February 10, 2011

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

Andrew B. Serwin
The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices.

Andrew Serwin.\(^1\)

Abstract

This article examines the history of privacy enforcement by the Federal Trade Commission, including the FTC’s jurisdiction under Section 5, and its privacy enforcement matters, as well as the FTC’s recently issued report, "Protecting Consumer Privacy in an Era of Rapid Change: A proposed Framework for Businesses and Policymakers", in which the FTC examines past enforcement models, noting their failings. In light of the FTC’s examination of past enforcement models, this article then analyzes these models, including the accountability-centric model that has previously been utilized in the United States, as well as the FTC’s proposed solution to the privacy problems of the Web 2.0 World—the adoption of best practices, including a "privacy by design" framework. The article then argues that the method to achieve the FTC’s goal of voluntary adoption of best practices is to focus on proportional protection for data based upon the sensitivity of the data in question, and to create a "safe harbor" from enforcement for businesses that choose to adopt the framework. This proposed framework could be linked in a meaningful way to existing EU processes, such as Binding Corporate Rules or the existing EU Safe Harbor program. By combining these elements, the FTC can achieve meaningful and focused self-regulation and provide appropriate protection to consumers, while giving business

\(^1\) Andrew B. Serwin is the founding chair of the Privacy, Security, and Information Management Practice and is 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 – 2009-2010 in the area of National: Privacy & Data Security, where he was described by clients as “a tireless worker, holding onto the ever-shifting puzzle pieces of the law in this area in a way that other privacy lawyers cannot” as well as by Legal 500 in Data Protection and Privacy. Mr. Serwin was also designated as a “Southern California Super Lawyer” from 2007-2010, and selected by his peers for inclusion in The Best Lawyers in America® 2010 and 2011 in the field of information technology law.

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 4,000 page treatise that examines all aspects of privacy and security laws, published by Thomson-West, which has been called “the best privacy sourcebook”, “an indispensable resource for privacy professionals at all levels”, and “a book that everybody in the information privacy field should have on their desk”. The treatise has been cited as authority by the Fourth Circuit in Ostergren v. Cuccinelli, 615 F.3d 263 (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”, 42 U. Mich. J.L. Reform 869 (2009) and “Poised on the Precipice: A Critical Examination of Privacy Litigation”, 25 Santa Clara Computer & High Tech. L.J. 883, cited by Hammond v. The Bank of New York Mellon Corp., 2010 WL 2643307, (S.D.N.Y., June 25, 2010), and Joseph Oat Holdings, Inc. v. RCM Digesters, Inc., 2010 WL 5065037, (3rd Cir. December 13, 2010).
an incentive to adopt best-practices, and also increase the level of international cooperation regarding privacy.
1. Introduction ...................................................................................................................... 5
2. What are the issues People are Concerned About? ...................................................... 6
3. The FTC--A Historical Perspective ............................................................................. 7
   a. The Formation of the FTC. ..................................................................................... 7
   b. The History of Privacy Enforcement. ................................................................. 8
4. The FTC’s Jurisdiction ................................................................................................. 10
5. Understanding the Theoretical Basis of the FTC’s Privacy Enforcement ............ 10
6. Understanding Section 5 ............................................................................................ 13
7. Unfair or Deceptive Acts or Practices--Rulemaking Authority. ............................ 13
8. Deception ..................................................................................................................... 14
   a. Likely to Mislead. ................................................................................................. 14
   b. The Act or Practice Must be Considered from the Perspective of the Reasonable Consumer................................................................. 15
   c. Materiality ........................................................................................................... 16
   d. Summarizing the Deception Elements. ............................................................... 17
   e. Deception and Notice and Choice Models of Enforcement......................... 17
9. Unfairness Authority .................................................................................................. 18
   a. The FTC’s December 1980 Statement Regarding Unfairness....................... 19
      i. Consumer Injury. ...................................................................................... 19
      ii. Violation of Public Policy ....................................................................... 21
      iii. Unethical or unscrupulous conduct......................................................... 22
   b. Distilling the Unfairness Statement. ................................................................. 22
   c. Unfairness and Harm-based Enforcement Models ......................................... 23
10. Enforcement Cases .................................................................................................... 23
    a. In the Matter of GeoCities—A Traditional Deception Model......................... 23
    b. In the Matter of ReverseAuction.com, Inc.—The Appearance of Unfairness. ......................................................................................................................... 25
    c. In the Matter of Eli Lilly—Voluntary Assumption of Heightened Burdens ...... 26
    d. In the Matter of Microsoft—A Continuation of Eli Lilly.................................. 27
    e. Misrepresentations Serving as the Basis for a Section 5 Deception Claim. ...... 27
    f. In the Matter of Vision I Properties, LLC—A New Model of “Deception” ...... 27
    g. In the Matter of BJ’s Wholesale Club, Inc. ...................................................... 28
    h. Other Unfairness Cases Based upon a Lack of Information Security. .......... 29
11. The Challenges of Notice and Choice and Harm-Based Models. ............................ 29
12. Understanding Proposed Models for Privacy ............................................................ 30
    a. Model 3--Accountability .................................................................................. 31
       i. Prior Concerns Regarding Accountability ................................................... 31
ii. Accountability and Privacy ................................................................. 32
b. Model 2--Models Based upon Processing Limitations ..................... 34
c. Model 1—Proportionality ................................................................. 35

13. Baking It In ......................................................................................... 37

14. Conclusion ....................................................................................... 39

1.
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 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 FTC Act to provide the FTC with authority to address harms to consumers. 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.

