Indictments Do Not a Common Law Make:
A Critical Look at the FTC's Consumer Protection "Case Law"

Berin Szoka

Introduction

Does the Federal Trade Commission build common law?[1] The FTC has, along with the Department of Justice, state attorneys general and private plaintiffs, clearly built a common law of antitrust: decades of court decisions have parsed the sparse text of the Sherman and Clayton Acts,[2] supplemented by a series of guidelines[3] summarizing how the FTC and DOJ have developed antitrust doctrines in various areas of competition law (horizontal mergers, vertical mergers, intellectual property, etc.).[4] Through these guidelines, the agencies have played a key role in co-evolving antitrust law with the courts. This process has allowed the agencies to engage in an ongoing dialogue with the third leg of the antitrust analytical stool: the economics profession, which includes economists both inside the agencies and in academe.

What about consumer protection, the other half of the FTC's twin mandate?[5] Congress has enacted a number of statutes authorizing the FTC to regulate specific concerns, from credit reporting[6] to children's privacy,[7] through standard notice-and-comment rulemaking under the Administrative Procedure Act.[8] The FTC has general authority to make formal regulations governing unfair or deceptive trade practices under the Magnuson-Moss Act of 1975, but abandoned use of "Mag-Moss" after Congress imposed a number of procedural safeguards on the process in 1980, as the result of a dramatic stand-off with Congress over the FTC's attempts

---

[1] *See generally, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) (arguing that the FTC's privacy jurisprudence is functionally equivalent to a body of common law that has developed through years of FTC enforcement actions), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913; [cite to 2010 Brill speech].

[2] Sherman Antitrust Act, ch. 647, 26 Stat. 209 (1890) (codified at 15 U.S.C. §§ 1-7 (2006)); Clayton Act, ch. 323, 38 Stat. 730 (1914) (codified as amended in scattered sections of 15 U.S.C.).

[3] U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, HORIZONTAL MERGER GUIDELINES (2010), *available at* http://www.justice.gov/atr/public/guidelines/hmg-2010.html.

[4] *See generally* Carl Shapiro, *The 2010 Horizontal Merger Guidelines: From Hedgehog to Fox in Forty Years*, 77 ANTITRUST L.J. 701 (2010), http://faculty.haas.berkeley.edu/shapiro/hedgehog.pdf.

[5] *See* 15 U.S.C. § 45 (2006); *see also* FED. TRADE COMM'N, ABOUT THE FTC: WHAT WE DO, *available at* http://www.ftc.gov/about-ftc/what-we-do (last visited May 12, 2014) ("The FTC is a bipartisan federal agency with a unique dual mission to protect consumers and promote competition.").

[6] Fair Credit Reporting Act, Pub. L. No. 90-321, 84 Stat. 1127 (1970) (codified as amended at 15 U.S.C. §§ 1601 to 1693r (2006)).

[7] Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-728 (1998) (codified at 15 U.S.C. §§ 6501 to 6506 (2006)).

[8] 5 U.S.C. §§ 553, 556-57 (2006) (setting forth proper procedures for administrative rule making).

to ban advertising to children and regulate everything from funeral home practices to employment to pollution.[9] Thus, most of the FTC's "regulation" of consumer protection now happens informally, through case-by-case adjudication.

Historically, with the notable exception of the FTC's activist binge in the 1970s, the FTC's Bureau of Consumer Protection has focused primarily on regulation of advertising. Through a mix of enforcement actions and industry-specific guides, the FTC attempted to ensure adequate substantiation of claims made by advertisers, to ensure that consumers got the "benefit of the bargain."[10] To some degree, the Bureau of Consumer Protection's process in this area resembled the Bureau of Competition's three-way dialogue with the courts and economists in antitrust law.[11]

But since the mid-1990s, the Bureau of Consumer Protection has extended the FTC's unfairness and deception powers into a variety of consumer protection issues raised by information technologies, which can be broadly grouped into three (overlapping) areas: privacy, data security and product design. The FTC has applied its deception authority in scenarios very different from traditional advertising cases, yet the agency has extended the presumption, developed in those cases, that all statements made to consumers are "material," one of the two elements laid out in the FTC's 1983 Deception Policy Statement.[12] Thus, for example, the FTC now deems deceptive practices that are inconsistent not only privacy policies and terms of service but also online help files[13] and various forms of business-to-business interaction such as patent demand letters.[14] Meanwhile, the FTC has revived the unfairness doctrine, which had been used sparingly since 1980, as a means of regulating a variety of practices that the FTC could not punish as deceptive.[15] Yet the Commission has done little to define the core elements

---

[9] *See* J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection* (2003), *available at* http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

[10] *See, e.g.*, Marshall A. Leaffer & Michael H. Lipson, *Consumer Actions Against Unfair or Deceptive Acts or Practices: The Private Uses of Federal Trade Commission Jurisprudence*, 48 GEO. WASH. L. REV. 521, 547 (1980) ("In cases in which injury to consumers is not quantifiable, or when damages would be inadequate under the 'out-of-pocket' rule, the courts may allow recovery under the 'benefit of the bargain' rule, which entitled a consumer to the difference between what she actually received in the transaction and what she would have received had the deceptive representation been true.").

[11] *Compare* FED. TRADE COMM'N, ABOUT THE BUREAU OF CONSUMER PROTECTION, *available at* http://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/about-bureau-consumer-protection (last visited May 12, 2014), *with* FED. TRADE COMM'N, ABOUT THE BUREAU OF COMPETITION, *available at* http://www.ftc.gov/about-ftc/bureaus-offices/bureau-competition/about-bureau-competition (last visited May 12, 2014).

[12] FED. TRADE COMM'N, FTC POLICY STATEMENT ON DECEPTION, IV (1983), *available at* http://www.ftc.gov/ftc-policy-statement-on-deception.

[13] [Cite to Apple case]

[14] [Cite to MPHJ's motion for declaratory judgment to stop the FTC's enforcement action against it]

[15] *See* Beales, *supra* n. 9.

laid out in the 1980 Unfairness Policy Statement: (1) substantial injury (2) that is not outweighed by countervailing benefit and (3) that is not reasonably avoidable by consumers.[16]

In total, the FTC has brought 55 data security enforcement actions,[17] 43 consumer privacy enforcement actions[18] and a smattering of other cases related to information technologies. Yet only one of these cases has resulted in a court decision, and only recently did two companies refuse to settle data security enforcement actions.[19]

For a variety of reasons, companies are deeply reluctant to challenge the FTC in court.[20] Settlement offers a relatively painless way for companies to make an investigation "go away," since the FTC has no statutory authority to impose monetary penalties for first-time violations of Section 5, and can thus, at most, only seek disgorgement of wrongful gains.[21] The costs of *not* settling can be considerable. The FTC can drag out its Civil Investigative Demand (CID) discovery process with few limitations or due process rights for the subjects of investigations,[22] which can both generate enormous legal bills and also waste the valuable time of key employees. Wyndham Hotels, for example, spent $5 million on direct legal expenses in the CID stage, before the FTC finally sued the company in federal court.[23] If a company does decide to sue, the FTC may insist on first bringing the action before the FTC's administrative law judge under Part III of the FTC's rules, so that the company must litigate the issue twice—first at the ALJ and then in appeal to the full Commission—before having its case heard before a neutral, independent Article III court. Throughout this process, the lack of prior legal decisions on point puts a defendant at a considerable disadvantage. Perhaps the greatest cost, though, is reputational. Privacy and data security are, apparently, simply more sensitive than, say, antitrust or advertising substantiation cases. Target, for example, lost around 20% of its quarterly revenue and 7.1% of its market capitalization after news of its data breach broke in

---

[16] FED. TRADE COMM'N, FTC POLICY STATEMENT ON UNFAIRNESS (1980), *available at* http://www.ftc.gov/ftc-policy-statement-on-unfairness.

[17] FED. TRADE COMM'N, BUREAU OF CONSUMER PROT. BUS. CTR., LEGAL RESOURCES: PRIVACY AND SECURITY: DATA SECURITY, *available at* http://business.ftc.gov/legal-resources/29/35 (last visited May 12, 2014).

[18] FED. TRADE COMM'N, BUREAU OF CONSUMER PROT. BUS. CTR., LEGAL RESOURCES: PRIVACY AND SECURITY: CONSUMER PRIVACY, *available at* http://business.ftc.gov/legal-resources/48/35 (last visited May 12, 2014) (excluding pure COPPA cases).

[19] Solove & Hartzog, *supra* note 1, at 610-11.

[20] *See id.*, at 611-13.

