enforcement of a number of other laws, including the FCRA, one of the United States' first federal privacy laws, as well as others such as Gramm-Leach-Bliley (GLB) and the Children's Online Privacy Protection Act (COPPA).[26]

Although these other grounds for enforcement can have implications for privacy, the main focus of the FTC, and consequently of this Article, will be section 5 and the FTC's authority regarding deception and unfair practices or acts.

V. UNDERSTANDING THE THEORETICAL BASIS OF THE FTC'S PRIVACY ENFORCEMENT

Before the FTC's deception and unfairness authority are examined in detail, the theory underlying the FTC's prior thinking, as well as privacy laws generally, should be explored to help provide a framework for the analysis of section 5 and the FTC's enforcement cases.

In prior works I have identified the first theoretical construct of privacy as originating in a famous Warren and Brandeis law review article, *The Right to Privacy*, which is characterized by "the right to be let alone."[27] I have conceptualized this period as "Privacy 1.0," and the driving concern at the time regarding privacy was the technological advances of the time, including the instant camera.[28] Notably, Warren

24. *See* 15 U.S.C. §§ 45, 52 (2006).

25. *Id.* Like many state versions of the FTCA, a false advertisement that violates section 12 is both independently unlawful and a violation of section 5. 15 U.S.C. § 52(b); *see also* CAL. BUS. & PROF. CODE §§ 17200, 17500 (West 2008).

26. FED. TRADE COMM'N, *supra* note 2, at ii, 4; *Privacy and Security*, FED. TRADE COMM'N, http://www.ftc.gov/privacy (last visited Aug. 31, 2011); *see* Fair Credit Reporting Act, Pub. L. No. 91-508, § 106, 84 Stat. 1114, 1128 (1970) (codified as amended in scattered sections of 15 U.S.C.); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 & 15 U.S.C.); Children's Online Privacy Protection Act of 1998, Pub. L. No. 106-170, 112 Stat. 2681 (codified as amended at 15 U.S.C. §§ 6501–6505 (2006)).

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

28. I previously noted:

> While privacy was not invented by Warren and Brandeis, *The Right to Privacy* was, and remains, the defining moment for privacy in the United States. Indeed, it is not an overstatement to say that their privacy theory was the foundation for privacy law in the United States, hence Privacy 1.0.

and Brandeis rejected harm-based models when they championed the right to be let alone.[29] A different way to understand the right to be let alone is to consider it as a notice-and-choice model. One cannot truly exercise the right to be let alone unless there is notice—an understanding of the potential occurrence—of the potential privacy invasion, and you have the opportunity to choose to be let alone—freedom to determine when and where one's information is disclosed or used.

Although Privacy 1.0 provided some structure for privacy, it did not completely answer the questions that courts and commentators were asking, particularly as technology advanced. Dean Prosser attempted to cure this by examining cases that resulted from the Privacy 1.0 construct, and he ultimately concluded that a harm-based model, which was later memorialized in the *Restatement (Second) of Torts*, was the

---

> Warren and Brandeis were deeply concerned about the inability of the common law to protect an individual's privacy, particularly at a time of technological advances:
>
> > The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.
>
> The technological advance that caused the most concern was the instant camera.
>
> > Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." . . . Of the desirability—indeed of the necessity—of some such protection, there can, it is believed, be no doubt. The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery.
>
> While the problem was clearly identified by Warren and Brandeis, finding a legal theory that provided adequate protection proved more difficult. They first considered the law of defamation as a model for invasions of privacy:
>
> > Owing to the nature of the instruments by which privacy is invaded, the injury inflicted bears a superficial resemblance to the wrongs dealt with by the law of slander and of libel, while a legal remedy for such injury seems to involve the treatment of mere wounded feelings, as a substantive cause of action.
>
> However, the law of defamation was ultimately rejected because it was based upon a "radically different class" of damages to an individual. This was in part because, if the action was otherwise lawful, common law, unlike Roman law, did not recognize a claim for mere mental injury.

Serwin, *supra* note 8, at 877–79 (footnotes omitted) (quoting Warren & Brandeis, *supra* note 27, at 195–97).

29. *See id.*

appropriate model.[30] This harm-based model was "Privacy 2.0," and it ultimately resulted in the four now-familiar privacy torts.[31]

The FTC has used similar models and characterized them in the same terms, but it identifies the timing of Privacy 1.0 and 2.0 a bit differently.[32] As noted in Part III.B, the FTC has primarily used two

---

30. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977).

31. I previously noted:

> While groundbreaking, Privacy 1.0 did not provide all of the structure needed by courts, particularly as technology advanced and concerns over privacy changed. Dean Prosser noted this disconnect in 1960:
>
> > Judge Biggs has described the present state of the law of privacy as "still that of a haystack in a hurricane." Disarray there certainly is; but almost all of the confusion is due to a failure to separate and distinguish these four forms of invasions, and to realize that they call for different things.
>
> Dean Prosser attempted to cure the disarray by creating the next theoretical construct of privacy—Privacy 2.0—by following a closely related path. In 1960, Dean Prosser examined a number of the cases that flowed from the Warren and Brandeis theory and categorized them into one of four categories, which ultimately served as the basis for the Restatement's four categories of privacy torts: intrusion upon seclusion, appropriation of name or likeness, publicity given to private life, and publicity placing a person in false light. While Dean Prosser's goal was a noble one, the current commentary on privacy suggests that the hurricane is still blowing quite strongly.

Serwin, *supra* note 8, at 883 (footnote omitted) (quoting William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 407 (1960)).

32. Commissioner Julie Brill noted:

> Let us go back and think about the early stages of privacy regulation in the 1990s. "Privacy 1.0," from my perspective, was the "Notice and Choice" Model. We called it the "Fair Information Practices" principles. Although you might not be familiar with that title, everyone is familiar with the underlying principles. During this stage, the FTC and the states looked at privacy issues through a regulatory framework that called for notice, choice, access, and security with respect to information. We evaluated privacy policies that way: privacy policies on the web, practices of companies, and various self-regulatory regimes were all examined through the lens of Fair Information Practices.
>
> The FTC, the states, and many consumer advocates called on Congress to enact these Notice and Choice principles into law. However, Congress did not enact sweeping legislation on these broad principles. But it did enact the Gramm-Leach-Bliley Act, which many of you are familiar with. The GLB Act embodies Notice and Choice principles. Consumers are given a one-time notice. They are required to read it, understand it, and make an intelligent choice that often will last for a long time. It is an interesting model and I am going to have some thoughts and critiques about it in a moment.
>
> Shortly after GLB was enacted, the Federal Trade Commission, as some of you know, switched gears, and moved from "Privacy 1.0" to "Privacy 2.0." It moved from a regulatory framework focused on Fair Information Practices to one focused on principles of harm. The Harm Model was first launched by former FTC Chairman Tim Muris, but it since has been embraced by many people, including in the states. The Harm Model focuses on harmful privacy

different models to promote consumer privacy: a notice-and-choice model, characterized by the fair information practice principles, and a harm-based approach.[33] The FTC recognizes that these models have been subject to criticisms, including that they have failed to keep pace with rapidly evolving technology.[34] The notice-and-choice model has resulted in lengthy privacy policies, drafted primarily by lawyers, that the FTC feels may not always adequately disclose companies' information practices in clear and understandable ways, which is actually a predictable result if one reviews the FTC's Deception Statement and its focus on disclosures to consumers. These challenges are ultimately not a complete surprise given that these same criticisms have been leveled against Privacy 1.0 and 2.0, and the FTC notice-and-choice and harm-based models rely upon the same underlying theories as Warren and Brandeis and Prosser, respectively.

As section 5 is examined, it is also helpful to try and classify the FTC's authority regarding deceptive and unfair trade practices in these terms so that the evolution of FTC enforcement can be fully understood. As more fully explained below, cases that rely upon deception are examples of the FTC's notice-and-choice model of enforcement, and the unfairness cases are examples of the FTC's harm-based approach.

> practices that present risks of physical security or economic injury. As a result, the Federal Trade Commission, and the states, started focusing on data security, data breaches, identity theft, and children's online privacy, as well as issues such as spam, spyware, and telemarketing, including the Do Not Call list.
>
> Let me expand a bit on the first two issues, data security and data breaches. During the Privacy 2.0 timeframe, regulators focused on enhancing tools to address data security and data breaches.

Julie Brill, Comm'r, Fed. Trade Comm'n, Remarks at Conference of Western Attorneys General Annual Meeting: Privacy 3.0 Panel (July 20, 2010), *available at* http://www.ftc.gov/speeches/brill/100720cwagtranscription.pdf. For a video recording of the presentation, see Chris Hoofnagle, *Commissioner Brill and Privacy 3.0 at the CWAG Privacy Panel*, BERKELEY BLOG (July 21, 2010), http://blogs.berkeley.edu/2010/07/21/commissioner-brill-and-privacy-3-0-at-the-cwag-privacy-panel-2/.

33. FED. TRADE COMM'N, *supra* note 2, at iii; *see also Fair Information Practice Principles*, FED. TRADE COMM'N, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified June 25, 2007).

34. FED. TRADE COMM'N, *supra* note 2, at iii. Indeed, if one accepts the argument advanced in this Article—that enforcement based upon deception is truly an example of the FTC-recognized notice-and-choice enforcement model, lengthy disclosure-laden "policies" are a predictable result as companies attempt to meet their legal requirements and minimize their enforcement risk.

VI. UNDERSTANDING SECTION 5

Section 45 of Title 15 of the United States Code, also known as section 5 of the FTCA,[35] provides the basis for FTC actions against unfair and deceptive trade practices. Specifically, "[t]he commission is empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in commerce and unfair or deceptive acts or practices in commerce."[36] The Commission may prevent persons, partnerships, or corporations,[37] with certain exceptions,[38] from using unfair methods of competition or unfair or deceptive acts or practices in or affecting commerce.[39]

The Commission's reach is not unlimited. It may not prevent unfair methods of competition involving commerce with foreign nations unless the competition has a direct, substantial effect on U.S. commerce. All remedies are available to the Commission with respect to unfair and deceptive acts or practices, including restitution to domestic or foreign victims.[40]

Over time, courts and the FTC worked to define FTC authority in the deception and unfairness arenas.[41] While this was occurring, there was a

---

35. Federal Trade Commission Act of 1914, Pub. L. No. 63-203, § 5, 38 Stat. 719 (codified as amended at 15 U.S.C. § 45 (2006)).

36. FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 235 (1972) (quoting 15 U.S.C. § 45(a)(6)); *see also* 15 U.S.C. § 45(a)(2).

37. The term *corporation* includes the following:

> [A]ny company, trust, so-called Massachusetts trust, or association, incorporated or unincorporated, which is organized to carry on business for its own profit or that of its members, and has shares of capital or capital stock or certificates of interest, and any company, trust, so-called Massachusetts trust, or association, incorporated or unincorporated, without shares of capital or capital stock or certificates of interest, except partnerships, which is organized to carry on business for its own profit or that of its members.