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 outreach2, 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 innovations by a range of companies are encouraging, many companies – both online and offline – do not adequately address consumer privacy interests.3

Said differently, while 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

---

2 Protecting Consumer Privacy in an Era of Rapid Change: A proposed Framework for Businesses and Policymakers, (December 2010)(“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.”).

3 Protecting Consumer Privacy, supra, note 2.
self-regulation, and to guide Congress. It also places the FTC’s prior privacy enforcement efforts in two categories—the “notice-and-choice” and “harm-based” models. While 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”.

The FTC is not the only entity looking at how to solve these issues. A number of groups and commentators have made suggestions regarding what model of privacy will help change the path of privacy. They 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.

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 then examine the FTC’s use of its deception and unfairness authority in privacy enforcement cases, then examine 3 proposed theoretical models for privacy, and finally will 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 voluntarily program, 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.

2. **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...

---

4 Protecting Consumer Privacy, supra note 2, at i, “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.”

5 Protecting Consumer Privacy, supra note 2, (“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 are often invisible to consumers.”).
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.\(^6\)

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.

While 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 Cooperation in the Enforcement of Laws Protecting Privacy (the “Recommendation”). 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.\(^7\)

3. **The FTC--A Historical Perspective.**

a. **The Formation of the FTC.**

The Federal Trade Commission was originally created in 1914 in order to protect competition between businesses. The original FTC Act was enacted concurrently with the Clayton Act, the

\(^6\) Protecting Consumer Privacy, supra note 2, page iv.

\(^7\) Protecting Consumer Privacy, supra note 2, page 17. The FTC also noted that in 2007 there was a recommendation from the OECD that OECD member countries should foster the establishment of an informal network of privacy enforcement authorities and should cooperate with each other to address cross-boarder issues arising from enforcement of privacy laws. See OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy. See also, [http://www.ftc.gov/opa/2010/09/worldprivacy.shtm](http://www.ftc.gov/opa/2010/09/worldprivacy.shtm), last visited December 31, 2010.
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. The original powers of the agency certainly did not include authority outside the examination of anti-competitive 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.  

This stands in stark contrast to the FTC of today, which on its website brands itself as the “nation’s consumer protection agency.” The FTC’s self-professed agenda is “to prevent fraud, deception, and unfair business practices in the marketplace.” The change in focus for the FTC to include consumer protection was achieved via amendments to Section 5 of the FTC Act in 1938 when the Act was extended to cover consumers, primarily through the addition of authority to address unfair and deceptive acts or practices. The 1938 amendments also granted the FTC more flexibility in addressing practices before they have reached a conclusion and had a significant and long term effect.

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. The FTC has subsequently expanded its efforts to protect consumer’s 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.”

---


10 Id.

11 FTC v. The Sperry and Hutchinson Co., 405 U.S. 233, 235, 92 S.Ct. 898 (1972) (“1938 Wheeler-Lea amendment 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 s 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.’ H.R.Rep.No.1613, 75th Cong., 1st Sess., 3 (1937). See also, S.Rep.No.1705, 74th Cong., 2d Sess., 2-3 (1936).”); FTC v. Colgate-Palmolive Co., 380 U.S. 374, 85 S. Ct. 1035, 1042 (1965); Guziak v. FTC, 361 F.2d 700, 703 (8th Cir. 1966).

12 Fashion Originators’ Guild of America v. Federal Trade Commission, 312 U.S. 457, 312 U.S. 668, 61 S. Ct. 703, 707, 48 U.S.P.Q. 483 (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. Federal Trade Commission, 159 F.2d 940, 73 U.S.P.Q. 203 (C.C.A. 6th Cir. 1947); Ford Motor Co. v. Federal Trade Commission, 120 F.2d 175 (C.C.A. 6th Cir. 1941).

13 Protecting Consumer Privacy, supra note 2, pg. ii.

14 Protecting Consumer Privacy, supra note 2, pg. iii.
For the FTC, the notice-and-choice model began in 2000, with the FTC recommending that Congress require business to comply with the Fair Information Practice Principles, which include notice and choice. Congress did not pass this legislation, so the FTC focused initially on raising public awareness, encouraged self-regulation, and also brought cases under Section 5 based upon its deception authority.\textsuperscript{15} Deception, as noted below, focuses on what “material” information the consumer was, or wasn’t told, particularly where the deception impacts a consumers’ choice regarding goods or services. Moreover, while 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.”\textsuperscript{16}

The second enforcement model, the harm-based approach represented a departure from the notice-and-choice model. While 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.\textsuperscript{17}

Both models have faced criticisms, 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.\textsuperscript{18} However, these models, despite these criticisms, are key to understanding the FTC’s pattern of enforcement and to beginning the discussion of the appropriate theoretical model for the future.