[21] *Id.*

[22] *See* 15 U.S.C. § 57b–1 (2006); *see also* FED. TRADE COMM'N, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY (2008), *available at* http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[23] *See* Brief for TechFreedom et al. as Amici Curiae Supporting Defendants, Wyndham Worldwide Corp. v. Fed. Trade Comm'n, at 10 (2013) (No. 13-1887), *available at* http://docs.techfreedom.org/Wyndham_Amici_Brief.pdf.

late 2013.[24] The FTC has an enormous bully pulpit and has not, especially in recent years, hesitated to use it to shame companies. Even if FTC staff does not explicitly offer to "go easy" on a company in exchange for agreeing to settle, it is difficult to imagine that fear of harsher treatment in the media does not play a significant role in encouraging companies to settle enforcement actions. The prospect of having to endure two public defeats (before the ALJ and Commission), and the negative publicity generated by each, before ever getting to Federal court, surely also plays a role in discouraging companies from litigating.

The net result is that the courts simply have not played the critical role in shaping modern consumer protection law as they have in antitrust. Perhaps for this reason, consumer protection law simply has not experienced the kind of methodological revolution wrought by the law and economics discipline in antitrust law. The Bureau of Economics plays an active role in the antitrust cases brought by the Bureau of Competition, but its role in the Bureau of Consumer Protection's cases is apparently limited primarily to the calculation of damages in the limited number of cases where the Commission actually seeks damages.[25] Rather than issuing guidelines analyzing past cases and developing the Commission's doctrines in economic terms, the Commission has, instead, issued a series of reports that recommend certain privacy or data security practices (or the "by design" processes underlying them).[26] Economics has played essentially no role in these reports, despite some involvement of economists in the workshops leading to these reports.

Thus, while the FTC has pursued case-by-case enforcement in both areas, the two processes differ fundamentally. In antitrust law, the courts have forced the FTC to develop and better explain its doctrines over time. This, in turn, has forced the agency to ground its work in economics. This process is reflected in both actual common law (court decisions) and administrative common law (cases adjudicated before an Administrative Law Judge and, ideally, through to the Commission). But in consumer protection, or at least "Consumer Protection 2.0" issues (beyond traditional advertising substantiation and marketing claims), no such evolution has occurred.[27] To understand why, this paper first examines the process used by the FTC, then considers a series of consumer protection cases

---

[24] *See* Zacks Equity Research, Has Target Lost Its Momentum? (Jan. 28, 2014), *available at* http://www.zacks.com/stock/news/121094/Has-Target-Lost-Its-Momentum.

[25] FED. TRADE COMM'N, ABOUT THE BUREAU OF ECONOMICS, *available at* http://www.ftc.gov/about-ftc/bureaus-offices/bureau-economics/about-bureau-economics (last visited May 12, 2014) ("In the consumer protection area, the Bureau provides economic support and analysis of potential Commission actions in both cases and rulemakings handled by the Bureau of Consumer Protection. Bureau economists also provide analysis of appropriate penalty levels to deter activity that harms consumers.").

[26] *See, e.g.*, FED. TRADE COMM'N, FTC ISSUES FINAL COMMISSION REPORT ON PROTECTING CONSUMER PRIVACY: AGENCY CALLS ON COMPANIES TO ADOPT BEST PRIVACY PRACTICES (2012), *available at* http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

[27] *But see* Solove & Hartzog, *supra* note 1, at 606-27 (arguing that FTC settlements essentially comprise a de facto body of common law).

FTC's Complaints & Settlements Process

What, exactly, is the FTC's supposed "common law?" Hartzog and Solove argue that while "[t]echnically, consent orders legally function as contracts rather than as binding precedent . . . in practice, the orders function much more broadly . . . ."[28] They assert that "the trajectory and development [of FTC enforcement] has followed a predictable set of patterns[,]" and that the body of FTC settlements is thus "the functional equivalent" of common law.[29] But is this really the case? In looking at the body of FTC settlements, what sort of patterns emerge?

Those attempting to decipher the FTC's past approach, and thus predict its future approach, have available a body of "cases" that typically consist of four key elements:

1. The complaint describes the facts alleged by the FTC and then asserts the FTC's legal theories in a conclusory way that does not really integrate the facts alleged and the underlying legal theories at stake.
2. What is commonly called the "settlement" may take a number of forms, but in all cases, the settlement is essentially an agreement approved by the commission (typically in an "Agreement Containing Consent Order"[30]) by which the company stipulates that it does not actually concede as true any of allegations in the FTC's complaint, waives any further legal action, and agrees to certain (invariably boilerplate) remedies, which usually include 20 years of audits and a commitment to follow the best practices developed by the FTC in its related reports. The important thing to note, in comparing these settlements to real common law, is that they do not offer further legal analysis. Even where the Commission also issues a formal Decision and Order,[31] that order is fundamentally different from the kind of order the Commission issues after internal adjudication, which must explain the FTC's legal analysis, rather than merely summarize the FTC's enforcement action and the terms of the settlement.[32]
3. An "Analysis of Proposed Consent Order to Aid Public Comment" summarizes the allegations of the complaint and the requirements of the consent order in a way that is more readable. Occasionally, the FTC may also publish the order in the Federal Register.[33]
4. Similarly, a press release explains the case, often in more detail than provided by the complaint, but with no real legal analysis.

---

[28] Solove & Hertzog, *supra* note 1, at 607.

[29] *Id.* at 608. In their article, the authors were referring to FTC settlements as particularly forming the functional equivalent of privacy common law, but their reasoning may be applied to FTC process more generally.

[30] See, e.g., http://www.ftc.gov/sites/default/files/documents/cases/2005/06/050616agree0423160.pdf

[31] See, e.g., http://www.ftc.gov/enforcement/cases-proceedings/112-3108/apple-inc

[32] See, e.g., http://www.ftc.gov/sites/default/files/documents/cases/2013/01/130116pomopinion.pdf

[33] *See, e.g.*, Fed. Trade Comm'n, TRENDnet, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 78 Fed. Reg. 55717 (Sept. 11, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/09/130911trendnetfrn.pdf.

FTC Commissioners sometimes issue statements explaining their positions and performing real analysis of the statute, but, as we shall see, such statements are relatively rare. Usually, it takes a strong dissent by one Commissioner to spur other Commissioners into explaining their analysis.[34] Even then, the deck is stacked against such dissent because the Commission is not actually voting on the merits of the case, only on whether to bring the investigation.

Section 5(b): the Statutory Standard for FTC Settlements

The most important, and unappreciated, detail about the FTC's so-called common law is that the complaints and settlements on which the FTC places so much reliance as sources of guidance for industry, do not, by their own terms, even purport to actually weigh the elements of unfairness and deception. These documents are best understood as indictments rather than full adjudications.

The reason is simple, and should be readily apparent to anyone who reads either the underlying statute or who reads the FTC's so-called "common law" documents carefully. Under Section 5(b),[35] the FTC is required to bring a complaint if two criteria are met: First, the Commission must have "reason to believe" that the defendant has committed a violation of Section 5. Second, the Commission must conclude "that [an enforcement action] would be to the interest of the public."[36] Former Commissioner Thomas Rosch explained this dual standard in a 2010 speech colorfully entitled, "So I Serve as Both a Prosecutor and a Judge – What's the Big Deal?":

> There is no statutory or regulatory definition regarding what it means to have a "reason to believe." Moreover, attempts to litigate the issue of what the FTC must do to meet that standard have gone nowhere: in its 1980 decision in *FTC v. Standard Oil of California*, the Supreme Court held that the FTC's application of the "reason to believe" standard in conjunction with voting out a complaint is not "final agency action" under the Administrative Procedure Act. Instead, the Court held, it is "a threshold determination that further inquiry is warranted"

---

[34] *See, e.g.*, Dissenting Statement of Commissioner Joshua D. Wright In the Matter of Apple, Inc., FTC File No. 112-3108 (Jan. 15, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/cases/140115applestatementwright_0.pdf; Statement of Chairwoman Edith Ramirez and Commissioner Julie Brill in the Matter of Apple Inc., FTC File No. 112-3018 (Jan. 15, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/cases/140115applestatementramirezbrill.pdf; Statement of Commissioner Maureen K. Ohlhausen in the Matter of Apple Inc., FTC File No. 112-3108 (Jan. 15, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/cases/140115applestatementohlhausen.pdf.

[35] "Whenever the Commission shall have reason to believe that any such person, partnership, or corporation has been or is using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce, and if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public, it shall issue and serve upon such person, partnership, or corporation a complaint stating its charges in that respect and containing a notice of a hearing upon a day and at a place therein fixed at least thirty days after the service of said complaint." 15 U.S.C. § 45(b),

[36] 15 U.S.C. § 45(b).

> and, as such, is not subject to judicial review. The "reason to believe" standard is therefore committed to each Commissioner's discretion. ….
>
> When outside parties come in to argue that the Commission lacks a "reason to believe," they tend to – errantly, in my view – focus primarily on the first question and argue that when all of the evidence is uncovered, they will prevail. The "reason to believe" standard, however, is not a summary judgment standard: it is a standard that simply asks whether there is a reason to believe that litigation may lead to a finding of liability. That is a low threshold.[37]

All the FTC's settlements ever purport to do is to satisfy this "low threshold." For example, in the Apple decision, discussed further below, Chairman Ramirez and Commissioner Brill were careful to couch their statement explaining why they voted to issue the complaint on "reason to believe" grounds, a term they use five times in a relatively short statement;[38] Commissioner Wright likewise explicitly addresses this legal standard in his conclusion.[39] Indeed, in rejecting Commissioner Wright's call for a "study of how consumers react to different disclosures before issuing its complaint against Apple," Ramirez and Brill specifically cite to this provision.[40] As a legal matter, they are correct: the bar really is set this low for the FTC to bring a complaint.