15 U.S.C. § 44 (Supp. 2006).

38. These exceptions include the following:

> [B]anks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title, common carriers subject to acts which regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended, except as provided in section 406(b) of [the Packers and Stockyards] Act . . . .

Id. § 45(a)(2) (citations omitted).

39. *Id.*

40. *Id.* § 45(a)(3)–(4)(B).

41. *See infra* Parts VIII–IX (discussing the FTC's and courts' process of defining deception and unfairness, respectively).

shift in the section 5 enforcement patterns as well because false advertising and other wrongs were initially the focus of the FTC's consumer agenda and privacy and information security were not focal points for the FTC.[42] Over time several section 5 cases have been premised upon allegations arising from privacy and information security issues.[43]

VII. UNFAIR OR DECEPTIVE ACTS OR PRACTICES—RULEMAKING AUTHORITY

In addition to enforcement authority, the FTC also has authority to prescribe interpretive rules and general statements of policy with respect to unfair or deceptive acts or practices in or affecting commerce, subject to several requirements.[44]

Generally speaking, "[p]rior to the publication of any notice of proposed rulemaking . . . the Commission shall publish an advance notice of proposed rulemaking in the Federal Register."[45] The advance notice must contain a brief description of the area of inquiry under consideration, the objectives that the Commission seeks to achieve, and possible regulatory alternatives under consideration by the Commission. It must also invite the response of interested parties with respect to such proposed rulemaking, including any suggestions or alternative methods for achieving such objectives.[46]

The Commission must also "submit such advance notice of proposed rulemaking to the Committee on Commerce, Science, and Transportation of

---

42. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 273 (2011); Earl W. Kintner, *Federal Trade Commission Regulation of Advertising*, 64 MICH. L. REV. 1269, 1274–76 (1966).

43. *See*, *e.g.*, FTC v. Accusearch Inc., 570 F.3d 1187, 1194 (10th Cir. 2009) (claiming violation of section 5 by company that obtained consumer telephone records); Vision I Props., LLC, 139 F.T.C. 296, 299, 303 (2005) (claiming unfair act in violation of section 5 by company for misleading representation of personal information disclosure); GeoCities, 127 F.T.C. 94, 96–97 (1999) (claiming deceptive practices used in connection with use of personal information).

44. 15 U.S.C. § 57a(a)–(b)(1) (2006).

> When prescribing a rule . . . the Commission shall . . . (A) publish a notice of proposed rulemaking stating with particularity the text of the rule, including any alternatives, which the Commission proposes to promulgate, and the reason for the proposed rule; (B) allow interested persons to submit written data, views, and arguments, and make all such submissions publicly available; (C) provide an opportunity for an informal hearing . . . and (D) promulgate, if appropriate, a final rule based on the matter in the rulemaking record . . . together with a statement of basis and purpose.

Id. § 57a(b)(1).

45. *Id.* § 57a(b)(2)(A).

46. *Id.* § 57a(b)(2)(A)(i)–(ii).

the Senate and to the Committee on Energy and Commerce of the House of Representatives."[47]

VIII. DECEPTION

Defining a deceptive trade practice was not a straightforward task. The FTC had to go through a process, including issuing a policy statement to Congress, which was not initially unanimously adopted by all of the commissioners, in an attempt to define deception.[48] The policy statement took the form of a letter to Congressman John D. Dingell dated October 14, 1983, in which the FTC identified several key elements that it considered when assessing whether an act or practice was deceptive. In sum, as recognized by the FTC in a later enforcement matter, *In re Cliffdale Associates*, consistent with the Policy Statement on Deception, the Commission will find an act or practice deceptive if "there is a representation, omission, or practice" that is "likely to mislead the consumer acting reasonably in the circumstances" and the representation, omission, or practice is material.[49] These elements are based upon the factors used in earlier Commission cases identifying whether or not an act or practice was deceptive, though it was phrased in a slightly different manner.[50] Each of these elements is examined below.

A. Likely To Mislead

In its Deception Statement, the FTC discussed what it would consider when determining whether the act or practice was likely to deceive. It first noted that in making this assessment, actual deception need not result, though the FTC must demonstrate that a representation, omission, or practice occurred. Thus, once the act or practice is established, the FTC must only show that it is likely to deceive.[51] This requirement was also discussed in *Cliffdale*, where the FTC stated that the requirement

47. *Id.* § 57a(b)(2)(B).

48. *See generally* Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, to Hon. John D. Dingell, Chairman, Comm. on Energy and Commerce, U.S. House of Representatives (Oct. 14, 1983) [hereinafter Deception Statement], *available at* http://www.ftc.gov/oia/assistance/consumerprotection/advertising/policy_deception.pdf, *appended to* Cliffdale Assocs., Inc., 103 F.T.C. 110 (1984).

49. *Cliffdale*, 103 F.T.C. at 165.

50. Sears, Roebuck & Co., 95 F.T.C. 406, 420, 423–24 (1980), *aff'd*, 676 F.2d 385 (9th Cir. 1982).

51. Deception Statement, *supra* note 48, at 2.

that an act or practice be "likely to mislead," for example, reflects a long-established principle that the Commission need not find actual deception to find that a violation of section 5 has occurred.[52] The FTC explained this standard as follows: "In the application of [the deception] standard to the many different factual patterns that have arisen in cases before the Commission, certain principles have become well established. One is that under Section 5 actual deception of particular consumers need not be shown."[53]

B. The Act or Practice Must Be Considered from the Perspective of the Reasonable Consumer

The second element of deception considered by the FTC is the requirement that the FTC examine the challenged act or practice from the perspective of "reasonable consumers under the circumstances."[54] In its Deception Statement, the FTC noted that an advertiser would not be charged with liability for every conceivable misconception, particularly if it is misunderstood by a small or insignificant group of individuals. As an example, the FTC stated:

> Some people, because of ignorance or incomprehension, may be misled by even a scrupulously honest claim. Perhaps a few misguided souls believe, for example, that all "Danish pastry" is made in Denmark. Is it therefore an actionable deception to advertise "Danish pastry" when it is made in this country? Of course not. A representation does not become "false and deceptive" merely because it will be unreasonably misunderstood by an insignificant and unrepresentative segment of the class of persons to whom the representation is addressed.[55]

---

52. *Cliffdale*, 103 F.T.C. at 165.

53. Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8350 (July 2, 1964) (to be codified at 16 C.F.R. pt. 408).

54. Deception Statement, *supra* note 48, at 3.

55. *Id*. at 3 (quoting Heinz W. Kirchner, 63 F.T.C. 1282, 1290 (1963)); *see also* Bristol-Myers Co., 102 F.T.C. 21, 311 (1983) (finding Bristol-Myer's advertising of Bufferin, Excederin, and Excederin P.M. to be false and misleading to the consumer group as a whole); Sterling Drug, Inc., 102 F.T.C. 395, 739 (1983) (finding Sterling Drug, Inc.'s advertising of Bayer Aspirin, Bayer Children Aspirin, Midol, Cope, and Vanquish misleading to the consumer group as a whole); Am. Home Prods. Corp., 98 F.T.C. 136, 343 (1981) (finding American Home Products' advertising of Anacin and Arthritis Pain Formula false and misleading to the consumer group as a whole). This was reaffirmed by the FTC's opinion in *Cliffdale*, which stated:

> Similarly, the requirement that an act or practice be considered from the perspective of a 'consumer acting reasonably in the circumstances' is not new. Virtually all representations, even those that are true, can be misunderstood by some consumers. The Commission has long recognized that the law should not be applied in such a way as to find that honest representations are deceptive simply because they are misunderstood by a few. Thus, the Commission has noted that an advertisement would not be considered deceptive merely because

However, the FTC will analyze specific market segments of consumers if the act or practice is targeted to a particular group.[56]

The FTC identified a number of factors it would consider when assessing whether a reasonable consumer would be misled and summarized its views as follows:

> In sum, the Commission will consider many factors in determining the reaction of the ordinary consumer to a claim or practice. As would any trier of fact, the Commission will evaluate the totality of the ad or the practice and ask questions such as: how clear is the representation? how conspicuous is any qualifying information? how important is the omitted information? do other sources for the omitted information exist? how familiar is the public with the product or service?[57]

C. Materiality

The last element identified by the FTC was that the representation, omission, or practice be material for deception to be found.[58] In essence, the FTC examines whether the information was important to consumers—whether it affected consumers' choices.[59] The starting point of this analysis is an examination of what claim has been made. If the claim is an express claim, this typically establishes the meaning of the claim according to the FTC.[60] If the claim is implied, the FTC will examine

---

> it could be "unreasonably misunderstood by an insignificant and unrepresentative segment of the class of persons whom the representation is addressed." In recent cases, this concept has been increasingly emphasized by the Commission.

Cliffdale, 103 F.T.C. at 165 (footnotes omitted).

56. Ideal Toy Corp., 64 F.T.C. 297, 310 (1964); *Heinz W. Kirchner*, 63 F.T.C. at 1290; Deception Statement, *supra* note 48, at 4.

57. Deception Statement, *supra* note 48, at 6.

58. *Id.* at 7.

59. The Deception Statement defined the term *materiality* as follows: "A 'material' misrepresentation or practice is one which is likely to affect a consumer's choice of or conduct regarding a product. In other words, it is information that is important to consumers. If inaccurate or omitted information is material, injury is likely." *Id.* (footnote omitted). In *Cliffdale*, the FTC formulated the standard in a similar way. 103 F.T.C. at 165–66 ("As noted in the Commission's policy statement, a material representation, omission, act or practice involves information that is important to consumers and, hence, likely to affect their choice of, or conduct regarding, a product. Consumers thus are likely to suffer injury from a material misrepresentation. A review of past Commission deception cases shows that one of the factors usually considered, either directly or indirectly, is whether or not a claim is material." (footnote omitted) (citing *Am. Home Prods. Corp.*, 98 F.T.C. 136; Ford Motor Co., 84 F.T.C. 729, 735 (1974), *aff'd*, 547 F.2d 954 (6th Cir. 1976))); *see* Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8325 (July 2, 1964) (to be codified at 16 C.F.R. pt. 408).

60. Deception Statement, *supra* note 48, at 7.

the representation, "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."[61] This does not require a showing of actual causation, including in advertising cases where the FTC need not make a showing that the consumer would not have purchased the product at issue but for the deception. Instead, the FTC can show that the consumer would have been less likely to make the purchase but for the deception.[62] In *International Harvester*, the FTC stated that it "presumes that all express claims are material, and that implied claims are material if they pertain to the central characteristics of the product, such as its safety, cost, or fitness for the purpose sold."[63]

D. Summarizing the Deception Elements

Ultimately, this test can be distilled down to three elements, and this formulation has been recognized by a number of courts, albeit in a slightly different order than discussed above. The FTC must prove (1) a material representation, omission, or practice (2) that is likely to mislead consumers (3) who are acting reasonably in the circumstances.[64] As noted above, the FTC is not required to prove that the defendants intended their misrepresentations to defraud or deceive or that they made them in bad faith.[65]

E. Deception and Notice-and-Choice Models of Enforcement

The FTC admittedly has used two enforcement models in privacy—notice-and-choice and consumer injury.[66] When one considers the deception doctrine's focus on the disclosure of material facts—particularly those that impact consumer choice—enforcement based upon the FTC's authority to stop deceptive trade practices is a clear example of privacy enforcement under the notice-and-choice model.