\textsuperscript{15} “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’ 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.” Protecting Consumer Privacy, supra note 2, pgs. 8-9.

\textsuperscript{16} In the Matter of Clifdale, 103 F.T.C. 110 (1984).

\textsuperscript{17} See, e.g., FTC v. Accusearch, Inc., 570 F.3d 1187 (10th Cir. 2009).

\textsuperscript{18} Protecting Consumer Privacy, supra note 2.
4. **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 basis of FTC jurisdiction is based upon practices being “unlawful” under the FTC Act, and the two main basis for finding a practice to be unlawful are Sections 5 and 12 of the FTC Act, also known as 15 U.S.C.A. §§ 45 and 52 respectively. Section 5 prohibits “deceptive” and “unfair” acts or practices, and Section 12 prohibits false advertisements.\(^{19}\) The FTC also has responsibility for enforcement of a number of other laws, including the Fair Credit Reporting Act, one of the United State’s first federal privacy laws, as well as others such as Gramm-Leach-Bliley, and the Children’s Online Privacy Protection Act.\(^{20}\)

While these other grounds for enforcement can have implications for privacy, the main focus of the FTC, and consequently this article, will be Section 5 and the FTC’s authority regarding deception and unfair practices or acts.

5. **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 the famous Warren & Brandeis law review article, *The Right to Privacy*, which is characterized by “the right to be let alone”.\(^{21}\) 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.\(^{22}\) Notably, Warren & Brandeis rejected harm-based models when they

---

\(^{19}\) Like many state versions of the FTC Act, a false advertisement that violates Section 12 is both independently unlawful, as well as a violation of Section 5. 15 U.S.C.A. § 52(b); see also, Cal. Bus. & Prof. Code §§ 17200 and 17500.


\(^{22}\) 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.

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
championed the right to be let alone. 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 (i.e. an understanding of the potential occurrence) of the potential privacy invasion, and you have the opportunity to choose to be let alone (i.e. freedom to determine when and where one’s information is disclosed or used).

While 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 ultimately he concluded that a harm-based model, which was later memorialized in the Restatement (Second) Torts, was the appropriate model. This harm-based model was Privacy 2.0 and it ultimately resulted in the now four familiar privacy torts.

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, PRIVACY 3.0--THE PRINCIPLE OF PROPORTIONALITY, 42 U. Mich. J.L. Reform 869 (2009)(internal citations omitted).

23 Id.

24 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. Id., at 883 (internal citations omitted).
The FTC has used similar models, and characterized them in the same terms, but identifies the timing of Privacy 1.0 and 2.0 a bit differently.\textsuperscript{25} As noted in Section 3(b), the FTC has primarily used two different models to promote consumer privacy: a notice and choice model, characterized by the Fair Information Practice Principles; as well as a harm-based approach.\textsuperscript{26} The FTC recognizes that these models have been subject to criticisms, including that they have failed to keep pace with rapidly evolving technology. The notice and choice model has resulted in lengthy privacy policy, 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.\textsuperscript{27} These challenges are ultimately not a complete surprise given that the 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 & 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 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.

\textsuperscript{25}“So, let’s go back and think about what Privacy 1.0 was. Privacy 1.0 from my perspective was the notice and choice model, or what we used to call Fair Information Principles and it’s something that everyone is familiar. In fact General McKenna [Washington Attorney General Rob McKenna (R)] was touching on it. It basically started in the mid-1990s and the FTC and the states were looking at privacy issues through this lens. They were looking for notice, choice, access and security with respect to information. And they evaluated, we all evaluated, privacy policies on the web that way, we looked at practices of companies that way, we looked at various self-regulatory regimes through that lens.

But shortly after the Gramm-Leach-Bliley Act (the “GLB”) was enacted the Federal Trade Commission, as some of you may know, switched gears, and moved from Privacy 1.0 to Privacy 2.0. So it moved from the concept of fair information principles to a harm model. And the harm-model was first launched by then Chairman Tim Murris, but it has since has been picked up by many, many folks including in the states. The harm model is one that focuses on harmful practices that present risks of physical security or economic injury. So the things that the Federal Trade Commission started focusing on and frankly the states started focusing on were data security, data breaches, which are a subset of data security, identity theft, children’s on-line privacy, and things like spam, spyware and telemarketing through the national do-not-call list. So just focusing on the first two, data security and data breaches, what a lot of the regulators did during this timeframe was focus on how to enhance tools that the federal government and the states had with respect to data security and data breaches.” A video recording of the presentation can be found at \url{http://blogs.berkeley.edu/2010/07/21/commissioner-brill-and-privacy-3-0-at-the-cwag-privacy-panel-2/}, last visited Aug. 10, 2010.

\textsuperscript{26}Protecting Consumer Privacy, supra note 2; \url{http://www.ftc.gov/reports/privacy3/fairinfo.shtm}, last visited December 31, 2010.