The other critical detail that starkly distinguishes the FTC's approach from a true common law approach is, as Commissioner Rosch notes, even if some third party had sufficient incentive to challenge the legal principle implicit in a settlement, the FTC's vote is not subject to judicial review because it is not a final agency action.[41] Thus, in practice, there is little to check the Commission's discretion.

In theory, the questions of whether to bring an enforcement action and whether a violation occurred are distinct; but in practice, when enforcement actions end in settlements (and when the two are often filed simultaneously), the two questions collapse into one. The FTC Act does not impose any additional requirement on the FTC to negotiate a settlement. Indeed, only if the Commission seeks a civil penalty (which is possible only for violations of a pre-existing consent decree or of an FTC rule, not for direct violations of Section 5) does the statute even require that the "settlement [be] accompanied by a public statement of its reasons and [be] approved by the court."[43] Thus, at best, the FTC's decisions are roughly analogous not to court decisions

---

[37] J. Thomas Rosch, Commissioner, Fed. Trade Comm'n, Remarks at the American Bar Association Annual Meeting (Aug. 5, 2010) (quoting FTC v. Standard Oil Co. of Cal., 449 U.S. 232, 241 (1980)), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/so-i-serve-both-prosecutor-and-judge-whats-big-deal/100805abaspeech.pdf.

[38] *See* Statement of Chairwoman Edith Ramirez and Commissioner Julie Brill, *supra* note 34, at 1-5.

[39] *See* Dissenting Statement of Commissioner Joshua D. Wright, *supra* note 34, at 17.

[40] Statement of Chairwoman Edith Ramirez and Commissioner Julie Brill, *supra* note 34, at 5, n. 16.

[41] Rosch, *supra* note 37, at 3.

[43] 15 U.S.C. 45(m)(3). See, e.g., FTC's Google Setttlement, http://www.ftc.gov/sites/default/files/documents/cases/2012/11/121120googleorder.pdf

on the merits, but to court decisions on motions to dismiss for "failure to state a claim upon which relief can be granted."[44] Or, perhaps even more precisely, the FTC's decisions are analogous to reviews of warrants in criminal cases, as Commissioner Rosch has argued.[45] It would be a strange criminal common law, indeed, that confused ultimate standards of guilt with the far lower standard of whether the police could properly open an investigation, yet this is essentially what the FTC's "common law" of settlements does.

Major Unresolved Questions

- Is the FTC bound by its Policy Statements? In the *Touch Tone* case, the FTC indicated it was not. This would give the FTC broad discretion to use its deception powers, and may
- However "customer" is defined, the FTC need not perform any meaningful analysis of whether the "reasonable" archetype of that class would actually have been deceived by the misrepresentation; and
- The FTC can bring deception cases for misrepresentations made to businesses, even large, sophisticated businesses like banks (a notion that will become relevant again with, among other things, patent demand letters).

Part II: Case Studies in the FTC's "Common Law" Approach

The FTC's experience with unfairness may be summarized in key parts as follows:

- **The Rise of Unfairness (1964-1975)**: Beginning with its Cigarette Advertising Rule, the Commission began using its unfairness authority to issue rules regulating a variety of practices, while also pursuing aggressive enforcement actions,
- **The Heyday of Unfairness (1975-1980)**: Emboldened by the Supreme Court's decision in *Sperry v. Hutchison* in 1972, the FTC stepped up its enforcement actions and, in 1975, persuaded Congress to give the agency rulemaking authority in the Magnuson-Moss act, something the FTC had claimed was implied by the FTC Act but not specifically authorized." The FTC soon devoted "more than half of its consumer protection resources to rule-making."[46]
- **The Winter of Unfairness (1980-1997)**: In 1980, Congress amended Mag-Moss to create procedural and evidentiary safeguards intended to avoid the abuses of the previous decade. The FTC has not conducted a new rulemaking since. Congress also essentially required the FTC to issue the Unfairness Policy Statement. In 1994, Congress finally reauthorized the FTC for the first time since 1980 and, when it did so, encoded the three-part test at the core of the Unfairness Policy Statement into Section 5. In the interim, the FTC had brought just sixteen unfairness cases, which fell into narrow

[44] F.R.C.P. 12(b)(6).

[45] Rosch, *supra* note 37, at 4-5.

[46] Stephen Calkins, FTC Unfairness: An Essay, 46 WAYNE L. REV. 1935, 1953 (2000)

categories: "(1) theft and the facilitation thereof (clearly the leading category); (2) breaking or causing the breaking of other laws; (3) using insufficient care; (4) interfering with the exercise of consumer rights; and (5) advertising that promotes unsafe practices."[47] Even as the FTC began to grapple with Internet policy issues in 1995, the FTC did not use unfairness.

- **The revival of unfairness** (1997-present)
  - **Online fraud and harms to children** (1997-2000)
  - **Data Security Regulation through Deception (2000-2005)**: In 2000, the FTC brought its first data security case. While these early cases alleged that practices were "unfair and deceptive," they were, in fact, pure deception cases.[48]
  - **The Return of Unfairness for Tech Cases (2000-2009)**:

A. The FTC Begins to Grapple with the Internet

Touch Tone: Pretexting (1999)

In 1999, the FTC settled its first "information broker" case – a settlement that helps to set the stage for the subsequent development of both unfairness and deception, while also illustrating key concerns about the differences between the FTC's process and a true common law process. The FTC alleged that a company called Touch Tone had obtained sensitive financial information about consumers through "pretexting," obtaining sensitive financial information about a consumer by calling their financial institutions and pretending to be them. Touch Tone sold access to its database of such sensitive information through the Internet.[49] The Commission alleged both that Touch Tone had deceived the bank (and perhaps also the account holder) and that the disclosure of sensitive financial information without consent was unfair.

On the most superficial level, the *Touch Tone* case is important because it illustrates that, when the Commission began reviving unfairness to regulate data and technology cases, it focused on clear fraud, whereas the data security cases it began bringing in 2005 focused on, essentially, negligence, and subsequent enforcement actions (e.g., Apple) would focus on ambiguous conduct with very clear, non-price trade-offs for users.

But several other aspects of *Touch Tone* bear examination as illustrations of the differences between the FTC's approach and a real common law. While few (if anyone) would argue, as a policy matter, that government should not punish both pretexting and the sale of sensitive financial information like bank account numbers and balances, the case presented two fundamental doctrinal questions and one important procedural question, which Commissioner Swindle raised in a scathing dissent, but which the Commission simply overruled. Because the

---

[47] Calkins at 1962.

[48] See, e.g., FTC v. Rennert, Complaint, FTC File No. 992 3245, http://www.ftc.gov/os/2000/07/iogcomp.htm (2000); In re Eli Lilly, Complaint, File No. 012 3214, http://www.ftc.gov/os/2002/05/elililllycmp.htm (2002)..

[49] http://www.ftc.gov/sites/default/files/documents/cases/1999/04/ftc.gov-touchtonecomplaint.htm

case was settled out of court, none of these issues were challenged – with, as we shall see, lasting implications that continue to shape consumer protection law today.

To start, Touch Tone's business model was clearly built on deceiving financial institutions – and, the majority implied, Touch Tone thus indirectly deceived account holders as well. But is that really "deception" under Section 5? Commissioner Swindle noted that the Deception Policy Statement requires that a misrepresentation be made to the consumer, but no statement was ever made to individual account holders in this case.[50] The only statements were made to the financial institutions themselves. While Swindle allowed that a bank might be considered a "consumer" under the Deception Policy Statement (something that is far from apparent from the statement), he noted that the Statement requires that the statement be assessed from the perspective of the reasonable consumer to determine "whether the consumer's interpretation or reaction is reasonable." No reasonable bank, he argued, would give away such sensitive financial information to a caller who provided merely a name and social security number. (This argument foreshadowed today's standard industry practice of requiring multiple verification questions, and is analogous to the FTC's arguments today regarding reasonable data security, although applied in a different context.) The majority simply asserted that:

> we find it difficult to imagine a more cognizable deceptive act or practice under Section 5 than this where a material and false statement to one entity (the bank), has the likely effect of injuring that entity as well as another (the account holder). We find that simple proposition fits comfortably within the purview of the Deception Statement and the plain language of Section 5.[51]

The debate then switched to the key procedural question – one that remains of vital importance today: Is the FTC actually bound by its policy statements? The Commission insisted it was not:

> [the Deception Policy] Statement was not issued by this agency to serve as a straitjacket for Section 5's deception authority. .... This Commission has never so held. And, with due respect to our colleague's unduly narrow interpretation, no Court of Appeals has found the Statement to preclude challenging as deceptive certain acts or practices that were not foreseen at the time or described within its four corners. In fact, both before and after the 1983 Statement the Commission has challenged deceptive statements made to one party that may injure that party or a third party.