---

61. *Cliffdale*, 103 F.T.C. at 166 (citing Bristol-Myers Co., 102 F.T.C. 21 (1983); Nat'l Dynamics Corp., 82 F.T.C. 488, 548 (1972), *aff'd per curiam*, 492 F.2d 1333 (2d Cir. 1973)).

62. *See* Leonard F. Porter, Inc., 88 F.T.C. 546, 628 (1976); Travel King, Inc., 86 F.T.C. 715, 774 (1975).

63. Int'l Harvester Co., 104 F.T.C. 949, 1057 (1984) (footnote omitted).

64. Deception Statement, *supra* note 48, at 1 (providing "guidance to the public" regarding the "Commission's enforcement policy against deceptive ads or practices"); *see also* Novartis Corp. v. FTC, 223 F.3d 783, 786 (D.C. Cir. 2000); United States v. Locascio, 357 F. Supp. 2d 536, 549 (E.D.N.Y. 2004); FTC v. Verity Int'l, Ltd., 124 F. Supp. 2d 193, 200 (S.D.N.Y. 2000).

65. *Verity Int'l*, 124 F. Supp. 2d at 200 n.42; *see, e.g.*, FTC v. World Travel Vacation Brokers, Inc., 861 F.2d 1020, 1029 (7th Cir. 1988).

66. FED. TRADE COMM'N, *supra* note 2, at iii.

IX. UNFAIRNESS AUTHORITY

The Supreme Court initially had to address two key issues regarding the FTC's unfairness authority. The first was whether the categories of conduct that could be considered unfair were fixed or in fact could change over time. In 1931, the Supreme Court answered this question, finding that the definition of unfairness was a fluid one that was not susceptible to being categorically fixed.[67] The Supreme Court expanded on this view in *FTC v. Sperry & Hutchinson Co.*, noting that when Congress created the FTC "it explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' by tying the concept of unfairness to a common-law or statutory standard or by enumerating the particular practices to which it was intended to apply."[68]

The second question the Supreme Court resolved was whether the FTC's jurisdiction went beyond conduct that violated the "letter or

---

67. FTC v. Raladam Co., 283 U.S. 643, 648 (1931); *see also* FTC v. R.F. Keppel & Bro., Inc., 291 U.S. 304, 310 (1934) ("Neither the language nor the history of the Act suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories.").

68. FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239–40 (1972). Senate Report 597 presents the reasoning that led the Senate Committee to avoid the temptations of precision when framing the Trade Commission Act:

> The committee gave careful consideration to the question as to whether it would attempt to define the many and variable unfair practices which prevail in commerce and to forbid their continuance or whether it would, by a general declaration condemning unfair practices, leave it to the commission to determine what practices were unfair. It concluded that the latter course would be the better, for the reason, as stated by one of the representatives of the Illinois Manufacturers' Association, that there were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others.

R.F. Keppel, 291 U.S. at 310 n.1 (citing S. REP. NO. 63-597, at 13 (1914)). The *R.F. Keppel* court opined:

> Neither the language nor the history of the Act suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories. The common law afforded a definition of unfair competition and, before the enactment of the Federal Trade Commission Act, the Sherman Act had laid its inhibition upon combinations to restrain or monopolize interstate commerce which the courts had construed to include restraints upon competition in interstate commerce. It would not have been a difficult feat of draftsmanship to have restricted the operation of the Trade Commission Act to those methods of competition in interstate commerce which are forbidden at common law or which are likely to grow into violations of the Sherman Act, if that had been the purpose of the legislation.

Id. at 310.

spirit" of antitrust laws. In answering this question, the Supreme Court broke the question down into two component questions—does section 5 permit the FTC to (1) define and proscribe an unfair competitive practice, even though the practice does not infringe on either the letter or the spirit of the antitrust laws, and (2) proscribe practices as unfair or deceptive in their effect upon consumers regardless of their nature or quality as competitive practices or their effect on competition?[69] The Supreme Court concluded that the answer to both questions was "yes," and therefore the Court did not require the FTC to show a violation of antitrust laws to declare a practice to be unfair.[70]

Though not central to its holding, the *Sperry & Hutchinson* Court also recognized that prior FTC decisions had identified three key factors in identifying whether an act was unfair to consumers: (1) whether the practice injures consumers, (2) whether it violates established public policy, and (3) whether it is unethical or unscrupulous.[71] Although these decisions answered two key initial questions regarding the FTC's unfairness authority, a number of cases and a statement from the FTC were necessary to help further define the somewhat elusive concept of unfairness.[72]

A. The FTC's December 1980 Statement Regarding Unfairness

On June 13, 1980, Senators Wendell Ford and John Danforth wrote the FTC and stated their desire to hold oversight hearings regarding the FTC's unfairness authority in consumer transactions and specifically whether the FTC's authority was limited to matters involving false or

---

69. *Sperry & Hutchinson*, 405 U.S. at 239.

70. *Id.* at 233, 244 ("Congress, as previously recognized by this Court, defines the powers of the FTC to protect consumers as well as competitors and authorizes it to determine whether challenged practices, though posing no threat to competition within the letter or spirit of the antitrust laws, are nevertheless either unfair methods of competition, or unfair or deceptive acts or practices. The Wheeler-Lea Act of 1938 reaffirms this broad congressional mandate . . . . Thus, legislative and judicial authorities alike convince us that the Federal Trade Commission does not arrogate excessive power to itself if, in measuring a practice against the elusive, but congressionally mandated standard of fairness, it, like a court of equity, considers public values beyond simply those enshrined in the letter or encompassed in the spirit of the antitrust laws." (citation omitted)).

71. *Id.* at 244 n.5; *see also* Letter from Michael Pertachuk, Chairman, Fed. Trade Comm'n et al., to Hon. Wendell H. Ford, Chairman, Consumer Subcomm., Comm. on Commerce, Science & Transp., and Hon. John C. Danforth, Banking Minority Member, Consumer Subcomm., Comm. on Commerce, Science & Transp. (Dec. 17, 1980) [hereinafter Unfairness Statement], *appended to* Int'l Harvester Co., 104 F.T.C. 949, 1070–76 (1984).

72. Although Congress clearly answered the question of whether the FTC's jurisdiction was limited to matters that were de facto antitrust violations, it did not clearly delineate the full scope of the FTC's authority, particularly regarding its unfairness authority.

deceptive commercial advertising.[73] On December 17, 1980, recognizing that the definition of unfairness was not "immediately obvious," the FTC responded to Senators Ford and Danforth with a letter that has become known as its "Unfairness Statement" and took the opportunity to state its views regarding the parameters of its unfairness authority. Although the FTC recognized its role in defining its unfairness authority, it also recognized that its discretion was not unlimited and in fact was subject to judicial review.[74]

Although the *Sperry & Hutchinson* factors were the starting point for the FTC, it recognized that the doctrine had continued to evolve in the intervening eight years, and the factors identified by the FTC were slightly different from those identified by the Supreme Court. Each of the *Sperry & Hutchinson* factors is discussed below, though ultimately the FTC in essence collapsed all three factors into the consumer injury prong of the *Sperry & Hutchinson* factors.

1. Consumer Injury

Recognizing that preventing consumer injury was the focus of the FTCA, the FTC stated its view that consumer injury alone can be sufficient to support a finding that a practice is unfair.[75] The Unfairness Statement identified three factors that the FTC would use to determine if there was sufficient consumer injury to satisfy the first factor of the *Sperry & Hutchinson* factors: (1) there must be substantial consumer injury (2) that is not outweighed by any offsetting consumer or competitive benefits that the sales practice also produces, and (3) the injury must be one that consumers could not have reasonably avoided.[76]

In assessing the first injury factor, the FTC requires that any consumer injury must be substantial and not based upon trivial or speculative

73. Unfairness Statement, *supra* note 71, at 1070–76.

74. *Id.* at 1071–72; *see, e.g.*, *Sperry & Hutchinson*, 405 U.S. at 249; *R.F. Keppel*, 291 U.S. at 314.

75. Unfairness Statement, *supra* note 71, at 1073 ("Unjustified consumer injury is the primary focus of the FTCA, and the most important of the three *S&H* criteria. By itself it can be sufficient to warrant a finding of unfairness. The Commission's ability to rely on an independent criterion of consumer injury is consistent with the intent of the statute, which was to '[make] the consumer who may be injured by an unfair trade practice of equal concern before the law with the merchant injured by the unfair methods of a dishonest competitor.'" (alteration in original) (quoting 83 CONG. REC. 3255 (1938) (remarks of Senator Wheeler))).

76. *Id.* at 1073–74.

harms.[77] The FTC's view was that this would typically require monetary harm or unwarranted health and safety risks but would not ordinarily include emotional impact or other "more subjective" harms.[78] In one of the few privacy cases to reference what "substantial harm" is under section 5, the Tenth Circuit noted that the FTC had concluded that the posting of names and telephone records online—which caused consumers to incur emotional harm from being stalked or otherwise harassed and substantial costs in changing telephone providers—caused "substantial injury" when it assessed whether the practices by defendants were unfair under section 5.[79]

In assessing the second injury factor, the FTC stated that it would consider the cost and benefit "tradeoffs" and would only find that a practice unfairly injures consumers if "it is injurious in its net effects," which includes an examination of the costs to the parties before the FTC, as well as the burdens placed upon society in general.[80] Finally, in assessing the third injury factor, the FTC stated that it relied upon market choice to a certain degree but that the FTC would act where it perceived that consumer choice was being impacted by the allegedly unfair business practice.[81]

2. Violation of Public Policy

In assessing the second *Sperry & Hutchinson* factor, the FTC stated that this factor examines whether the alleged conduct violates public

---

77. *Id.* at 1073.

78. *Id.*

79. FTC v. Accusearch Inc., 570 F.3d 1187, 1193–94 (10th Cir. 2009). This issue was not argued on appeal, so it is dicta, but it is one of the few published cases to even reference this issue.

80. Unfairness Statement, *supra* note 71, at 1073–74 ("The Commission is aware of these tradeoffs and will not find that a practice unfairly injures consumers unless it is injurious in its net effects. The Commission also takes account of the various costs that a remedy would entail. These include not only the costs to the parties directly before the agency, but also the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters." (footnote omitted)).