\textsuperscript{27}“Protecting Consumer Privacy, supra note 2, page 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.
6. **Understanding Section 5.**

15 U.S.C.A. § 45, also known as Section 5 of the FTC Act, provides the basis for FTC actions against unfair and deceptive trade practices. Specifically, ‘The 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.’ The Commission may prevent persons, partnerships, or corporations, with certain exceptions, from using unfair methods of competition or unfair or deceptive acts or practices in commerce.

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. Over time, courts and the FTC worked to define its authority in the deception and unfairness arenas. While this was occurring, there was a 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. Over time a number of Section 5 cases have been premised upon allegations arising from privacy and information security issues.

7. **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.

---


30 This includes banks, savings and loan institutions described in 15 U.S.C.A. Section 57a(f)(3), Federal credit unions described in 15 U.S.C.A. Section 57a(f)(4), 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.


34 15 U.S.C.A. § 57a(a)-(b)(1). “When prescribing a rule, the Commission must (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
Generally speaking, prior to the publication of any notice of proposed rulemaking, the Commission must publish an advance notice of proposed rulemaking in the Federal Register. The advance notice must contain a brief description of the area of inquiry under consideration, the objectives which the Commission seeks to achieve, and possible regulatory alternatives under consideration by the Commission; and invite the response of interested parties with respect to such proposed rulemaking, including any suggestions or alternative methods for achieving such objectives.\(^\text{35}\)

The Commission must also submit such advance notice of proposed rulemaking to the Committee on Commerce, Science, and Transportation of the Senate and to the Committee on Energy and Commerce of the House of Representatives.\(^\text{36}\)

8. **Deception.**

Defining a deceptive trade practice was not a straight forward 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. 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 the Matter of Cliffdale*, 103 F.T.C. 110 (1984), 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 consumers acting reasonably under the circumstances; and the representation, omission, or practice is material. 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.\(^\text{37}\)

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.\(^\text{38}\) This requirement was also discussed in *In the Matter of Cliffdale Associates*, 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.”


\(^{37}\) *Sears Roebuck and Co.*, 95 F.T.C. 406 (1980), aff’d, 676 F.2d 385 (9th Cir. 1982).

where the FTC stated that the requirement 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.\(^{39}\) 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 been well established. One is that under Section 5 actual deception of particular consumers need not be shown.\(^{40}\)

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.”\(^{41}\) 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.\(^{42}\)

\(^{39}\) See generally, Deception Statement, supra note 38.

\(^{40}\) Statement of Basis and Purpose, Cigarette Advertising and Labeling Rule, p. 84, 29 FR 8324 (1964).

\(^{41}\) Deception Statement, supra note 38.

\(^{42}\) Deception Statement, supra note 38; citing, Heinz W. Kirchner, 1963 WL 66830, 63 F.T.C. 1282, 1290 (1963); see also, See, e.g., American Home Products, D. 8918 (1981) [98 F.T.C. 136]; Sterling Drug, D. 8919 (July 5, 1983) [102 F.T.C. 395]; Bristol-Myers, D. 8917 (July 5, 1983) [102 F.T.C. 21]. This was reaffirmed by the FTC in Cliffdale, 103 F.T.C. 110 (1984) (“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 (sic) 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 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.”).
However, the FTC will analyze specific market segments of consumers if the act or practice is targeted to a particular group.43

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?44

c. Materiality.

The last element identified by the FTC was that the representation, omission or practice be material for deception to be found.45 In essence, the FTC examines whether the information was important to consumers—i.e. whether it affects consumers’ choices.46 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.47 If the claim is implied the FTC will examine 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

43 Deception Statement, supra note 38; Heinz W. Kirchner, 63 F.T.C. 1282 (1963); Ideal Toy Co., 64 F.T.C. 297, 310 (1964).

44 Deception Statement, supra note 38.

45 Deception Statement, supra note 38.

46 The Deception Statement defined 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.” Deception Statement, supra note 39; In In the Matter of Cliffdale Associates, Inc., the FTC formulated the standard in a similar way. “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.”), citing, American Home Products; Ford Motor Co., 84 F.T.C. 729 (1974), modified, 547 F.2d 954 (6th Cir. 1976), reissued, May 16, 1977 (slip opinion). See Statement of Basis and Purpose, Cigarette Advertising and Labeling Rule.”

nature of the transaction. 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 be less likely to make the purchase, but for the deception. In *In Re the Matter of 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 purposes sold."

\[48\]

\[49\]

\[50\]

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 slightly different order than discussed above. The FTC must prove: (1) a material representation, omission, or practice; (2) that is likely to mislead consumers; that (3) are acting reasonably in the circumstances. As noted above, the FTC is not required to prove that the defendants intended their misrepresentations to defraud or deceive, or made them in bad faith.

\[51\]

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. 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.

\[52\]

\[53\]
9. 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. The Supreme Court expanded on this view in *FTC v. The Sperry and Hutchinson Co.*, 405 U.S. 233, 92 S.Ct. 898 (1972), and noted 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 further identifying the particular practices to which it this phrase was intended to apply.