Swindle urged the FTC to file for an injunction against Touch Tone under Section 13(b) to solve the immediate problem and, rather than settling the matter,

---

[50] http://www.ftc.gov/sites/default/files/documents/cases/1999/04/ftc.gov-touchtoneswindlestatement.htm#N_7_

[51] http://www.ftc.gov/sites/default/files/documents/cases/1999/04/ftc.gov-majoritystatement.htm

> bring this case as an administrative proceeding in order to develop and articulate a reasoned explanation for departing from the well-established requirements of the Deception Statement. Because this new theory of deception based directly on the statute requires application of the Commission's expertise to a novel regulatory issue, it should be adjudicated in an administrative proceeding. *See FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1028 (7th Cir. 1988).

Swindle explained the need for such a statement as follows:

> Although this case does not satisfy the legal standard set forth in the Deception Statement, the Commission could take the unprecedented step of adopting an interpretation of deception under Section 5 that is broader than the interpretation enshrined in Commission adjudicative decisions incorporating the Deception Statement. Principles of administrative law, however, require the Commission to state that it is departing from its previous policy and explain why it is doing so. "When an agency undertakes to change or depart from existing policies, it must set forth and articulate a reasoned explanation for its departure from prior norms." *Telecommunications Research and Action Center v. FCC*, 800 F.2d 1181, 1184 (D.C. Cir. 1986); *see also Midwestern Transp., Inc. v. ICC*, 635 F.2d 771, 777 (10th Cir. 1980) ("[A]n agency must apply criteria it has announced as controlling or otherwise satisfactorily explain the basis for its departure therefrom.").

Instead of addressing these issues, the Commission simply settled the matter, thus setting two precedents – or, at least, what count as "precedents" in the FTC's "common law" approach:

- However "customer" is defined, the FTC need not perform any meaningful analysis of whether the "reasonable" archetype of that class would actually have been deceived by the misrepresentation;
- The FTC can bring deception cases for misrepresentations made to businesses, even large, sophisticated businesses like banks (a notion that will become relevant again with, among other things, patent demand letters); and
- The FTC remains free to set aside its own policy statements at whim (except, of course, insofar as the Commission is specifically bound by statute, as it is by Congress's 1994 incorporation of part of the Unfairness Policy Statement[52]).

On unfairness, the complaint simply asserted that the "disclos[ure] or [sale of] private financial information obtained through [pretexting], without the knowledge or consent of the consumers to whom such information relates… cause or are 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." This presaged the FTC's 2012 Privacy

[52] See 15 U.S.C. 45(n).

Report's assertion that certain categories of data are inherently sensitive.[53] Swindle objected: "We have never held that the mere disclosure of financial information, without allegations of ensuing economic or other harm, constitutes substantial injury under the statute." He contrasted the complaint's conclusory assertion, noting that in other enforcement actions, the FTC had shown that the disclosure of credit card information caused monetary harm in the form of unauthorized charges.[54] Or, the Commission staff had "identified the substantial injury stemming from the unauthorized release of children's personally identifiable information as being the risk of injury to or exploitation of those children by pedophiles who use such information to identify and recruit children for sexual relationships."[55] In other words, Swindle did not read the Unfairness Policy Statement to require monetary harm alone, but to require *some* analysis to establish harm flowing from the disclosure of information.

The majority claimed the Commission has previously recognized that the misuse of certain types of information can be "legally unfair," citing *Beneficial Corp.,* 86 F.T.C. 119 (1975). Swindle noted that the "fiduciary relationship" there existed between the customer and his tax preparer – and *not*, as the Administrative Law Judge held, uncontradicted by the Commission's final decision, emphasized, based on "broad ethical desiderata, such as the need to protect personal privacy of individuals."[56] That concept, Swindle argued, vaguely foreshadowing the FTC's data security enforcement actions, "might have supported an unfairness allegation against the bank for the unauthorized disclosure of its depositors' account numbers and balances" – but not, without further analysis of substantial injury, against Touch Tone, who had no such fiduciary relationship with the consumers who were ultimately defrauded.

More fundamentally, Swindle again harkened back to the Commission's policy statements – this time, on unfairness, and to Section 5(n). The *Beneficial* case rested "almost exclusively on general public policy regarding the confidentiality of tax information and the privileged nature of a tax preparer's relationship with its customers." But as Swindle notes, the 1980 Unfairness Policy Statement and its 1994 incorporation codification into Section 5(n) provide that: "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."

Swindle's point, as with recent Commissioner Wright's dissent in *Apple*, was not that the FTC should have done nothing, but that its analysis was simply inadequate:

---

[53] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, at 59 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[54] *FTC v. Capital Club of North America Inc.*, No. 94-6335 (D.N.J. Jan. 19, 1995) (consent).

[55] Letter from Jodie Bernstein, Director, Bureau of Consumer Protection, Federal Trade Commission, to Center for Media Education (July 15, 1997).

[56] *Id.* at 149.

> the Commission has not been presented with any evidence that would create reason to believe that consumers are likely to suffer a substantial injury -- *i.e*., economic harm or a threat to health or safety -- from defendants' actions. Merely to "posit" that substantial consumer injury "could" flow from the disclosure of private financial information does not satisfy the statute's requirement that the challenged practice "cause[] or [be] likely to cause substantial injury to consumers."

Finally, Swindle warned:

> Third, the concept of "financial information" is extremely broad and may be construed to extend well beyond bank account numbers and balances to reach many types of information that some consumers may consider "private" in a colloquial sense. I am concerned that this case represents a foray into broader privacy regulation.

Indeed, the FTC's 2012 Report "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers" has become de facto privacy regulation, premised on this kind of distinction around sensitivity.[57] That may well be good policy, but the FTC has never grounded it in any meaningful analysis of its legal authority the way that antitrust common law, for example, has grounded certain per se rules or rules of reason in doctrine explained case-by-case over time.

The majority's statement in *Touch Tone* also foreshadowed the FTC's later claims that it was taking a "common law" approach when it declared:

> Section 5 of the FTC Act deliberately incorporates a flexible standard, so that the Commission may react to changes in the marketplace. We would be remiss to fail to apply our statutory authority where we see conduct that both we and courts could readily find is likely injurious to consumers.[58]

Reverse Auction

The FTC's settlement in *Touch Tone* led directly to its first Internet-related unfairness case – against *ReverseAuction.com*, which had violated eBay's terms of use by creating harvesting user emails from the site eBay.[59] The company had sent spam emails to eBay users, falsely claiming the user's eBay account was about to expire in order to lure them to its competing auction site (Count I). The Commission alleged that the emails were deceptive both in claiming that the

---

[57] http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

[58] [cite]

[59] FTC v. ReverseAuction.com, Complaint, File No. 002-3046, http://www.ftc.gov/enforcement/cases-proceedings/reverseauctioncom-inc (2000).

user's account was about to expire and that eBay had provided the email addresses, "or otherwise knew of, or authorized, ReverseAuction's dissemination of the unsolicited commercial e-mail to eBay registered users" (Count II). The Commission alleged that Reverse Auction had deceived eBay by violating eBay's terms of service to obtain the email addresses in the first place (Count III). The Commission unanimously approved the latter two counts but divided on the first.

As with *Touch Tone*, the complaint contained no real analysis of the deception claim in Count I. The Commission asserted – and it seems difficult to dispute – that ReverseAuction had willfully misled eBay "by registering as an eBay user, represented to eBay, expressly or by implication, that it would comply with the terms and conditions of eBay's User Agreement, including the agreement to refrain from using any personal identifying information of any eBay user obtained through the eBay web site for the purposes of sending unsolicited commercial e-mail."[60] But who was the "customer" for purposes of analysis under the Deception Policy Statement, and was it "reasonable" that they were misled by this misrepresentation? Or was the Commission acting beyond the four corners of the Deception Policy Statement, as Swindle argued it had done in *Touch Tone*. The complaint, of course, answered none of these questions, even indirectly, nor did the Commission issue an aid for public comment on the settlement. Nor, indeed, the Commission issue any statement at all. To understand the decision, we have only the statement of Commissioner Mozelle Thompson supporting the settlement, and the dissenting statements of Commissioners Swindle and Leary.