81. *Id.* at 1074 ("Normally we expect the marketplace to be self-correcting, and we rely on consumer choice—the ability of individual consumers to make their own private purchasing decisions without regulatory intervention—to govern the market. We anticipate that consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory. However, it has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. Most 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.").

policy "as it has been established by statute, common law, industry practice, or otherwise."[82] This factor was used in two different ways by the FTC: "to test the validity and strength of the evidence of consumer injury" or, in other cases, for a "dispositive legislative or judicial determination that such injury is present."[83]

The FTC then further defined how it would view public policy in unfairness cases:

> To the extent that the Commission relies heavily on public policy to support a finding of unfairness, the policy should be clear and well-established. In other words, the policy should be declared or embodied in formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the courts, rather than being ascertained from the general sense of the national values. The policy should likewise be one that is widely shared, and not the isolated decision of a single state or a single court. If these two tests are not met the policy cannot be considered as an "established" public policy for purposes of the *S&H* criterion. The Commission would then act only on the basis of convincing independent evidence that the practice was distorting the operation of the market and thereby causing unjustified consumer injury.[84]

In any event, given that the considerations the FTC utilizes regarding public policy expressly relate to the examination of the first *Sperry & Hutchinson* factor, consumer injury, it is not surprising that the FTC stated that it generally considered the violation of the public policy prong to be part of its examination of the evidence of consumer injury for the first *Sperry & Hutchinson* element.[85]

3. Unethical or Unscrupulous Conduct

Although the FTC identified the third *Sperry & Hutchinson* factor in the Unfairness Statement, it dismissed it as largely duplicative. In the

82. *Id.*
83. *Id.* at 1074–75.
84. *Id.* at 1076.
85. *Id.* at 1075 ("As we have indicated before, the Commission believes that considerable attention should be devoted to the analysis of whether substantial net harm has occurred, not only because that is part of the unfairness test, but also because the focus on injury is the best way to ensure that the Commission acts responsibly and uses its resources wisely. Nonetheless, the Commission wishes to emphasize the importance of examining outside statutory policies and established judicial principles for assistance in helping the agency ascertain whether a particular form of conduct does in fact tend to harm consumers. Thus the agency has referred to First Amendment decisions upholding consumers' rights to receive information, for example, to confirm that restrictions on advertising tend unfairly to hinder the informed exercise of consumer choice.").

FTC's view, conduct that was unethical would typically produce consumer injury or violate policy.[86]

B. Distilling the Unfairness Statement

Ultimately, the focus on consumer injury in unfairness cases permits the distillation of the *Sperry & Hutchinson* factors into an examination of the consumer injury prong, which was ultimately codified in section 5.[87] At the time the Unfairness Statement was issued, there was a dispute over whether the FTC's authority in certain areas, including children's advertising, should be extended and whether its unfairness authority should be eliminated. Ultimately, the Unfairness Statement was codified by Congress via an amendment to 15 U.S.C. § 45(n), which now reflects the consumer injury focus. Under this formulation a practice is unfair if it (1) causes or is likely to cause substantial injury to consumers (2) that is not reasonably avoidable by consumers themselves and (3) not outweighed by countervailing benefits to consumers or to competition.[88]

Recognizing the FTC's statements regarding the somewhat subordinate role of public policy, § 45(n) also states that "[i]n determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination."[89] Consistent with these amendments, the FTC has stated its view that an act or practice is unfair if the injury it causes, or is

86. *Id.* at 1076 ("Finally, the third *S&H* standard asks whether the conduct was immoral, unethical, oppressive, or unscrupulous. This test was presumably included in order to be sure of reaching all the purposes of the underlying statute, which forbids 'unfair' acts or practices. It would therefore allow the Commission to reach conduct that violates generally recognized standards of business ethics. The test has proven, however, to be largely duplicative. Conduct that is truly unethical or unscrupulous will almost always injure consumers or violate public policy as well. The Commission has therefore never relied on the third element of *S&H* as an independent basis for a finding of unfairness, and it will act in the future only on the basis of the first two.").

87. Federal Trade Commission Act of 1914, Pub. L. No. 63-203, § 5, 38 Stat. 719, (codified as amended at 15 U.S.C. § 45 (2006)).

88. FTC v. Accusearch, Inc., 570 F.3d 1187, 1193 (10th Cir. 2009) (citing 15 U.S.C. § 45(n)); Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 970 (D.C. Cir. 1985) ("Although Congress has subsequently solicited statements and held oversight hearings on the question of whether the FTC's unfairness authority should be eliminated or permanently restricted, it has taken no definitive legislative action to define the limits of that authority. Bills were introduced in both the 97th and 98th Congresses which would have amended section 5 to provide a definition of unfair acts or practices. The definition proposed in these bills was the definition supplied by the Commission at the request of Congress in a 1980 policy statement." (footnotes omitted)).

89. 15 U.S.C. § 45(n).

likely to cause, is (1) substantial, (2) not outweighed by other benefits, and (3) not reasonably avoidable.[90]

Although not many cases have litigated the scope of the FTC's unfairness authority, there are some that have provided further guidance and approved the factors referenced above.[91]

C. Unfairness and Harm-Based Enforcement Models

As noted in the recent FTC report, the second privacy enforcement model identified by the FTC was a harm-based model. When the elements of the FTC's unfairness authority are considered, particularly in light of the injury-centric analysis that has been adopted, it becomes clear that the FTC's unfairness authority is a harm-based model of enforcement.

X. ENFORCEMENT CASES

A. In re GeoCities*—A Traditional Deception Model*

In re GeoCities was the first section 5 case arising from privacy allegations. In this case the FTC alleged that GeoCities engaged in deceptive conduct by making misrepresentations in its privacy policy, including that it would "NEVER give your information to anyone without your permission."[92] The FTC's specific allegations included that GeoCities had represented, expressly or by implication, that the personal identifying information collected through its "new member application" form was used only for limited purposes—for the purpose of providing to members the specific e-mail advertising offers and other products or services they requested—but in actuality the personal identifying information collected through GeoCities' new member application form was not just used for those limited purposes. The FTC

90. FED. TRADE COMM'N, ADVERTISING AND MARKETING ON THE INTERNET: RULES OF THE ROAD 2 (2000).

91. *See* Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1364–65 (11th Cir. 1988) (applying Unfairness Statement factors); Spiegel, Inc. v. FTC, 540 F.2d 287, 292–93 (7th Cir. 1976) (citing with approval the *Sperry & Hutchinson* unfairness factors); FTC v. IFC Credit Corp., 543 F. Supp. 2d 925, 937 n.5 (N.D. Ill. 2008) ("The legislative history demonstrates that Congress's intent was to codify the FTC's Unfairness Policy Statement of 1980, which was contained in a letter in response to a request from the Consumer Subcommittee of the Committee on Commerce, Science and Transportation, requesting the Commission's views on cases under § 5.").

92. GeoCities, 127 F.T.C. 94, 96–98 (1999) (complaint).

also alleged that GeoCities had sold, rented, or otherwise marketed or disclosed this information, including information collected from children, to third parties who used this information for purposes other than those for which members had given permission.[93] The FTC therefore alleged that the representations made by GeoCities were false and misleading.[94]

The matter was resolved via consent judgment, with a twenty-year duration, that placed a number of requirements that would over time become more familiar to companies that became subject to consent judgments.[95] These included the requirement that GeoCities:

- Not make any misrepresentation, expressly or by implication, about its collection or use of personal identifying information from or about consumers;
- Not misrepresent the identity of the party collecting any personal identifying information from consumers or the sponsorship of any activity on its website;
- Not collect personal identifying information from any child if GeoCities has actual knowledge that the child does not have a parent's permission to provide the information;
- Post a clear and prominent notice on its website explaining GeoCities' practices with regard to its collection and use of personal identifying information. The notice must include the following: (1) what information is being collected, (2) its intended use(s), (3) the third parties to whom it will be disclosed, (4) how the consumer can obtain access to the information, and (5) how the consumer can have the information removed from GeoCities' databases. The notice must appear on the website's home page and at each location on the site at which such information is collected, although the collection of so-called tracking information need only be disclosed on the home page;
- Implement a procedure to obtain "express parental consent" prior to collecting and using children's identifying information, a procedure commonly referred to as "opt-in";
- Notify all consumers—in the case of children, their parents—and give them an opportunity to have their information removed from GeoCities' and third parties' databases;

93. *Id.* at 97–98.
94. *Id.*
95. This matter was also the first children's online enforcement matter, which occurred prior to the enactment of COPPA.

- Retain certain personally identifiable information in its "archived database" for the limited purposes of site maintenance, computer file backup, blocking a child's attempt to register without parental consent, or responding to requests for such information from law enforcement agencies or pursuant to judicial process. GeoCities must disclose its retention of information in the archived database in its privacy notice;
- For five years, place a clear and prominent hyperlink within its privacy notice directing visitors to the FTC's website to view educational material on consumer privacy;
- Meet certain recordkeeping requirements;
- Deliver a copy of the order to certain company officers and personnel;
- Establish an "information practices training program" for employees and GeoCities' community leaders, volunteers who provide a variety of services to GeoCities' members; and
- Notify the Commission of any change in its corporate structure that might affect compliance with the order; and file compliance reports with the Commission.[96]

This matter presented what would become a traditional model for the FTC in privacy matters—companies making representations that the FTC alleged were untrue and these representations serving as the basis for a claim that the respondent had engaged in deceptive conduct under section 5. This would remain the pattern of enforcement for a number of years,[97] though as will be shown by the following consent judgments, there was some indication that deception would not be the exclusive basis for FTC enforcement in the privacy arena.

B. In re ReverseAuction.com, Inc.—*The Appearance of Unfairness*

The FTC led a complaint against ReverseAuction.com based upon the allegation that the company had wrongfully signed into eBay's website and obtained personally identifiable information about users, including e-mail addresses and eBay ratings.[98] Reverseauction.com then allegedly

96. *Geocities*, 127 F.T.C. at 123–32 (decision and order).
97. *See, e.g.*, Telebrands Corp., 140 F.T.C. 278, 368 (2003) (complaint), *aff'd*, 457 F.3d 354 (4th Cir. 2006); Unither Pharma, Inc., 136 F.T.C. 145, 162 (2003) (complaint).
98. Complaint, FTC v. Reverseauction.com, Inc., FTC File. No. 002-3046 (D.D.C. Jan. 6, 2000), *available at* http://www.ftc.gov/os/2000/01/reversecmp.htm.

took this information and spammed the eBay users, falsely representing their eBay accounts were going to expire. ReverseAuction.com was a competitor of eBay, and it was alleged to have done this to promote its own website.[99] The matter was based upon an alleged misrepresentation, as was *GeoCities*, but for the first time, as an alternative theory, the FTC charged that the misrepresentation was also an unfair practice.[100] When the consent judgment and complaint were reviewed by the commissioners, it drew separate opinions from three of the commissioners—Thompson, Swindle, and Leary—regarding the alternative use of the FTC's unfairness authority.[101] Commissioners Swindle and Leary concurred in part and dissented in part because although they supported the assertion that the practices of ReverseAuction.com were deceptive, they disagreed with the FTC's use of its unfairness authority because the conduct at issue did not give rise to substantial injury.[102]

---

99. *Id.*

100. *Id.* ("In the alternative, ReverseAuction's use of the e-mail addresses, eBay user IDs, and feedback ratings of eBay registered users for the purposes of sending unsolicited commercial e-mail, in violation of its agreement to comply with eBay's User Agreement, is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or competition, and therefore was, and is, an unfair practice.").