The second question the Supreme Court resolved was whether the FTC’s jurisdiction went beyond conduct that violated the “letter or 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 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? The Supreme Court concluded that the answer to both questions was yes and, as such, did not require the FTC to show a violation of antitrust laws to declare a practice to be unfair.

---


55 “Senate Report No. 597, 63d Cong., 2d Sess., 13 (1914), 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.’ . . . 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.” *R.F. Keppel*, at 310, 54 S.Ct., at 425.

56 “Congress, as previously recognized by this Court, see *FTC v. R. F. Keppel & Bros.*, 291 U.S. 304, 54 S.Ct. 423, 78 L.Ed. 814 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. Pp. 903-906. . . . 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,
Though not central to its holding, the *Sperry & Hutchinson* Court also recognized that prior Commission 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; (3) whether it is unethical or unscrupulous. While these decisions answered two key initial questions regarding the FTC’s unfairness authority, a number of cases and a statement from the FTC was necessary to help further define the somewhat elusive concept of 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 invoking false or deceptive commercial advertising. 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. The Unfairness Statement is reproduced in an appendix to *In the Matter of International Harvester*. While 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.

While 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 are discussed below, though ultimately the FTC in essence collapsed all three factors into the consumer injury prong of the Sperry & Hutchinson factors.

i. Consumer Injury.

Recognizing that preventing consumer injury was the focus of the FTC Act, the FTC stated its view that consumer injury alone can be sufficient to support a finding that a practice is unfair.


58 While 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.

59 Unfairness Statement, supra, note 57.

60 Id., citing *Sperry & Hutchinson Co.*, supra, note 57; *FTC v. R.F. Keppel & Bro.*, supra, note 57.

61 Unfairness Statement, supra, note 57, (“Unjustified consumer injury is the primary focus of the FTC Act, and the most important of the three S & H criteria. By itself it can be sufficient to warrant a finding of
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 which consumers could not have reasonably avoided. 62

In assessing the first injury factor, the FTC requires that any consumer injury must be substantial, and not based upon trivial or speculative harms. 63 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. 64 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 (in cases from being stalked or otherwise harassed) and substantial costs in changing telephone providers, caused “substantial harm, when it assessed whether the practices by defendants were unfair under Section 5. 65

In assessing the second injury factor, the FTC stated that it would consider the cost and benefit “tradeoffs” and would only find 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. 66 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. 67

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.”), citing 83 Cong.Rec. 3255 (1938) (remarks of Senator Wheeler).

62 Unfairness Statement, supra, note 57.

63 Unfairness Statement, supra, note 57.

64 Unfairness Statement, supra, note 57.

65 FTC v. Accusearch, Inc., 570 F.3d 1187 (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 these issue.

66 Unfairness Statement, supra, note 57, (“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.”).

67 Unfairness Statement, supra, note 57, (“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
ii. Violation of Public Policy.

In assessing the second Sperry & Hutchinson factor, the FTC stated that this factor examines whether the alleged conduct violates public policy “as it has been established by statute, common law, industry practice, or otherwise.” 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, it can be considered for a “dispositive legislative or judicial determination that such injury is present.”

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 a 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.

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 little surprise that the FTC stated that it generally considered the violation of public policy prong to be part of its examination of the evidence of consumer injury for the first Sperry & Hutchinson element.

---

68 Unfairness Statement, supra, note 57.
69 Unfairness Statement, supra, note 57.
70 Unfairness Statement, supra, note 57.
71 Unfairness Statement, supra, note 57, (“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..."
iii. Unethical or unscrupulous conduct.

While the FTC identified the third Sperry & Hutchinson factor in the Unfairness Statement, it dismissed it as largely duplicative as in the FTC’s view conduct that was unethical would typically produce consumer injury or violate policy.\(^{72}\)

b. Distilling the Unfairness Statement.

Ultimately, the focus on consumer injury in unfairness cases permit the distillation of the Sperry & Hutchinson factors into an examination of the consumer injury prong, which was ultimately codified in Section 5. At the time the Unfairness Statement was issued there was a dispute over whether the FTC’s authority in certain areas, including regarding 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.A. § 45(n), which now reflects the consumer injury focus and under this formulation practice is unfair if 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.\(^{73}\)

Recognizing the FTC’s statements regarding the somewhat subordinate role of public policy, § 45(n) also states: “In 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.”\(^{74}\)

Consistent with these amendments, the FTC has stated its view that an act or practice is unfair if

---

\(^{72}\) Unfairness Statement, supra, note 57, (“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.”)

\(^{73}\) FTC v. Accusearch, supra note 17, citing 15 U.S.C.A. § 45(n); American Financial Services Assn. v. FTC, 767 F.2d 957 (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. See Letter from Federal Trade Commission to Senators Ford and Danforth (Dec. 17, 1980), reprinted in H.R.Rep. No. 156, Pt. 1, 98th Cong., 1st Sess. 33-40 (1983).”) (internal citations committed).

\(^{74}\) 15 U.S.C.A. § 45(n).
the injury it causes, or is likely to cause, is: substantial; not outweighed by other benefits; and is not reasonably avoidable.\textsuperscript{75}

While there are not a significant number of cases that have litigated the scope of the FTC’s unfairness authority, there are some that have provided further guidance and approved the factors referenced above.\textsuperscript{76}

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.