Remarkably, only a year after Swindle had protested so strongly against the lack of deception analysis, he and Leary joined in the deception theory in Count I:

> ReverseAuction represented to eBay that it would not use the information it obtained about other members to send unsolicited commercial e-mail. ReverseAuction, however, sent unsolicited e-mails promoting its auction site to eBay members using e-mail addresses harvested from eBay's site**. ReverseAuction thereby deceived eBay directly and, in doing so, also misled other members of the eBay community** who believed that all participants in the eBay marketplace would abide by the same privacy rules.[61]

This theory does, indeed, seem plausible: it is certainly easy to imagine that eBay customers based their decision to used eBay's service on their understanding that other eBay users would not harvest email addresses, and that this spoke to the "basic question" asked by the Deception Policy Statement: "whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service."[62] What is remarkable is that this important

[60] ReverseAuction Complaint. http://www.ftc.gov/sites/default/files/documents/cases/2000/01/www.ftc_.gov-reversecmp.htm

[61] Id. (emphasis added).

[62] DPS

question simply was not analyzed at all in the complaint or other parts of the "case," not even in the statements of the two most vocal critics of the majority (Commissioners Leary and Swindle).

Only Commissioner Thompson, a Democrat appointee and generally supportive of the Commission's increasingly activist approach, expressed concern about this important doctrinal question. On the one hand, he quoted approvingly from *Touch Tone* ("Section 5 of the FTC Act deliberately incorporates a flexible standard, so that the Commission may react to changes in the marketplace.") and defended the Commission's alternative unfairness theory on Count I (ReverseAuction's harvesting of email eBay user addresses). But at the same time, he argued that "the unfairness, rather than the deception claim is more appropriate at this time." He did not question the Commission's legal analysis of whether ReverseAuction's violation of eBay's terms of service itself constituted deception. He simply argued, as a prudential matter, that it might undermine the self-regulation the Commission was then trying to encourage:

> if industry "self-regulation" is to have meaning and if we seek to create an overall market climate in support of data privacy, industry needs to be encouraged to take direct independent action against those who violate the terms of their privacy agreements. It would be unfortunate if inclusion of a deception count were viewed as preempting industry enforcement efforts by focusing on the contractual relationship between eBay and ReverseAuction rather than the direct effect on consumers. I believe that at this important time, we need to encourage and support and supplement the work of industry in this area - not act as a substitute for its own enforcement activity. I encourage industry to continue its efforts to develop privacy policies consistent with fair information practices.

Thompson raised an important question: How, if at all, should the Commission use Section 5 to regulate relationships between businesses? As we shall see, this critical question would arise later in both the FTC's data security and patent cases.[63] The point, for the moment, is simply that, yet again, an important doctrinal question was swept under the rug because there was neither a true common law process (adjudication by a court) nor even an administrative common law process (adjudication by the FTC's ALJ and then the issuance of a full order by the Commission). As a result, the Commission left no analysis of a critical important doctrinal question.

The debate between Thompson and the minority focused on the unfairness theory plead as an alternative justification for Count I. The Complaint asserted three forms of injury:

---

[63] Ohlhausen Bosch dissent at 4, http://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-ohlhausen/121126boschohlhausenstatement.pdf ("If the Commission continues on the path begun in *N-Data* and extended here, we will be policing garden variety breach-of-contract and other business disputes between private parties.").

- "using [eBay users'] e-mail addresses, eBay user IDs, and feedback ratings for purposes other than those consented to or relied upon by such consumers, including the purpose of sending them unsolicited commercial e-mail solicitations;"
- "undermining their ability to avail themselves of the privacy protections promised by online companies," specifically, the eBay user agreement's prohibition on the collection of user information for the purposes of disseminating unwanted commercial e-mail solicitations" and
- "causing them to believe, falsely, that their eBay user IDs were about to expire"

Presumably out of sensitivity to the Commission's checkered history with Unfairness (the codification of the Unfairness Policy Statement had occurred little more than five years earlier) Commissioner Thompson "insisted this I believe this action is not an overly expansive view of the unfairness doctrine, but instead represents a reasoned and tailored response to the circumstances presented." He continued: "The Commission does not here declare that sending unsolicited commercial e-mail ('spamming') is unfair in all circumstances, nor does it suggest that privacy invasions cause substantial injury in all circumstances." Yet he also proposed the diffuse theory of harm that has come to undergird so much of the FTC's approach to privacy in recent years:

> 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.

Swindle and Thompson agreed that ReverseAuction "could undermine consumer confidence in such privacy arrangements [as offered by eBay's terms of service], but considered this as part of the public interest analysis justifying the deception theory, not substantial injury justifying the unfairness theory.[64] Leary later explained his view:

> Every breach of contract involves a "deception" in this sense, but surely not all contract breaches are violations of Section 5. What made this case different for me is the context of the breach: a pattern of broken promises in circumstances that suggested the respondent never intended to keep them, which had an impact on a large number of people and businesses, in a new market medium that could itself be damaged by lack of trust.[65]

---

[64] "Because proliferation of the kind of deceptive conduct in which ReverseAuction allegedly engaged could undermine consumer confidence in such privacy arrangements, we believe that it is appropriate to pursue this matter under a deception theory."

[65] http://www.ftc.gov/public-statements/2000/04/unfairness-and-internet

In a footnote, Leary added the critical caveat: "Because this case was settled, I cannot be sure that the other Commissioners agreed with this rationale."[66] Indeed. It would be hard to find a clearer statement of the difference between the FTC's settlement-by-settlement approach and a true common law. In the FTC's approach, the most analysis we ever get is in dissents and the statements they engender in response. But even then, these statements tend to be very short (Commissioner Wright's 17-page dissent in Apple being the dramatic exception to the rule), with little room for detailed analysis. But regardless of how thorough an analysis any one Commissioner might offer, those attempting to follow the thread of the Commission's approach over time still "cannot be sure" what the precise legal holding was in a particular case, or why, or what that quasi-precedent (technically non-binding through it may be) portends for enforcement in the future.

Leary continued:

> It could be argued, however, that consumers had also been deceived by ReverseAuction because they made the same promises that others did, in the expectation that similar promises would be honored by other participants on the auction site. Like the organizer of a club or other association, eBay was the "hub" of a wheel of interconnecting agreements by people on the rim, who did not make direct promises to each other.

But again, the critical caveat: "This would have been, perhaps, an appealing deception theory, if the case had been litigated." If only!

Unfairness

On a less lofty note, Commissioner Thompson added:

> The injury caused by ReverseAuction's conduct, far from being speculative, is a tangible misappropriation of personal protected information that enabled the company to send personalized deceptive e-mail messages to scores of consumers.

Swindle and Leary responded:

> 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.
>
> Consumers do not have a substantial privacy interest in the e-mail addresses and other information that ReverseAuction harvested since consumers had already

[66] Id. note 50.

> agreed to make this information available to millions of other eBay members (albeit with restrictions on using it for commercial solicitations). Moreover, a substantial portion of this information is available without restriction to non-members who visit eBay's web site. Merely obtaining consumers' e-mail addresses without their explicit consent and sending them e-mail solicitations does not cause substantial injury.
>
> The injury in this case was caused by deception: that is, by ReverseAuction's failure to honor its express commitments. It is not necessary or appropriate to plead a less precise theory.

Swindle elaborated on this position a year later, in dissenting from another FTC enforcement action against pretexters akin to that in *Touch Tone*:

> Merely positing that privacy is a property right and that depriving consumers of a property right is substantial injury would read the word "substantial" right out of the statute: all misappropriation or theft of any property would become "unfair," regardless of the amount of economic harm or whether the loss posed a threat to health or safety. Similarly, merely asserting that the kind of information that can be obtained through pretexting is information that can be used to facilitate identity theft does not lead to the conclusion that pretexting causes or is likely to cause identity theft.[67]

In other words, the Commission ought to have grounded its analysis of injury in the three elements of Section 5 – but it never has.

Grappling with Children's Information

The case of children's privacy illustrates another important reason why the FTC's approach fails to reach the kind of doctrinal rigor of common law: it has often been short-circuited by statutory grants of authority requiring the FTC to issue regulations in a particular area through the Administrative Procedures Act rather than Magnuson-Moss.

Perhaps nothing so outraged Congress in the 1970s that the FTC's attempt to ban marketing to children as unfair.[68] So it is perhaps unsurprising that the FTC was reluctant to use unfairness again to protect children from a variety of emerging harms. In 1991, the Commission settled an enforcement action against a 900 number that specifically targeted children with television commercials depicting an animated rabbit who urged children to "get a pencil and write down my secret phone number."[69] Two other such settlements followed.[70] Commissioner Leary,

---

[67] Information Search, Inc., and David J. Kacala, http://www.ftc.gov/sites/default/files/documents/cases/2001/04/pretextswindle.htm

[68] [Cite to Beales Unfairness essay].