101. FTC v. ReverseAuction.com, Inc., FTC File No. 002-3046 (D.D.C. Jan 6, 2000) (Swindle & Leary, Comm'rs, concurring in part and dissenting in part) (citing 15 U.S.C. § 45(n) (2006)), *available at* http://www.ftc.gov/os/2000/01/reverses1.htm; *id.* (Thompson, Comm'r, dissenting), *available at* http://www.ftc.gov/os/2000/01/reversemt.htm.

102. Commissioners Swindle and Leary dissented:

> We do not, however, support the unfairness theory in Count One. The Commission has no authority to declare an act or practice unfair unless it "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."

Id. (Swindle & Leary, Comm'rs, concurring in part and dissenting in part) (citing 15 U.S.C. § 45(n)), *available at* http://www.ftc.gov/os/2000/01/reverses1.htm. The commissioners continue:

> The statutory requirement of substantial injury is actually derived from the Commission's own Statement of Policy, issued in 1980. The Commission explained at that time that, "[t]he Commission is not concerned with trivial or merely speculative harms. In most cases a substantial injury involves monetary harm . . . . Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair."
>
> We do not say that privacy concerns can never support an unfairness claim. In this case, however, ReverseAuction's use of eBay members' information to send them e-mail did not cause substantial enough injury to meet the statutory standard.

Id. (citations omitted) (citing Unfairness Statement, *supra* note 71, at 1070–76).

Commissioner Thompson believed that the conduct of ReverseAuction.com had caused substantial injury to consumers and thus believed that the FTC's use of its unfairness authority was proper.[103] Specifically, Commissioner Thompson stated:

> I believe the harm caused in this case is especially significant because it not only breached the privacy expectation of each and every eBay member, it also undermined consumer confidence in eBay and diminishes the electronic marketplace for all its participants. This injury is exacerbated because consumer concern about privacy and confidence in the electronic marketplace are such critical issues at this time.[104]

Ultimately, Commissioner Thompson's view prevailed, and as is shown by later cases, the FTC ultimately went beyond this initial foray into unfairness.

---

103. Commissioner Thompson dissented:

> I believe that ReverseAuction's behavior caused substantial injury to members of the eBay community, that the injury could not have been avoided by those members, and it was not outweighed by countervailing benefits. I believe the harm caused in this case is especially significant because it not only breached the privacy expectation of each and every eBay member, it also undermined consumer confidence in eBay and diminishes the electronic marketplace for all its participants. This injury is exacerbated because consumer concern about privacy and confidence in the electronic marketplace are such critical issues at this time.
>
> In voting for an alternative pleading, the Commission does not here declare that sending unsolicited commercial e-mail ("spamming") is unfair in all circumstances, nor does it suggest that privacy invasions cause substantial injury in all circumstances. Instead, the Commission posits that, under the facts presented here, it is unfair for ReverseAuction to improperly obtain personal information for its use. Accordingly, a majority of the Commission believes that the specific relationship, obligations, and expectations of this electronic community make ReverseAuction's behavior "unfair" under Section 5. Moreover, the injury caused by ReverseAuction's conduct, far from being speculative, is a tangible misappropriation of personal protected information that enabled the company to send personalized deceptive e-mail messages to scores of consumers. In its statement on *Touch Tone*, a majority of the Commission recognized that, "Section 5 of the FTCA deliberately incorporates a flexible standard, so that the Commission may react to changes in the marketplace." For these reasons, I believe this action is not an overly expansive view of the unfairness doctrine, but instead represents a reasoned and tailored response to the circumstances presented.

Id. (Thompson, Comm'r, dissenting) (citation omitted), *available at* http://www.ftc.gov/os/2000/01/reversemt.htm.

104. *Id.*

C. In re Eli Lilly—*Voluntary Assumption of Heightened Burdens*

Eli Lilly was one of the first FTC actions that addressed, at least implicitly, a company's voluntary assumption of heightened privacy burdens arising from representations made to consumers.[105] This matter arose from an e-mail that Eli Lilly sent to customers taking Prozac.[106] Instead of masking the names in the e-mail, Eli Lilly included all of the customers' names. The company had made specific representations on its website regarding its concern for customer privacy on its website, and these representations were relied upon by the FTC in its assertion that Eli Lilly had violated the FTCA.[107] The case is generally perceived as supporting the view that the FTC will read statements regarding concern for customer privacy as creating heightened burdens. It also for the first time focused on the alleged lack of employee training, in that the FTC alleged that the company unreasonably failed to provide appropriate training for its employees regarding consumer privacy and information security, provide appropriate training and oversight for the employee who sent the e-mail, and implement appropriate checks on employees who used sensitive customer data.[108]

Although the theory was novel in other ways for the FTC, the complaint in this matter focused on the traditional allegation of a misrepresentation that was considered to be deceptive and did not contain the alternative count allegations regarding unfairness that the *ReverseAuction.com* matter did, and the unfairness count that raised issues in *ReverseAuction.com* did not surface again for several years.

D. In re Microsoft—*A Continuation of* Eli Lilly

Microsoft was the second case that dealt with heightened privacy burdens created by a privacy policy, and this matter dealt with the issue much more directly than the *Eli Lilly* matter. Microsoft was alleged to have made a number of representations regarding privacy, including that it followed "strict" privacy policies.[109] The FTC alleged that in fact Microsoft did not maintain a high level of security and did not use reasonable and appropriate measures to maintain privacy or security.[110] The FTC also alleged that Microsoft had made misrepresentations regarding

105. *See* Eli Lilly & Co., 133 F.T.C. 763, 789–90 (2002) (analysis of proposed consent order).
106. *Id.* at 789.
107. *Id.* at 789–90.
108. *See id.* at 790.
109. *See* Microsoft Corp., 134 F.T.C. 709, 710–11 (2002).
110. *See id.* at 712.

the amount of personally identifiable information it collected.[111] This matter clearly stated the FTC's view that statements in a privacy policy to the effect that a company has implemented heightened privacy and security standards will bind the company to burdens that may be in excess of what the law would otherwise require.[112]

E. Misrepresentations Serving as the Basis for a Section 5 Deception Claim

The FTC continued to bring section 5 enforcement actions against companies that made misrepresentations regarding privacy or information security for several years. These included *In re National Research Center for College & University Admissions, Inc.*;[113] *In re Educational Research Center of America, Inc.*;[114] *In re Guess?, Inc.*;[115] *In re MTS, Inc.*;[116] *In re Gateway Learning Corp.*;[117] and *In re Petco Animal Supplies, Inc.*[118] All of these cases, although different in certain ways, presented the traditional model of FTC enforcement: alleged misrepresentations regarding information security and privacy that gave rise to a section 5 claim that did not, like *ReverseAuction.com*, directly rely upon the FTC's unfairness authority.

F. In re Vision I Properties, LLC*—A New Model of Deception*

In the case of *In re Vision I Properties, LLC*, the FTC started an investigation of a company that provided a shopping cart service for other e-commerce websites.[119] These websites made specific representations regarding privacy, including that personal information was not sent, sold, or leased to third parties. The FTC alleged that CartManager, a company that provided shopping cart services for these websites, violated the FTCA.[120] In most cases, the portions of the websites gathering the information were CartManager's, but CartManager did not disclose

111. *See id.* at 714–15.
112. *See* discussion *supra* Part X.C.
113. 135 F.T.C. 13 (2003).
114. 135 F.T.C. 578 (2003).
115. 136 F.T.C. 507 (2003).
116. 137 F.T.C. 444 (2004).
117. 138 F.T.C. 443 (2004).
118. 139 F.T.C. 102 (2005).
119. 139 F.T.C. 296, 297 (2005).
120. *Id.* at 299.

that the information practices on these pages were different than the other pages, and these pages appeared to be part of the same website.[121] The FTC claimed that CartManager also began renting information to third parties despite the privacy statements made by the retailers.[122] CartManager also allegedly failed to disclose its information practices to its clients.[123]

This matter presented a different enforcement pattern. Although it relied upon an alleged misrepresentation that was deceptive, it was not a direct representation to consumers because CartManager did not have direct consumer contact.[124] At the time, the matter raised the question of whether the FTC was shifting its enforcement pattern to move away from always requiring an alleged misrepresentation to the consumer or if it viewed the misrepresentation to have flowed through CartManager's customers to the consumers. This question was answered in *In re BJ's Wholesale Club, Inc.*

G. In re BJ's Wholesale Club, Inc.

In re BJ's Wholesale Club, Inc. represents a marked departure from prior FTC actions because it was the first time the FTC used its unfairness authority and did not also allege deceptive practices for privacy and security misrepresentation.[125] Thus, unlike other cases, deception was not an issue in this matter.

BJ's Wholesale Club operated a number of membership warehouse stores.[126] As part of its normal business, BJ's accepted credit cards as a form of payment from its members.[127] BJ's collected personally identifiable information from its customers to authorize their credit cards.[128] It also used wireless technology, including wireless access points and scanners, to monitor inventory.[129] The FTC filed a complaint against BJ's, alleging that it had failed to encrypt information while it was in transit or stored on the network, stored personally identifiable information in a file format that permitted anonymous access, failed to use readily

121. *Id.* at 298–99.
122. *Id.* at 298.
123. *Id.* at 299.
124. *Id.* at 297.
125. *See* BJ's Wholesale Club, Inc., 140 F.T.C. 465, 468 (2005) (complaint); *see also* Joel B. Hanson, *Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements*, SHIDLER J.L. COMM. & TECH., May 23, 2008, at 1, 3, http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/412/vol4_no4_art11.pdf?sequence=1.
126. *BJ's Wholesale Club*, 140 F.T.C. at 466.
127. *See id.*
128. *Id.*
129. *Id.* at 466–67.

accessible security measures to limit access, failed to employ sufficient measures to detect unauthorized access or conduct security investigations, and created unnecessary business risks by storing information after it had any further use for the information, in violation of bank rules.[130]

The FTC alleged that as a result of this conduct millions of dollars in fraudulent purchases had been made.[131] Though there was no federal statute that the company's conduct violated directly, the FTC concluded that these acts constituted an unfair business practice under the FTCA and brought an enforcement action against BJ's.[132] This matter also was resolved via consent order, and the FTC required BJ's to implement a comprehensive information security plan, obtain a security assessment, and file reports over the next twenty years, as well as other administrative requirements.[133]

This case is notable because it represents a different enforcement pattern from prior FTC actions. In the past, the FTC had only acted in the security arena when a company was subject to heightened security burdens—under statutes such as HIPAA, COPPA, or GLB—or the company had made specific security promises. Here, the FTC has shown that even in the absence of a specific representation or a statutory burden, companies can face enforcement action for a lack of information security based upon the FTC's unfairness authority and not based upon deception. Thus, the unanswered question in *In re Vision I Properties, LLC* was answered by the FTC, and it is clear that the FTC views the lack of information security, whether there is a deceptive statement to consumers or not, as an unfair business practice.[134]

H. Other Unfairness Cases Based upon a Lack of Information Security

Though *In re BJ's Wholesale* was the first unfairness case based upon a lack of information security, it was certainly not the last. *In re DSW*,

130. *Id.* at 467.
131. *Id.*
132. *See id.* at 468 ("As described in Paragraphs 7 and 8 above, respondent's failure to employ reasonable and appropriate security measures to protect personal information and files caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was an unfair act or practice.").
133. *See id.* at 470–72 (decision and order).
134. *Id.* at 468 (complaint); *see, e.g.*, Vision I Props., LLC, 139 F.T.C. 296, 301–02 (2005).