10. Enforcement Cases.


*In the Matter of 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.”\textsuperscript{77} 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 request—but in actuality the personal identifying information collected through GeoCities’s New Member Application form was not just used for those limited purposes and that GeoCities had also sold, rented, or otherwise marketed or disclosed this information, including information collected from children, to third parties who have used this information for purposes other than those for which members have given permission. The FTC therefore alleged that the representations made by GeoCities were false and misleading. Therefore, the representation set forth in Paragraph 13 was, and is, false or misleading.\textsuperscript{77}

The matter resolved via consent judgment, with a 20 year duration, that placed a number of requirements that would over time become more familiar to companies that became subject to


\textsuperscript{76} See, *Spiegel, Inc. v. FTC*, 540 F.2d 287 (7th Cir. 1976)(citing with approval the *Sperry & Hutchinson* unfairness factors); *Orkin Exterminating Company, Inc. v. FTC*, 849 F.2d 1354, 1364-65 (11th Cir. 1988)(applying Unfairness Statement factors); *FTC v. IFC Credit Corp.*, 543 F.Supp.2d 925, (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.”)

\textsuperscript{77} [http://www.ftc.gov/os/1999/02/9823015cmp.htm](http://www.ftc.gov/os/1999/02/9823015cmp.htm), last visited December 31, 2010.
consent judgments. 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;
- Cannot 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;
- Must post a clear and prominent notice on its Web Site explaining GeoCities’ practices with regard to its collection and use of personal identifying information. The notice must include the following: (i) what information is being collected; (ii) its intended use(s); (iii) the third parties to whom it will be disclosed; (iv) how the consumer can obtain access to the information; and (v) how the consumer can have the information removed from GeoCities’ databases. The notice must appear on the Web site’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;
- Must 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”;
- Must notify all consumers (in the case of children, their parents) and to give them an opportunity to have their information removed from GeoCities’ and third parties’ databases;
- Must retain certain personally identifiable information in its “archived database” for the limited purposes of site maintenance, computer file back-up, blocking a child’s attempt to register without parental consent, or to respond 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 must place a clear and prominent hyperlink within its privacy notice directing visitors to the FTC’s Web site to view educational material on consumer privacy;
- Must meet certain recordkeeping requirements;
- Must 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 to file compliance reports with the Commission.

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 – years, though as will be shown by

---

78 This matter was also the first children’s online enforcement matter, which occurred prior to the enactment of COPPA.
following consent judgments, there was some indication that deception would not be the exclusive basis for FTC enforcement in the privacy arena.

b. **In the Matter of 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. ReverseAuction.com then allegedly took this information and spammed the eBay users, falsely representing their eBay account was going to expire. ReverseAuction.com was a competitor of eBay and it was alleged to have done this to promote its own website. 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. When the consent judgment and complaint was reviewed by the Commissioners it drew separate opinions from three of the Commissioners—Commissioners Thompson, Swindle, and Leary regarding the alternative use of the FTC’s unfairness authority. Commissioners Swindle and Leary concurred in part and dissented in part, because while 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.

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. Specifically, Commissioner Thompson stated:

**79** “17. 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 themselves and not outweighed by countervailing benefits to consumers or to competition.” 15 U.S.C.A. § 45(n) (emphasis added). 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." Letter from the Commission to the Consumer Subcommittee of the Senate Committee on Commerce, Science, and Transportation, *Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction*, 4 Trade Reg. Rep.(CCH) ¶ 13.203 (Dec. 17, 1980), reprinted in *International Harvester, Inc.*, 104 F.T.C. 949, 1070-76 (1984). 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.” [http://www.ftc.gov/os/2000/01/reversecmp.htm](http://www.ftc.gov/os/2000/01/reversecmp.htm), last visited December 31, 2010.

**80** “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." 15 U.S.C.A. § 45(n) (emphasis added). 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." Letter from the Commission to the Consumer Subcommittee of the Senate Committee on Commerce, Science, and Transportation, *Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction*, 4 Trade Reg. Rep.(CCH) ¶ 13.203 (Dec. 17, 1980), reprinted in *International Harvester, Inc.*, 104 F.T.C. 949, 1070-76 (1984). 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.” [http://www.ftc.gov/os/2000/01/reversesl.htm](http://www.ftc.gov/os/2000/01/reversesl.htm), last visited December 31, 2010.

**81** “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
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. Ultimately, Commissioner Thompson’s view prevailed, and as is shown by later cases, the FTC ultimately went beyond this initial foray into unfairness.

c. **In the Matter of 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 to representations made to consumers. This matter arose from an e-mail that Eli Lilly sent to customers taking Prozac. Instead of masking the names in the e-mail, Eli Lilly included all of the customers' names in an e-mail. 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 FTC Act. 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 use sensitive customer data.

While 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 the Matter of 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. 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. The FTC also alleged that Microsoft had made misrepresentations regarding the amount of personally identifiable information it collected. 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 bind the company to burdens that may be in excess of what the law would otherwise require.