[69] Audio Communications, Inc., 114 F.T.C. 414 (1991)(consent order).

despite his skepticism of unfairness, defended these enforcement actions as legitimate uses of the doctrine in his 2000 speech about unfairness:

> Some "unfairness" cases seem primarily dependent on the particular vulnerability of a class of consumers. Children are the most conspicuous example. An illustration is In re Audio Communications, Inc. In this consent, the Commission challenged television advertisements that invited children to make 900 number calls to cartoon and other characters, which resulted in expensive phone bills for their parents. Because children were directly targeted through television ads on otherwise innocuous programs, parents had no reasonable way to avoid the charges. There was no claim of misrepresentation and the conduct might well have been entirely legal had the marketing appeals been directed at adults. Moreover, there is no suggestion that it is inherently wrong to advertise these particular services, or any others, in a way that appeals to children unless the services or products are illegal for children to buy. The problem with this particular scheme was that children could directly incur charges without adult supervision, and there was no more specific prohibition that seemed to apply.[71]

What is remarkable about this story, from a process perspective and in terms understanding the FTC's "common law" approach, is how quickly – and how – it ended. In 1992, after the FTC had brought just three cases, Congress passed the Telephone Disclosure and Dispute Resolution Act,[72] requiring the FTC to issue what became the Pay-Per-Call Rule of 1993.[73] Since then, the FTC has handled such issues through enforcement of its regulations, not Section 5.

A similar pattern played out in with children's privacy online: the FTC asserted a new interpretation of Section 5, which Congress quickly codified in the Children's Online Privacy Protection Act of 1998. In 1997, FTC staff asserted that, as FTC Pitofsky summarized the staff's view in September 1998 Congressional testimony:

> it is a deceptive practice to expressly or impliedly misrepresent the purpose for which personal identifying information is being collected from children (e.g., to represent that the information is collected for a game or contest when it is actually collected for the purpose of compiling a mailing list)… [and] it is likely to be an unfair practice to collect personal identifying information from children and sell or otherwise disclose that information to third parties without providing

---

[70] See Teleline, Inc., 114 F.T.C. 399 (1991) (consent order); Phone Programs, Inc., 115 F.T.C. 977 (1992)(consent order); Fone Telecommunications, Inc., Docket No. C-3432 (June 14, 1993) (consent order).

[71] Leary speech.

[72] [cite]

[73] 16 C.F.R. Part 308.

> parents with adequate notice and a prior opportunity to control the collection and use of the information.[74]

That August, the FTC had settled what Pitofsky called a "precedent-setting 'privacy on the Internet' case" against GeoCities, then among the largest networks of websites, for having "collected personal identifying information from its members, both children and adults, and misled them as to its use."[75] Most interesting about the *GeoCities* case is that, despite the staff's embrace of unfairness to ban the sale of PII from children without parental consent (a position embraced by the Chairman in the testimony quoted immediately above), the case rested entirely on deception. As with other cases, the Commission did not actually analyze who was the "customer" that was misled by the misrepresentations at issue, taking for granted either that it was sufficient that children were the misled customers, or that it was their parents who were misled, either directly or indirectly. Nor did the Commission indicate why it did not use unfairness.

But by October, these questions were moot: Congress enacted COPPA and, just as with 900 numbers, tasked the FTC with issuing rules under the APA to address the problem. It is remarkable how closely COPPA parallels the terms of the FTC's consent decree with Geocities, which both required verifiable parental consent for children under 13. Legislative action thus mooted the concern raised by Commission Swindle in his statement on Geocities:

> I want to emphasize that my support for these provisions as a remedy for alleged law violations in this particular case does not necessarily mean that I would support imposing these requirements on other commercial Internet sites through either legislation or regulation.[76]

State of Unfairness in 2000

So where did this leave unfairness at the turn of the millennium? The speech by Commissioner Leary mentioned above was given at a law school symposium on "Unfairness and the Internet." Commissioner Leary surveyed the state of the Commission's unfairness actions thus far. He summarized pre-Internet cases:

> The overall impression left by this body of law is hardly that policy has been created from whole cloth. Rather, the Commission has sought through its unfairness authority to challenge commercial conduct that under any definition

---

[74] Note 23, http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-protection-childrens-privacy-world-wide-web/priva998.pdf (summarizing Letter to Kathryn C. Montgomery, President, and Jeffrey A Chester, Executive Director, Center for Media Education, from Jodie Bernstein, Director, Bureau of Consumer Protection, Federal Trade Commission, regarding "Petition Requesting Investigation of, and Enforcement Action Against SpectraCom, Inc.," July 15, 1997.).

[75] Pitofsky testimony.

[76] http://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015swindlestatement.htm

> would be considered wrong but which escaped or evaded prosecution by other means.[77]

Leary reiterated his concerns about the use of *Touch Tone*[78] and ReverseAuction over "whether the privacy invasion involved in ReverseAuction was sufficiently 'substantial' to support an unfairness theory." Yet he concluded on a note of optimism:

> The extent of the disagreement should not be exaggerated, however. The majority did not suggest that all privacy infractions are sufficiently serious to be unfair and the minority did not suggest that none of them are. The boundaries of unfairness, as applied to Internet privacy violations, remain an open question.
>
> The Commission has so far used its unfairness authority in relatively few cases that involve the Internet. These cases, however, suggest that future application of unfairness will be entirely consistent with recent history. Internet technology is new, but we have addressed new technology before. I believe that the Commission will do what it can to prevent the Internet from becoming a lawless frontier, but it will also continue to avoid excesses of paternalism.
>
> The lessons of the past continue to be relevant because the basic patterns of dishonest behavior continue to be the same. Human beings evolve much more slowly than their artifacts.[79]

So, what Leary's optimism justified? Did the FTC exercise the discretion inherent in its "flexible approach" appropriately? Let us fast forward to the present, and then consider what happened in between.

Apple (2014)

In January 2014, the Commission announced the most divisive consumer protection case in recent memory. The Commission negotiated a settlement with Apple, including a record $32.5 million in refunds to consumers, for having "billed consumers for millions of dollars of charges

---

[77] Thomas B. Leary, Former Commissioner of the Fed. Trade Comm'n, *Unfairness and the Internet*, II (Apr. 13, 2000), *available at* http://www.ftc.gov/public-statements/2000/04/unfairness-and-internet. The overall impression left by this body of law is hardly that policy has been created from whole cloth. Rather, the Commission has sought through its unfairness authority to challenge commercial conduct that under any definition would be considered wrong but which escaped or evaded prosecution by other means.

[78] *Id.* at II-C ("The unfairness count in Touch Tone also raised interesting questions about whether an invasion of privacy by itself meets the statutory requirement that unfairness cause "substantial injury." Unlike most unfairness prosecutions, there was no concrete monetary harm or obvious and immediate safety or health risks. The defendants' revenue came, not from defrauding consumers, but from the purchasers of the information who received exactly what they had requested.").

[79] *Id.*, at III-IV.

incurred by children in kids' mobile apps without their parents' consent."[80] As the FTC's triumphant press release explained:

> The complaint alleges that Apple does not inform account holders that entering their password will open a 15-minute window in which children can incur unlimited charges with no further action from the account holder. In addition, according to the complaint, Apple has often presented a screen with a prompt for a parent to enter his or her password in a kids' app without explaining to the account holder that password entry would finalize any purchase at all.
>
> The settlement requires Apple to modify its billing practices to ensure that Apple obtains consumers' express, informed consent prior to billing them for in-app charges, and that if the company gets consumers' consent for future charges, consumers must have the option to withdraw their consent at any time.[81]

The settlement prompted a 17-page dissent from Commissioner Josh Wright,[82] who had previously said little about consumer protection cases, apparently preferring to focus on competition matters. Not only is this dissent far longer than any other dissent in a consumer protection case in recent memory (and perhaps ever); it also succeeded in prompting a 6-page statement from FTC Chairman Edith Ramirez and Commissioner Julie Brill,[83] plus a three page statement from Commissioner Maureen Ohlhausen (Wright's fellow minority commissioner).[84] This degree of analysis is itself extraordinary. This level of analysis could well represent a shift towards better-reasoned explanations of the Commission's decisions on significant doctrinal shifts. That, in turn, could well make the FTC's case-by-case approach more like the common law, by replicating internally some of the analytical discipline imposed by courts when they review decisions.

But Wright's dissent is essentially a condemnation of the minimal level of analytical rigor found in FTC Section 5 complaints, specifically regarding unfairness theories, but potentially also of deception as well. On the other hand, while the other Commissioners deserve credit for doing far more to explain their analysis than the Commission's analysis, the degree of rigor to their legal and economic analysis falls significantly short of what one would expect from a common law process. Indeed, it falls significantly short of the kind of analysis the FTC itself has offered in the limited number of unfairness cases it has brought in federal court since 1980 – including the very cases cited by the majority.

---

[80] http://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million

[81] Id.

[82] ("Wright Apple Dissent") http://www.ftc.gov/sites/default/files/documents/cases/140115applestatementwright_0.pdf

[83] http://www.ftc.gov/sites/default/files/documents/cases/140115applestatementramirezbrill.pdf

[84] http://www.ftc.gov/sites/default/files/documents/cases/140115applestatementohlhausen.pdf

This is not to say that the majority commissioners are necessarily wrong in their conclusion that the FTC should have filed (and settled) a complaint against Apple. Even Commissioner Wright allowed that the FTC *might* have been able to bring such a case; he merely insisted that the "Commission should have conducted a much more robust analysis to determine whether the injury to this small group of consumers justifies the finding of unfairness and the imposition of a remedy."[85]

The Low Bar for Bringing Complaints under 5(b)

The *Apple* case amply demonstrates that the FTC's "common law" turns more on Section 5(b) (the low procedural bar for bringing complaints) than on 5(a) (the supposed legal standard underlying the FTC's unfairness and deception authority).