Inc.,[135] *In re Reed Elsevier Inc. & Seisint, Inc.*,[136] *In re TJX Cos., Inc.*,[137] *In re CVS Caremark Corp.*,[138] though it also relied upon allegations of deception, and *In re Dave & Busters, Inc.*[139] all relied upon the FTC's unfairness authority to allege that a lack of data security, even without an alleged misrepresentation regarding privacy, was sufficient to establish a section 5 violation.

XI. THE CHALLENGES OF NOTICE-AND-CHOICE AND HARM-BASED MODELS

In its recent guidance, the FTC recognized that the notice-and-choice and harm-based models of enforcement had been criticized for a number of reasons. The notice-and-choice, deception, or Privacy 1.0 model, which requires some form of misrepresentation but only requires a likelihood of consumer injury, is perceived to have led to lengthy privacy policies that consumers do not read, which truly defeats the notice-and-choice theory completely.[140] The harm-based, unfairness, or Privacy 2.0 model, which requires significant consumer harm, has also been criticized by commentators for being too reactive,[141] and as is shown by the failures of privacy litigation, proving substantial harm is an elusive and often difficult achievement.[142]

Ultimately, although these concepts have formed the basis of the FTC's privacy enforcement efforts, the FTC recognized that these models had limitations, including the reactive nature of these doctrines.

---

135. 141 F.T.C. 117, 118–20 (2006) (complaint).

136. No. C-4226, 2008 WL 3150420, at *6 (F.T.C. July 29, 2008) (decision and order).

137. No. C-4227, 2008 WL 3150421, at *4 (F.T.C. July 29, 2008) (decision and order).

138. No. C-4259, 2009 WL 1892185, at *4 (F.T.C. June 18, 2009) (decision and order).

139. No. C-4291, 2010 WL 1249871, at *4 (F.T.C. Mar. 25, 2010) (consent agreement).

140. FED. TRADE COMM'N, *supra* note 2, at 26–27.

141. *See id.* at 33 n.86 ("George Washington University Law School Professor Daniel Solove has criticized the harm-based approach for being too 'reactive' and called for an architectural approach to protecting privacy that involves 'creating structures to prevent harms from arising rather than merely providing remedies when harms occur.'" (quoting Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1242 (2003)).

142. *See* Andrew B. Serwin, *Poised on the Precipice: A Critical Examination of Privacy Litigation*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 883, 885 (2009) ("However, the road to plaintiffs' recovery in privacy litigation is littered with a number of issues that can derail a case before it truly starts, not the least of which is that plaintiffs in many cases cannot prove actual damage, and may actually lack standing to bring an action. Moreover, even if the case clears this hurdle, many class actions fail the certification requirements because of issues unique to privacy litigation."); *see also* Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060, 2010 WL 2643307, at *2 (S.D.N.Y. June 25, 2010) (citing Serwin, *supra*, at 931–95).

That Privacy 2.0, the model advocated by Prosser and adopted by the FTC in its unfairness enforcement, has failed to address privacy concerns, particularly those created by innovation, is well established.[143] Privacy 2.0 is a harm- and tort-centric model created *by courts* when their decisions were now-famously placed in context by Prosser.[144] It has been the touchstone for privacy since 1960, but as the FTC recognized, Privacy 2.0 has been criticized for being too reactive and not keeping pace with innovation.[145] Indeed, to understand the latency of litigation one need only ask someone who is a party to it to describe his or her view of how long litigation can take to resolve. Moreover, based upon the past history of Privacy 2.0, it is clear that a litigation-based model will inherently fail to provide proactive guidance. Guidance under the Privacy 2.0 model comes from what published decisions are made by courts, or the few public settlements entered by government agencies, such as the FTC or state attorneys general. In many cases private litigation settles on confidential terms, and in any case, guidance under the Privacy 2.0 model is inherently limited by the discovery of issues and a party's, governmental or otherwise, willingness to litigate the problem. There are also jurisdictional limits on privacy litigation, both for private parties and for the FTC.[146]

These points illustrate, as more fully discussed below, that models based upon accountability—meaning enforcement—have already been tried in the United States and have failed. Both Privacy 1.0 and 2.0 focused on enforcement as the model to drive compliance, and the FTC, as well as many other commentators, recognized the limitations of these models.[147] This led the FTC to suggest a new model that was more proactive and provided more flexibility—the privacy-by-design framework.[148] Although the model is a significant step in the right

143. Solove, *supra* note 141, at 1228, 1232–33.
144. *See* Prosser, *supra* note 31, at 383, 389.
145. *See* FED. TRADE COMM'N, *supra* note 2, at iii.
146. Private parties face the problem that harm is often difficult to prove. The FTC faces the issue that its jurisdiction is not unlimited, and it can only act under section 5 if it can prove deception and a likelihood of harm or consumer injury that is "substantial." 15 U.S.C. § 45 (2006).
147. *See, e.g.*, Note, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1891 (2007) ("The dangers that accompany Privacy 2.0 . . . are capable of more invasive and damaging harms than were conceivable at the birth of the Internet. The law has yet to catch up to these new harms, but now it is time to try." (footnote omitted)).
148. FED. TRADE COMM'N, *supra* note 2, at 39–41.

direction, it will need to be defined in a more complete way before it can be implemented by businesses in a meaningful way.[149]

XII. UNDERSTANDING PROPOSED MODELS FOR PRIVACY

There are in essence three main proposed constructs for privacy being discussed. It is helpful to understand these models and what they propose in order to try and chart a path forward. Before that is examined, it is helpful to understand the basic structure of existing privacy laws and internal policies. Although privacy-by-design is a model being discussed, it is a model focused on implementation of privacy, and it is best placed in the first or second elements of what is discussed below.

Privacy laws do in essence three things: (1) classify or identify data that is to be regulated; (2) regulate the processing of data through conduct limitations, including the level of consent required to collect or use the data, data security limitations, use restrictions, and other limitations; and (3) provide for enforcement for violation of point (2). Internal policies that are adopted at companies regarding data governance do effectively the same thing: define what data is being covered, restrict its use, and provide for some form of enforcement, though the enforcement is much different from a consumer class action or an FTC enforcement action.

The point of identifying these three elements is to give context for the models that are being discussed, to help define what these models are and what they are not, and to argue that proportionality is the key principle that must be the basis of any new regime.

A. Model 3—Accountability

Models based upon accountability have been put forward by some as a viable solution to the privacy concerns of today, including the reactive nature of current privacy regimes.[150] You will note that though this is the first model I discuss, I list it as the third model, and the reason for that will become clear below.

---

149. Flexibility in meeting the challenges of the Web 2.0 has long been recognized as necessary by the FTC. Slade Bond, Comment, *Doctor Zuckerberg: Or, How I Learned To Stop Worrying and Love Behavioral Advertising*, 20 KAN. J.L. & PUB. POL'Y 129, 143 (2010) (citing Joel Winston, Fed. Trade Comm'n, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising: Behavioral Advertising: Tracking, Targeting, & Technology*, *in* 2 PRACTISING LAW INST., TENTH ANNUAL INSTITUTE ON PRIVACY AND DATA SECURITY LAW 411, 431 (2009)).

150. *See, e.g.*, Sudhir Aggarwal et al., *Trust-Based Internet Accountability: Requirements and Legal Ramifications*, J. INTERNET L., Apr. 2010, at 3, 3–6.

1. Prior Concerns Regarding Accountability

Although accountability has gained attention in recent times in the privacy realm, it is not a new concept in privacy and is in fact a concept that has been discussed in a number of different governance contexts. Although accountability has a role in governance, accountability is a concept that has been questioned at some level by other commentators. In an article that examined the role of accountability in public administration, one of the main challenges with accountability—defining what it actually means—was identified.[151] Noting the "chameleon" quality of accountability, one author noted, "Accountability is a cherished concept, sought after but elusive. New models of administrative reform promise to provide heightened accountability through managerial controls. Interviews with 15 Chief Executives of Australian public sector organisations reveal the chameleon quality of accountability. Accountability is subjectively construed and changes with context."[152]

Accountability has also been noted by some scholars as being an ever-expanding concept that has gone beyond its original purpose—external enforcement.

> But more recently, in academic usage at least, "accountability" has increasingly been extended beyond these central concerns and into areas where the various features of core "accountability" no longer apply. For instance, "accountability" now commonly refers to the sense of individual responsibility and concern for the public interest expected from public servants ("professional" and "personal" accountability), an "internal" sense which goes beyond the core external focus of the term. Secondly, "accountability" is also said to be a feature of the various institutional checks and balances by which democracies seek to control the actions of the governments (accountability as "control") even when there is no interaction or exchange between governments and the institutions that control them. Thirdly, "accountability" is linked with the extent to which governments pursue the wishes or needs of their citizens (accountability as "responsiveness") regardless of whether they are induced to do so through processes of authoritative exchange and control.[153]

Although some scholars have proposed solutions to these issues, acceptance of accountability, particularly in an expanded form, is far from unanimous. These concerns are important to factor in when accountability models for privacy are examined.

---

151. Amanda Sinclair, *The Chameleon of Accountability: Forms and Disclosures*, 20 ACCT., ORGS. & SOC'Y 219, 219–22 (1995).

152. *Id.* at 219.

153. Richard Mulgan, *'Accountability': An Ever-Expanding Concept?*, 78 PUB. ADMIN. 555, 556 (2000).

2. Accountability and Privacy

Accountability models in the privacy arena are, not surprisingly, focused on holding people accountable for what they do with data. "As a result, a growing faction in the cryptography and security community has embraced greater reliance on *accountability* mechanisms: When an action occurs, it should be possible to determine (perhaps after the fact) whether a rule has been violated and, if so, to punish the violators in some way."[154] Although accountability-based models must have rules of the road regarding a variety of topics, including security, use restrictions, and restrictions on third-party transfers, to mete out punishment for violation, an accountability model generally focuses on after-the-fact enforcement.