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 the Matter of The National Research Center For College and University Admissions, Inc.; In the Matter of Educational Research Center of America, Inc.; In the Matter of Guess?, Inc.; In the Matter of MTS, Inc., d/b/a Tower Records/Books/Video; In the Matter of Gateway Learning; and In the Matter of Petco Animal Supplies*. All of these cases, while 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, as directly rely upon the FTC’s unfairness authority.

f. **In the Matter of Vision I Properties, LLC—A New Model of “Deception”.**

In the case of *In the Matter of Vision I Properties, LLC, d/b/a CartManager International*, the FTC started an investigation of a company that provided a shopping cart service for other e-commerce websites. 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 FTC Act. In most cases, the portions of the websites that gathered the information were CartManager's, but CartManager did not disclose that the information practices on these pages was different than the other pages and these pages appeared to be part of the same website. The FTC claimed that CartManager also began renting information to third-parties, despite the privacy statements made by the retailers. CartManager also allegedly failed to disclose its information practices to its clients.

This matter presented a different enforcement pattern. While it relied upon an alleged misrepresentation that was deceptive, it was not a direct representation to consumers, as CartManager did not have direct consumer contact. 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 the Matter of BJ’s Wholesale Club, Inc.*

g. *In the Matter of BJ's Wholesale Club, Inc.*

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

BJ's Wholesale Club operates a number of membership warehouse stores. As part of its normal business, BJ's accepted credit cards as a form of payment from its members. BJ's collected personally identifiable information from its customers to authorize their credit cards. It also used wireless technology, including WAPs (wireless access points) and scanners to monitor inventory. 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; did not use readily 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 use for the information, in violation of bank rules.

The FTC alleged that as a result of this conduct millions of dollars in fraudulent purchases had been made. Though there was no federal statute that BJ's conduct directly violated, the FTC concluded that these acts constituted an unfair business practice under the FTC Act and brought an enforcement action against BJ's. This matter also 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 20 years, as well as other administrative requirements.

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 with *CartManager* 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.

83 “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.”

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

While In the Matter of BJ’s Wholesale was the first unfairness case based upon a lack of information security, it was certainly not the last. In the Matter of DSW, Inc., In the Matter of Reed Elsevier Inc. and Seisint, Inc., In the Matter of The TJX Companies, Inc., In the Matter of CVS Caremark Corporation (though it also relied upon allegations of deception), and In the Matter of Dave & Busters, Inc., 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.

11. 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/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. The harm-based model/unfairness/Privacy 2.0 model, which requires “significant” consumer harm, has also been criticized by commentators for being too “reactive” and, as is shown by the failures of privacy litigation, proving harm, particularly “substantial harm” is an illusive and often difficult achievement.85

Ultimately, while 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. 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.86 Privacy 2.0 is a harm and tort-centric model created by courts when their decisions were now famously placed in context by Prosser. 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.87

---

84 As stated by the FTC in its recent report at footnote 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.” Daniel J. Solove, Identity Theft, Privacy, and the Architecture of Vulnerability, 54 Hastings L.J. 1227, 1232-45 (2003).”

85 “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.” Serwin, POISED ON THE PRECIPICE: A CRITICAL EXAMINATION OF PRIVACY LITIGATION, 25 Santa Clara Computer & High Tech L.J. 883 (2009); see also, Hammond v. The Bank of New York Mellon Corp., 2010 WL 2643307 (S.D.N.Y. June 25, 2010), citing Id.

86 Solove, supra, note 84.

87 Id.
of litigation one need only ask someone who is a party to it to describe their 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, governmental or otherwise, being willing to litigate the problem. There are also jurisdictional limits on privacy litigation, both for private parties, as well as the FTC.88

These points illustrate, as more fully discussed below, that models based upon “accountability”—in other words enforcement—have already been tried in the United States, and have failed. Both Privacy 1.0 and 2.0 focus on enforcement as the model to drive compliance and the FTC, as well as many other commentators recognize the limitations of these models. This led the FTC to suggest a new model that was more proactive and provided more flexibility—the “privacy by design” framework. While the model is a significant step in the right direction, it will need to be defined in a more complete way before it can be implemented by businesses in a meaningful way.89

12. 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. While 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 effectively do 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 than a consumer class action or an FTC enforcement action.

88 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”.

The point of identifying these 3 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. You will note that though this is the first model I discuss, I list it as Model 3, and the reason for that will become clear below.

i. Prior Concerns Regarding Accountability.