More important than the 5(a) question (was Apple's practice really unfair?) may be the meta-question about 5(b)'s application across the board: What, exactly, should be required to bring a complaint in the first place – and, secondarily, to settle it? As noted above, this question highlights the single most important difference between the FTC's process and an actual common law process.

Commissioners Ramirez and Brill were careful to couch their statement in terms of whether the Commission has "reason to believe" a violation occurred, a term they use five times; Commissioner Wright likewise explicitly addresses this legal standard in his conclusion.[88] Indeed, in rejecting Commissioner Wright's call for a "study of how consumers react to different disclosures before issuing its complaint against Apple," Ramirez and Brill specifically cite to this provision. As a legal matter, they are correct: the bar really is set this low for the FTC to bring a complaint. It is unlikely a court would challenge the FTC's decision to issue a complaint in this case on *either* prong of the standard. Commissioner Rosch explained the "public interest" standard as follows:

> perhaps the argument that is often the most persuasive to me yet is made with the least frequency is that voting out a complaint would not be in the public interest, as Section 5 requires. That could occur in any number of circumstances, including when we are challenging conduct that is causing minimal consumer harm, when the case will not establish an important proposition of law (or may even establish bad law), when there is no clear remedy, or when there are other arguments for why a case is a poor use of the Commission's finite resources.

Commissioner Wright makes a powerful case as to why the public interest might not be served by an enforcement action against Apple – or, at least, what kind of methodology would be required to know. The kind of analysis he proposes would be a welcome change from the

[85] Wright Apple Dissent at 2.

[88] [Cite[

Commission's usual conclusory complaints. It would be a better way to determine both whether the Commission should bring an enforcement action and whether a violation actually occurred. But his ultimate claim – that "The Commission has no foundation upon which to base a reasonable belief that consumers would be made better off if Apple modified its disclosures to confirm to the parameters of the consent order"[89] – is an exceedingly difficult claim to make as a legal matter: Even if he is correct that the Commission had not shown the settlement would make consumers better off, as we ourselves believe, this is a claim to be resolved by votes among independent commissioners operating with legal discretion to decide for themselves what they had "reason to believe" might have occurred and what would be in the "public interest."

And herein lies perhaps the most important reason why the FTC's body of consent agreements is not a common law: Besides not being binding precedent and not well explained, the question the FTC is answering in each is not whether the defendant actually did violate Section 5, but merely whether the Commission has "reason to believe" the defendant *might* have and whether the Commission believes an investigation is in the public interest.

Let us first consider what the Commission's complaint and statements by the majority and minority said in Apple, and then contrast them with actual litigated cases.

The Commission's Analysis in Apple

The Commission claimed it was merely following "a long line of FTC cases establishing that the imposition of unauthorized charges is an unfair act or practice." But as Commissioner Wright notes, "Many of these cases involve unauthorized billing or cramming – the outright fraudulent use of payment information. Other cases involve conduct just shy of complete fraud – the consumer may have agreed to one transaction but the defendant charges the consumer for additional, improperly disclosed items."[93] Wright notes that "there is no evidence Apple intended to harm consumers by not disclosing the fifteen-minute window."[94] The majority responds the FTC's application of unfairness should not depend on the "intentions of the accused Party,"[95] citing the 11th Circuit's 1988 decision in *Orkin*. But all *Orkin* actually said was that "a practice may be found unfair to consumers without a showing that the offending party intended to cause consumer injury."[96] Wright was not arguing that the lack of any intention by Apple to harm consumers should end the inquiry, merely that the case turned on Apple's attempt to balance trade-offs for consumers, most notably between ease and convenience of use of the Apple store and elegance of user interface on the one hand, and further limiting the possibility that parents would incur charges made by their children during this window.

[89] Wright Apple Dissent at 17.

[93] Wright Apple Dissent at 1.

[94] *Id*.

[95] Ramirez-Brill Apple statement at 2.

[96] Id. at 1368.

Essentially (though explicitly), Wight argued that resolving legitimate design challenges[97] should be governed by a rule of reason of reason, and that the majority was applying something closer to a per se rule.

Commissioners Ramirez and Brill places great weight on precedents supporting aggregation of small harms borne by individual consumers: "It is well established that substantial injury may be demonstrated by a showing of either small harm to a large number of people or large harm in the aggregate.[98] They see this as a definitive response to Commissioner Wright's comment that the unauthorized charges at issue involved ""a miniscule percentage of consumers" and claim that it is on this basis that he concludes that the harm. But this does not do justice to Wright's argument. Wright, in fact, allows for such aggregation, but insists that "substantiality is analyzed relative to the magnitude of any offsetting benefits."[99] Ramirez and Brill charge that "This conflates the third prong of the unfairness test, calling for a weighing of countervailing benefits against the relevant harm, with the substantial injury requirement."[100] This formalism misses what is abundantly apparent from reading the Unfairness Policy Statement, given its core emphasis on "weighing" countervailing benefits: the standard is ultimately one of cost-benefit analysis. Indeed, while that term does not itself appear in the Unfairness Policy Statement, it appears eleven times in the International Harvester decision to which the statement was formally attached.[101]

The majority applies a clear double standard, aggregating small harms dispersed across many consumers, while dismissing any suggestion that countervailing benefits should be assessed on an aggregate basis. They have clear precedent on their side for aggregation of costs (which Wright, too, acknowledges). But neither side can point to any such precedent regarding aggregation of benefits. But this is precisely Wright's point: this is a different case from the cases cited by the majority. As a doctrinal edge case, this illustrates a vital difference between the Commission's approach and a true common law: Rather than resolve this important question, the majority simply wins and, because Apple is unwilling to litigate the case, that is the end of the matter. The two sides do not even specifically address this issue (although Wright's proposed methodology rests on the idea of aggregating benefits).

Ramirez and Brill explain their analysis:

> This is not a case about Apple's "choice to integrate the fifteen-minute window into Apple users' experience on the platform," as Commissioner Wright implies. What is at issue is Apple's failure to disclose the 15-minute window to parents

---

[97] Cf infra at __ (discussing Frostwire and Designerware).

[98] Majority Apple statement at 3 (See FTC v. Neovi, Inc., 604 F.3d 1150, 1157 (9th Cir. 2010), amended, 2010 WL 2365956 (9th Cir. June 15, 2010); Orkin, 849 F.2d at 1365; FTC Unfairness Statement n.12).

[99] Wright Apple Dissent at 5.

[100] Ramirez-Brill Apple statement at 3.

[101] [Cite]

> and other account holders in connection with children's apps, not Apple's use of a 15-minute window as part of the in-app purchasing sequence
>
> Under the proposed consent order, Apple is permitted to bill for multiple charges within a 15-minute window upon password entry provided it informs consumers what they are authorizing, allowing consumers to make an informed choice about whether to open a period during which additional charges can be incurred without further entry of a password. The order gives Apple full discretion to determine how to provide this disclosure. But we note that the information called for, while important, can be conveyed through a few words on an existing prompt. The burden, if any, to users who have never had unauthorized charges for in-app purchases, or to Apple, from the provision of this additional information is de minimis. **Nor do we believe** the required disclosure would detract in any material way from a streamlined and seamless user experience. **In our view**, the absence of such minimal, though essential, information does not constitute an offsetting benefit to Apple's users that even comes close to outweighing the substantial injury the Commission **has identified**.

In the same vein, they continue:

> **we do not think** that Commissioner Wright's **belief** that Apple "has more than enough incentives to disclose" is justified. Indeed, his argument appears to presuppose that a sufficient number of Apple customers will respond to the lack of adequate information by leaving Apple for other companies. But customers cannot switch suppliers easily or quickly. Mobile phone and data contracts typically last two years, with a penalty for early termination. In addition, the time and effort required to learn another company's operating system and features, not to mention the general inertia often observed for consumers with plans for cellular, data, and Internet services, **could very well mean** that Apple customers **may not be** as responsive to Apple's disclosure policies as seems to be **envisioned** by Commissioner Wright.[102]

What matters for our purposes is not which side is correct, but merely to observe that Ramirez and Brill themselves are not even purporting to argue that their analysis would be adequate to actually resolve the ultimate question of liability under Section 5(a), merely to justify issuance of a complaint under Section 5(b). Their argument is carefully couched in terms of what they "believe" about countervailing benefits relative to the "substantial injury the Commission has identified," and a skepticism about Wright's "belief" that Apple has adequate incentives to strike the right balance for consumers between more disclosure and other values, like seamlessness of user interface design.