Apart from the general criticisms of accountability noted above, the flaw in a model that focuses on accountability is clearer to understand when one reexamines the three elements of laws identified above. A focus on accountability means a focus on the third element, which is the least important of the three elements. More importantly, a focus on enforcement ignores the last fifty years of privacy law in the United States, as well as the inherently retrospective nature of a model that is enforcement-centric. Simply put, accountability models inherently must focus on after-the-fact enforcement to set standards, and that is the opposite of a system that is proactive and voluntary—what the FTC is currently seeking.

Other accountability advocates argue that the model should be accountability-centric.[155] The problem with this argument is two-fold. As noted above, enforcement-centric models have been tried in the United States, and they have not worked, though external enforcement has been the basis of privacy theory since Prosser's 1960 article, which was based upon a court-created tort-centric model.[156] Moreover, to the extent that what these advocates are saying is really that there should be penalties for violating the law, it is a point that cannot be disputed because it underlies every existing law. If that is truly the argument, then it is not informative to privacy practitioners because there are always some consequences for violating a law and focusing on

154. Joan Feigenbaum, Accountability as a Driver of Innovative Privacy Solutions 2 (Oct. 2010) (unpublished manuscript), *available at* http://www.law.yale.edu/documents/pdf/ISP/Feigenbaum_Accountability.pdf.

155. *See, e.g.*, Jon S. Hoak, *HP Ethics from the Top Down . . . and the Bottom Up*, 33 U. DAYTON L. REV. 225, 227–28 (finding that the accountability model best protects personal data and privacy standards).

156. *See supra* text accompanying notes 143–46.

consequences does not provide the proactive guidance the FTC seeks to generate.[157]

There are some accountability models that focus more on data owners' being accountable for data in that they are required to take steps to control data, and this is seen as a way to encourage the adoption of best practices, which is in essence an expansion of the external focus of accountability as noted by Mulgan.[158] However, at this time there generally is not a fixed definition around what data should be protected and how it should be protected. Instead, there may be reference to internal values regarding information, or ethics, which highlights the chameleon quality of accountability concepts.[159] Said differently, the challenge with these types of accountability models is that information ethics is in the eye of the beholder. Left to their own devices, what privacy-centric and nonprivacy-centric companies will conclude is appropriate will vary dramatically, as noted by the FTC in its recent report.[160] Therefore, these models provide little guidance to companies that are not culturally privacy-centric and will not solve the problem as articulated by the FTC.

It should also be noted that any model based upon accountability inherently focuses on privacy in a different way than privacy-by-design. Privacy-by-design is a way to embed privacy into technology, and its express purpose is proactive prevention, not after-the-fact enforcement. Indeed, the first of the seven principles of privacy-by-design is:

> The *privacy-by-design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred—it aims to *prevent* them from occurring. In short, *privacy-by-design* comes before-the-fact, not after.[161]

Given any accountability model's inherent retrospective view, accountability and privacy-by-design are not concepts that take the same view of how to improve privacy. To the extent that accountability advocates argue that privacy-by-design makes organizations more

157. *See supra* Part XI and note 146. For a general discussion of privacy litigation, see ANDREW B. SERWIN, 2 INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE § 28 (2010).

158. Mulgan, *supra* note 153, at 555–56.

159. *Id.* at 555–60.

160. *See generally* FED. TRADE COMM'N, *supra* note 2.

161. Ann Cavoukian, *The 7 Foundational Principles*, PRIVACY BY DESIGN (Jan. 2011), http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

accountable for the data throughout the organization, this is really more a concept of responsibility for implementing appropriate processing restrictions, which is really a focus on the second point of three. Accountability as a model looks at enforcement, and an enforcement model without clear focus on data classification and processing limitations is an empty vessel that provides no guidance, which is what proportionality principles provide. At some level an accountability-centric model would be like passing comprehensive privacy legislation and simply saying, "If you violate someone's privacy you will be liable for a $10,000 fine," without defining what data is covered or what acts are prohibited. This is not what accountability advocates have put forward, and that guidance can be built in through data classification and processing limitations, but that illustrates the point—accountability is the third step in a three-step process and therefore should not be the focal point of privacy theory, particularly because the experience in the United States demonstrates accountability models have not worked.

B. Model 2—Models Based upon Processing Limitations

There is an emerging model of privacy that focuses on restrictions on processing of information, which are in some circles referred to as use-limitation models, though they go beyond mere use limitations. It is worth noting here that some advocates for privacy view use-limitation models as accountability models.[162] They are not. Use limitation is focused on restricting the use of information. Although there may be consequences for misuse, that does not turn a model focused on use restriction into an accountability model any more than it turns every existing privacy law in the United States that restricts the use of data into an accountability statute. This also becomes clear when one examines the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[163]

The OECD Guidelines identify a number of principles regarding the use of data. Three of them are of particular importance. First is the purpose specification principle, which states:

---

162. Andrew Shen, Comment to *Online Profiling Project*, *P994809/Docket No. 990811219-9219-01*, FED. TRADE COMM'N (Nov. 8, 1999), http://www.ftc.gov/bcp/workshops/profiling/comments/shen.htm.

163. *See* ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 3, 15 (1980), *available at* http://www.it.ojp.gov/documents/OECD_FIPs.pdf.

> The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.[164]

This is clearly a use-based principle. Second is the use-limitation principle, which states that "[p]ersonal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law."[165] Again, this is a use-based principle that is similar to what some have advocated. If accountability were about use limitation, these principles would be the accountability principle. They are not. There is also an accountability principle that states that a "data controller should be accountable for complying with measures which give effect to the principles stated above."[166] In other words, accountability is the enforcement mechanism for other principles that are defined in other ways. Without the other principles, accountability is simply an empty vessel, and use-based models provide a part of the framework needed for accountability.

Although use-based models themselves are not inherently incorrect, they focus on the second point of law, as noted above. Restrictions on the use of information are critical to any system, but they cannot be the underlying basis of the system because the decisions to restrict use must be based upon something, which is step one in the analysis. To continue the analogy from above, it would be like passing legislation that provides restrictions on the use of data without defining data in the first place. Again, that is not what advocates of use-based systems are arguing for, but it again illustrates the point that use-based restrictions only truly function as part of a system of proportional protections and penalties.

C. Model 1—Proportionality

In Privacy 3.0, I argued that it was widely recognized that the current theoretical construct of privacy—Prosser's tort-based enforcement or accountability model—had failed.[167] What was needed was a model that provided appropriate but not overinclusive or underinclusive protection,

164. *Id.* at 3.
165. *Id.*
166. *Id.* at 4.
167. Serwin, *supra* note 8, at 874–75.

particularly in the rapidly changing Web 2.0 world where information sharing was the basis of a number of now-ubiquitous services, such as Facebook.[168]

I also recognized that society would benefit from information sharing, though there should be restrictions, or use limitations, on the sharing.

> Instead, a theory of proportional protection places higher restrictions and access barriers on truly sensitive information that either has limited or no use to third-parties and has great capacity to damage individuals and society, while simultaneously permitting the necessary and appropriate access to those having a legitimate need to know certain information, particularly when that information is less sensitive. Proportionality also has the advantage of minimizing the societal impact of privacy issues because enforcement and compliance will be focused on the most appropriate levels of sensitive information.[169]

In other words, use limitations should be proportional to the sensitivity of data.

Although an examination of data elements for sensitivity could lead to improving privacy protection, that model did not seem to provide prospective guidance. As such, I proposed creating four tiers—highly sensitive, sensitive, slightly sensitive, and nonsensitive.[170] By creating these tiers, one could associate certain use restrictions and enforcement with each tier.[171] As noted below, I did not simply focus on sensitivity as part of proportionality but rather as a broader set of issues that needed to be defined once the four tiers of information were created. Thus, there are common elements that I will be discussing regarding each tier, including:

- whether information can be gathered without notice or consent;
- whether consent must be opt-in or opt-out;
- the effect of consent;
- the types of processing that can be done;
- can information be gathered under false pretenses;
- are there time restrictions upon the retention of the data;
- data security requirements;
- data destruction requirements;

---

168. When considering whether Prosser's model works for the Web 2.0 world, I stated:

> This Article argues that the answer is no and instead argues that the common law based prior scholarship was relevant for its day, but it cannot account for the technology and societal values of today, our statutorily-driven privacy protections, and the [FTC] enforcement centric model, and should therefore not provide the theoretical construct for existing or future laws or court decisions. This is all the more true in light of recent FTC guidance regarding behavioral advertising, in which the FTC expressly recognized the need to balance support for innovation and consumer protection, as well as the "benefits" provided to consumers by behavioral advertising.

Id. at 874.

169. *Id.* at 876.

170. *Id.* at 900.

171. *See id.* at 901.

- what steps are required, or permitted, to mitigate any mishandling of information; and
- penalties for misuse of the information, including the imposition of statutory penalties in certain cases.[172]

As is clear from these bullet points, use limitation, such as "the types of processing that can be done," and the effect of consent as well as accountability, such as the "penalties for misuse of the information, including the imposition of statutory penalties in certain cases," are inherent in proportionality.[173]

One could ask, How are these models different, and why should one predominate? The answer really is two-fold. The Privacy 3.0 model, by starting but not ending the analysis with data sensitivity, permits business and government to more efficiently focus resources on protecting the information that can create the most mischief if lost or misused, while simultaneously avoiding overregulation of data as well. Second, I think there is a significant "best practice" value in focusing first on sensitivity in the way I articulated in 2008.[174] As noted above, use limitation, consent, enforcement, and other issues would be defined by the tiers, not by the individual data elements themselves. The data elements would be examined based upon sensitivity and then placed into a tier. Once the individual data elements were placed into a tier, the use restrictions and other issues would flow from the tier, not the data element. Current use-limitation models tend to focus more on the data elements themselves, and there are two advantages of the approach I advocated. The first is that data sensitivity can change over time, and this system permits more flexibility for data to move to a higher or lower tier. The second is that it permits privacy to be more proactive. When a new technology is created that uses a new form of sensitive data, these tiers and the data elements placed within them can be examined, and companies seeking guidance can use past placement of data elements to appropriately protect new forms of data. To the extent that advocates of accountability believe in an ethics- or value-based accountability system, the tiers permit companies to make value judgments regarding a large number of data sets, including emerging forms of data, in a consistent and cohesive way.

172. *Id.* at 901–02.
173. *Id.* at 902.
174. *See id.* at 900.

Some commentators have suggested that this model of privacy does not account for the context of information.[175] This is an argument that does not factor in the complete model of proportionality. Although it is true that a pure data sensitivity analysis does not capture each and every context for data, the other elements identified above that flow from data sensitivity do factor in the context of data, particularly when use restrictions are created based upon sensitivity because the restrictions on use will vary in context and, more importantly, the restrictions will vary depending on who is attempting to process the data.