While accountability has gained attention in recent times in the privacy realm, it is not a new concept in privacy and in fact is a concept that has been discussed in a number of different governance contexts. While 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. 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 organizations reveal the chameleon quality of accountability. Accountability is subjectively construed and changes with context.\(^90\)

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.\textsuperscript{91}

While 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.

ii. 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.”\textsuperscript{92} While accountability-based models must have rules of the road regarding a variety of topics, including security, use restrictions, restrictions on third-party transfers, and other topics, 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 re-examines 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 50 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. The problem with this argument is two-fold. As noted above, enforcement-centric models have been tried in the U.S. 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.\textsuperscript{93} Moreover, to the extent that what these advocates are saying is really there should be

\begin{itemize}
\item \textsuperscript{91} Richard Muligan, ‘Accountability’: An Ever-Expanding Concept, Public Administration Vol. 78 No. 3, 2000, 555.
\item \textsuperscript{92} Feigenbaum, Accountability as a Driver of Innovative Privacy Solutions, \url{http://www.law.yale.edu/documents/pdf/ISP/Feigenbaum_Accountability.pdf}, last visited January 12, 2011.
\item \textsuperscript{93} Privacy 2.0 is a harm and tort-centric model created by courts when their decisions were now famously placed in context by Prosser. 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. Ultimately, however, an essential element of an accountability model is, of course, enforcement based upon accountability to voluntarily adopted best practices, as well as by regulators and private plaintiffs. Taking the second point first, to the extent the
penalties for violating the law, it is a point that cannot be disputed as 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 consequences does not provide the proactive guidance the FTC seeks to generate.\textsuperscript{94}

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 Muligan. 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. Said differently, the challenge with these type of accountability models is that information ethics is in the eye of the beholder. Left to their own devices, what a “privacy-centric” and non-privacy-centric company will conclude is appropriate will vary dramatically, as noted by the FTC in their recent report. As such, 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 imbed 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:

\begin{quote}
The \textit{Privacy by Design} (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events \textit{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 \textit{prevent} them from occurring. In short, \textit{Privacy by Design} comes before-the-fact, not after.\textsuperscript{95}
\end{quote}

model focuses on external enforcement, it is likely to fail. 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. Indeed, to understand the latency of litigation one need only ask someone who is a party to it to describe their 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.

\textsuperscript{94} 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, governmental or otherwise, being willing to litigate the problem. There are also jurisdictional limits on privacy litigation, both for private parties, as well as the FTC.

\textsuperscript{95} \url{http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf}, last visited January 15, 2011.
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 “accountable” for the for 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 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 since 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. They are not. Use limitation is focused on restricting the use of information. While there may be consequences for misuse, that does not make a model focused on use restriction into an accountability model, any more than it makes every existing privacy law in the United States that restricts the use of data an “accountability” statute. This also becomes clear when one examines the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

The OECD guidelines identify a number of principles regarding the use of data. Three of them are of particular importance. The Purpose Specification Principle, which states, “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.” This is clearly a used-based principle. The Use Limitation Principle, which states, “Personal 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.” Again, 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” which states “A data controller should be accountable for complying with measures which give effect to the principles stated above.” 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.
While 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

There are some that have interpreted my Privacy 3.0 article, first published over 3 years ago as a chapter in my privacy treatise, as advocating purely a focus on sensitivity and ignoring other issues. If this were true, I would have called the article Privacy 3.0—The Principle of Sensitivity. I did not because I believe that while sensitivity is extremely important, and data classification is the first step in the analysis, it is truly only the first step, which is why I chose the word proportionality.

In Privacy 3.0 I argued that it was widely recognized that the current theoretical construct of privacy—Prosser’s tort-based enforcement/accountability model—had failed. What was needed was a model that provided appropriate, but not over or under-inclusive protection, 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.

I also recognized that society would gain 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

96 Serwin, supra, note 22.

97 When considering whether Prosser’s model work 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 Federal Trade Commission (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 870.
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.  

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

While 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 non-sensitive. By creating these tiers, one could associate certain use-restrictions and enforcement with each tier. As noted below, I did not simply focus on sensitivity as part of proportionality, but rather 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. These include:
- 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;
- 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.

As is clear from these bullet points—use-limitation—i.e.—“the types of processing that can be done” and the effect of consent, as well as “accountability”—i.e.—“penalties for misuse of the information, including the imposition of statutory penalties in certain cases” are inherent in proportionality.

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

---

98 Id., at 876.
99 Id., at 901-902.
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. 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 a “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.

Some commentators have suggested that this model of privacy does not account for the “context” of information. This is an argument that doesn’t factor in the complete model of proportionality. While it is true that purely a 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 as the restrictions on use will vary on context and more importantly 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 either having too few, or too many restrictions.

13. **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. While 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 than the prior enforcement cases in that while 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 privacy. Otherwise, the level of consumer injury for unfairness goes far beyond “a risk of harm” since 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. As such, 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 4 tiers of sensitivity, and more fully detailed in Privacy 3.0, 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. 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.

This program could follow the model of the EU Safe Harbor program, or Binding Corporate Rules, or BCRs, which are 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.

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 like “privacy (or security) by design,” which would be driven through economic value because of reduced regulatory risk rather than using a “Sword of Damocles” over the head of any

100 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.


102 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.
handler of consumer information; the carrot versus the stick approach.

This would give companies an incentive to proactively focus its 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 productive as otherwise possible.

Whether this is accomplished via the FTC’s rulemaking authority, referenced in Section 7, or if additional legislation is required, pursuing a framework that incorporates Privacy 3.0, includes a safe harbor for those companies that choose to comply, and that 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.

14. 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 have been criticized by many scholars. The new path must be provide appropriate incentives to 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.