Ultimately, the issue is not choosing between use limitations, accountability, or sensitivity but rather what the first step in the process is. Focusing on proportionality in the method identified in Privacy 3.0 permits informed decisions to be made regarding use limitations and accountability. To focus on either without first addressing sensitivity so that use restrictions and accountability can be proportional runs the risk of having either too few or too many restrictions.

XIII. BAKING IT IN

There is a path that would provide more flexibility to the FTC and more guidance to business in the Web 2.0 World. I have previously proposed Privacy 3.0, which is a model based upon data sensitivity that makes the safeguards required to be implemented for personal information contextually connected to the sensitivity of that information using a proportional methodology.[176] Although this may seem like a radical departure from prior FTC enforcement, if the concept is put into different terms, it is truly just a small step away from prior guidance and enforcement, but this small step provides much-needed predictability and, perhaps even more importantly, flexibility as technology changes.

Stated differently, examining the sensitivity of data through the totality of the circumstances surrounding the individuals and the context of the personal information is simply determining the risk of harm that can result from the improper or unauthorized disclosure or use of the personal information. The more sensitive the data is, the higher the risk of harm to consumers. This is a different approach at a certain level from the prior enforcement cases because although likelihood of harm is considered by the FTC, it is typically only done so in the context of a deception case, which requires a misstatement of some kind regarding

175. *See, e.g.*, Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 17 (2007).

176. *See generally* Serwin, *supra* note 8 (describing the principal of proportionality as it relates to Privacy 3.0).

privacy.[177] Otherwise, the level of consumer injury for unfairness goes far beyond a risk of harm because actual harm appears to be required.

Moreover, if Privacy 3.0 were considered, it would not directly be the basis of enforcement by the FTC. Part of the rationale of using sensitivity rather than the Privacy 1.0 and 2.0 doctrines is that harm is frequently difficult to prove and therefore litigation frequently fails to address the stated concerns of individuals. Therefore, I would propose that the risk of harm analysis be used to create the Privacy 3.0 framework and the framework would be the basis of a safe harbor program administered by the FTC. The "Privacy 3.0 Safe Harbor" program would rely upon the four tiers of sensitivity, and as more fully detailed in Privacy 3.0, it would provide clear guidance regarding what information practices were permitted for each tier, including what level of consent, both implicit and explicit, would be required to process data.[178] Companies that agreed to and implemented the data classification framework, and the resulting restrictions and permissions that would be created based upon the sensitivity of information, would not be subject to enforcement action if there was a data incident. However, companies that voluntarily chose to participate in the Privacy 3.0 Safe Harbor would be subject to enforcement if they failed to meet the requirements of the program or falsely claimed to comply when they in fact did not.[179]

This program could follow the model of the European Union (EU) Safe Harbor program[180] or binding corporate rules (BCRs),[181] which are

177. *See, e.g.*, Vision I Props., LLC, 139 F.T.C. 296 (2005) (finding that renting out personal information was deceptive and violated customer's privacy).

178. Serwin, *supra* note 8, at 902–06. This safe harbor program would differ from the existing EU Safe Harbor program in its implementation and the contemplated level of detail in the filings and commitments. *See id.* at 884–89.

179. *See, e.g.*, Onyx Graphics, Inc., 74 Fed. Reg. 53,503, 53,504 (F.T.C. Oct. 19, 2009) (proposed consent agreement); Dirs. Desk LLC, 74 Fed. Reg. 53,247, 53,248–49 (F.T.C. Oct. 16, 2009) (proposed consent agreement); World Innovators, Inc., 74 Fed. Reg. 53,255, 53,256–57 (F.T.C. Oct. 16, 2009) (proposed consent agreement); Collectify Inc., 74 Fed. Reg. 53,254, 53,255 (F.T.C. Oct. 16, 2009) (proposed consent agreement); ExpatEdge Partners, LLC, 74 Fed. Reg. 53,250, 53,251–52 (F.T.C. Oct. 16, 2009) (proposed consent agreement); Progressive Gaitways Inc., 74 Fed. Reg. 53,249, 53,250 (F.T.C. Oct 16, 2009) (proposed consent agreement).

180. *See* Tracy DiLascio, *How Safe is the Safe Harbor? U.S. and E.U. Data Privacy Law and the Enforcement of the FTC's Safe Harbor Program*, 22 B.U. INT'L L.J. 399, 415–16 (2004); *U.S.-E.U. Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated Apr. 11, 2011).

181. *See Overview—BCR*, EUR. COMM'N, http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm (last updated Nov. 4, 2010).

approaches many companies are now using to comply with EU data protection laws. This would encourage international cooperation while simultaneously permitting companies that have implemented a program based upon the EU Safe Harbor or BCRs to build upon existing work by companies, though this model would focus protection on information by doing a data risk analysis under the "principle of proportionality."[182]

An additional side benefit from an economic standpoint is that such a program would remove uncertainty from the information environment, allowing organizations to provide protections and safeguards more efficiently by focusing security and protective resources on those data that are more sensitive. In turn, this could provide the economic stimulus to promote greater valuation in concepts such as privacy- or security-by-design, which would be driven through economic value because of reduced regulatory risk rather than using a sword of Damocles[183] over the head of any handler of consumer information—the carrot versus the stick approach.

This would give companies an incentive to proactively focus their compliance efforts on the most critical information and therefore proactively prevent consumer harm in many cases. Without a focus on sensitivity, compliance efforts can often be unfocused and not as efficient or as productive as otherwise possible.

Whether this is accomplished via the FTC's rulemaking authority, referenced in section 7, or whether additional legislation is required, pursuing a framework that incorporates Privacy 3.0, includes a safe harbor for those companies that choose to comply, and links in some form to the existing EU models will provide the appropriate combination of protections and incentives for businesses so that proactive privacy protection can be achieved in a way that maximizes international coordination and cooperation.

After the publication of this Article on the Social Science Research Network but prior to its publication in this journal, draft federal privacy legislation was announced by Senator Kerry.[184] The legislation

182. *See generally* SERWIN, *supra* note 157, § 37, at 1480–86 (explaining Privacy 3.0, the principle of proportionality). Tying the proposed program in some way to the existing BCR process would further the FTC's goal of increasing international cooperation and would also give companies further incentives to pursue the BCR process. It would also streamline a number of the international data transfer issues, at least with the EU. FED. TRADE COMM'N, THE FTC IN 2011: FEDERAL TRADE COMMISSION ANNUAL REPORT 54 (2011), *available at* http://www.ftc.gov/os/2011/04/2011ChairmansReport.pdf.

183. *See* Cavoukian, *supra* note 161.

184. Julia Angwin, *Senators Offer Privacy Bill To Protect Personal Data*, WALL ST. J., Apr. 13, 2011, http://online.wsj.com/article/SB10001424052748703385404576258942268540486.html; Press Release, John Kerry, Kerry Urges Common Sense Commercial Privacy

includes some of the concepts discussed in this Article, including a safe harbor, and it distinguishes between sensitive personally identifiable information and personally identifiable information, though it presents a model that is somewhat of a use-based approach.[185] This bill is discussed briefly because it is still in draft form and may be modified at a later time.

The bill places restrictions on "covered entit[ies]."[186] The term *covered entity* is defined as "any person who collects, uses, transfers or stores covered information concerning more than 5,000 individuals during any consecutive 12-month period" and is subject to FTC jurisdiction, as well as common carrier and nonprofit organizations.[187] The information covered by the bill includes (1) personally identifiable information; (2) sensitive personally identifiable information, which is personally identifiable information that "if lost, compromised, or disclosed without authorization . . . carries significant risk of economic or physical harm"; and (3) unique identifiable information, defined as "a unique persistent identifier associated with an individual or a networked device."[188] Additionally, the bill covers "any information that is collected . . . in connection with personally identifiable information or unique identifier information."[189]

The bill creates obligations by creating certain rights for individuals, and through this, the bill creates certain compliance obligations on covered entities.[190] This includes the right to security and accountability, which requires the FTC to institute a rulemaking process within 180 days to implement this right.[191] There is also a right to notice and individual participation, as well as the right to purpose specification, data minimization, constraints on distribution, and data integrity.[192] Violation of these requirements and the implementing rules is considered to be an

---

Protections (Mar. 16, 2011), *available at* http://kerry.senate.gov/press/release/?id=d18a9191-7fa3-437c-af24-3b6ca3a28f10.

185. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. §§ 3(6), 202(b), 501(a) (2011); Angwin, *supra* note 184.

186. S. 799 § 3(2); Andrew Serwin & Megan O'Sullivan, *New Post on the Kerry Bill*, PRIVACY & SECURITY SOURCE (Mar. 29, 2011), http://www.privacysecuritysource.com/new-post-on-the-kerry-bill/.

187. S. 799 §§ 3(2)–(3), 401.

188. *Id.* § 3(3), (6), (9).

189. *Id.* § 3(3)(A)(iii).

190. *Id.* §§ 101, 201, 301.

191. *Id.* § 101(a).

192. *See id.* §§ 201–202, 301–303.

unfair and deceptive trade practice under the FTCA.[193] This bill can be enforced by the FTC or state attorneys general, and civil penalties are available for the violation of the bill.[194] There is no private right of action for the violation of the bill, and the bill would preempt many aspects of existing state laws, though there are several carve-outs from preemption.[195]

The bill also contains a safe harbor for a company that creates its own program that exempts the company from compliance with the FTCA, though the program must be "substantially the same as or more protective of privacy" than the requirements of the bill.[196]

The bill is still in draft form, and it is unclear what modifications, if any, will be made before it is introduced and whether it will be considered by Congress and adopted, but it is an important first step in the process of creating federal privacy legislation that encourages the adoption of comprehensive privacy programs, though it does not incorporate certain ideas that are suggested in this Article that would likely encourage broader adoption of best practices.[197]

XIV. CONCLUSION

Whatever nomenclature is used to describe Privacy 1.0 and 2.0, it cannot be questioned that these models have failed, and the FTC's report raises legitimate questions about prior privacy enforcement models and their value in a Web 2.0 world. Given the current business models of the Internet, privacy models must change in order to create the appropriate incentives for business to adopt best practices and protect consumer privacy in an appropriate way. If change is truly desired, then we must turn away from prior failed models, such as enforcement-centric models that have not worked and that have been criticized by many scholars. The new path must provide appropriate incentives for business to adopt best practices that are proportional to the sensitivity of data. In short, Privacy 3.0 must be based upon the principle of proportionality.

193. *Id.* § 402 ("A knowing or repetitive violation of a provision of this Act . . . shall be treated as an unfair or deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.").

194. *See id.* §§ 402–404.

195. *Id.* §§ 405–406.

196. *Id.* § 502(a).

197. The bill has been referred to the Senate Committee on Commerce, Science, and Transportation, the first step in the legislative process. *See S. 799: Commercial Privacy Bill Act of 2011*, GOVTRACK.US, http://www.govtrack.us/congress/bill.xpd?bill=s112-799 (last updated May 2, 2011).