---

[102] Ramirez-Brill at 5-6 (emphasis added)

However correct as a matter of FTC administrative procedure and interpretation of Section 5(b) this approach might be, it contrasts starkly with the cases cited by Ramirez and Brill. This obvious difference is, as Wright notes, that, in all these cases, the defendant was trying to trick customers into buying things they did not want with no cognizable benefit to the customer. The less obvious difference, which neither side in *Apple* notes, is that, even in these much more clear-cut cases, the Commission bolstered its analysis with actual empirical evidence. The reason should, by now, by obvious: In making its case before a federal judge seeking either an injunction or a final judgment, the Commission needed real evidence. Again, in a *real* common law, mere assertions do not suffice – and the Commission has proven itself perfectly capable of providing the evidence needed to win cases.

Wright notes:

> Staff has not conducted a survey or any other analysis that might ascertain the effects of the consent order upon consumers. The Commission should not support a case that alleges that Apple has underprovided disclosure without establishing this through rigorous analysis demonstrating – whether qualitatively or quantitatively – that the costs to consumers from Apple's disclosure decisions have outweighed benefits to consumers and the competitive process. The absence of this sort of rigorous analysis is made more troublesome in the context of a platform with countless product attributes and where significant consumer benefits are intuitively obvious and borne out by data available to the Commission. We cannot say with certainty whether the average consumer would benefit more or less than the marginal consumer from additional disclosure without empirical evidence. This evidence might come from a study of how customers react to different disclosures. However, given the likelihood that the average benefit of more disclosure to unaffected customers is less than the benefit to affected customers who are likely to be customers closer to the margin, **I am inclined to believe** that Apple has more than enough incentive to disclose.

Wright's reference to what the Commission can "say with certainty," is of course far more than the Commission is required to establish under its "reason to believe" standard, but it can be understood as a proposal for how the FTC should weigh whether the complaint – really, the settlement – is in the public interest. Ramirez and Brill conclude that, because "The burden, if any, to users who have never had unauthorized charges for in-app purchases, or to Apple, from the provision of this additional information is de minimis," "it was unnecessary for the Commission to undertake a study of how consumers react to different disclosures before issuing its complaint.[103]

[103] Ramirez-Brill at 5 and note 16.

Ramirez and Brill cite four cases where the FTC sought preliminary injunctions against companies making fraudulent charges on consumers' bills. In three, the FTC received an in junction and, in a fourth, the FTC settled the complaint. But in all four, the FTC had clear empirical evidence of consumer harm. All four pointed to "chargeback" rates, the percentage of credit card charges reversed by credit card issuers after consumers complained, as being far above the 1% threshold generally monitored by credit card issuers as evidence that a company might be engaged in fraud.[104] Two of the cases provided additional empirical survey data showing that consumers did not want these charges – the same kind of survey methodology proposed by Wright even though its focus was on injury rater than, as Wright's proposed study would have been, on both whether Apple misled customers and on how they might react to the kind of additional disclosure required by the FTC's settlement.

For example, in *FTC v. Willms*, the unfair practice was enrolling customers in "free" or "risk-free" trials for products without "adequately inform[ing them] that the purchase was not free or that they were being enrolled in a recurring fee program wherein they would be charged for products or services unless they opted out shortly after placing their order."[105] In support of the deception count, the FTC provided both "substantial anecdotal testimony" and statistical evidence showing that Willms' billing practices were actually misleading."[106] In support of the unfairness count, the FTC cited statistical evidence showing that up to 22.7% of defendants charges to consumers were charged back to the company, far above the 1% threshold that credit card issuers use to detect fraudulent activity.[107]

In *FTC v. Inc21.com Corp.*, the issue was a similar form of fraud: "cramming" of various unauthorized charges onto telephone bills.[108] Here, the FTC's evidence of injury was overwhelming: "nearly 97 percent of defendants' tens of thousands of "customers" did not agree to purchase defendants' products and over $37 million in largely unauthorized charges flowed directly to defendants through LEC billing."[109] The court rejected the countervailing

---

[104] [Cite]. In FTC v. Crescent Publ'g Grp., Inc., 129 F. Supp. 2d 311, 322 (S.D.N.Y. 2001), the company had misrepresented the point at which "free tour" of its pornographic sites ended and made unauthorized charges against visitors' credit cards. "Crescent and affiliates had an average charge back rate of approximately 10.51 percent in 1999. High in itself, this figure does not reflect the full extent of customer dissatisfaction as it does not include the additional 28 percent of sales that the companies credited back to customers during the same period." In Complaint, FTC v. Jesta Digital, LLC, No. 1:13-cv-01272 (D.D.C. filed Aug. 20, 2013), the FTC settled an unfairness case against a company that showed ads on Android mobile devices claiming that the user had viruses on their device and inviting them to click on the banner ad's "REMOVE" button, which took them to a site offering downloads of antivirus software for $9.99/month. The Commission offered empirical evidence showing that only .372% of customers actually got a download link http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130821jestacmpt.pdf

[105] FTC v. Willms, No. 2:11-CV-828 MJP, 2011 WL 4103542, at *9 (W.D. Wash. Sept. 13, 2011);

[106] Id at ___.

[107] Id. at *9.

[108] *FTC v. Inc21.com Corp.*, 745 F. Supp. 2d 975 (N.D. Cal. 2010), aff'd, 475 Fed. Appx. 106 (9th Cir. Mar. 30, 2012).

[109] At 1004.

benefits cited by the defendants ("spending over $350,000 in search-engine marketing fees for JumPage customers") as "far outweighed by the $37 million in unauthorized payments extracted from them" and probably no benefit at all anyway: "nearly 97 percent of defendants' "customers" never wanted these "benefits" in the first place. Moreover, 96 percent of defendants' "customers" stated that they received *no services* from defendants or their products." The Commission also provided empirical evidence regarding avoidability: "only five percent of defendants' "customers" ever noticed these charges appearing on their telephone bills."[110]

In summary, in an actual common law situation, even where the cases were much easier, the Commission provided empirical evidence to establish substantial injury. Yet in the *Apple* case, the Complaint merely asserts:

> Apple has received at least tens of thousands of complaints related to unauthorized in-app charges by children in these and other games. …. Many consumers report that they and their children were unaware that in-app activities would result in real monetary loss…. Many children incur unauthorized in-app charges without their parents' knowledge. [111]

Neither Ramirez and Brill nor Ohlhausen provide any additional empirical data. The complaint asserts, in the conclusory boilerplate apparently copy-pasted from other FTC's complaints, that Apple's product design decisions "cause or are likely to cause substantial injury to consumers that consumers themselves cannot reasonably avoid and that is not outweighed by countervailing benefits to consumers or competition consumers themselves cannot reasonably avoid and that is not outweighed by countervailing benefits to consumers or competition.[112]

On avoidability, Ramirez and Brill declare that "An injury is not reasonably preventable by consumers unless they had an opportunity to make a 'free and informed choice' to avoid the harm," quoting the Ninth Circuit's 2010 decision in *Neovi*.[113] They conclude "In light of Apple's failure to disclose the 15-minute purchasing window, it was reasonable for parents not to expect that when they input their iTunes password they were authorizing minutes of unlimited purchases without the child having to ask the parent to input the password again." In *Neovi*, a website operator created a website that "allowed users to create and deliver unverified checks drawn from unauthorized accounts;" through a "profound lack of diligence," the website was used to cash hundreds of thousands of unverified checks, resulting in $402 million in consumer fraud. The court held that:

---

[110] At 1004. The court held that: "This order declines to allow defendants to blame unsuspecting consumers for failing to detect and dispute unauthorized billing activity. As other courts have wisely concluded, the burden should not be placed on defrauded customers to avoid charges that were never authorized to begin with."

[111] Apple Complaint at 6, http://www.ftc.gov/sites/default/files/documents/cases/140115applecmpt.pdf

[112] Apple complaint at 6.

[113] FTC v. Neovi, 604 F.3d 1150 (9th Cir. 2010).

> It is likely that some consumers never noticed the unauthorized withdrawals. Even if the consumer did notice, obtaining reimbursement required a substantial investment of time, trouble, aggravation, and money. Further, Defendants' uncooperativeness only increased this outlay. Neither could consumers mitigate the period of time during which they lost access to and use of the funds taken using Defendants' fraudulent checks. Regardless of whether a bank eventually restored consumers' money, the consumer suffered unavoidable **injuries** that could not be fully mitigated.[114]

Clearly, there is *some* analogy to the Apple case, insofar as both involve the question of a consumer's duty to monitor credit card bills for signs of fraud. But Wright notes a number of distinguishing characteristics that the majority simply does not address:

> By entering their password into the Apple device – an action that is performed in response to a request for permission – parents were effectively put on notice that they were authorizing a transaction. Although the complaint alleges that the fifteen-minute window was not expressly disclosed to parents, regular users of Apple's platform become familiar with the opportunity to make purchases without entering a password every time. Even if some parents were not familiar with the fifteen-minute window, the requirement to re-enter their password to authorize a transaction arguably triggered some obligation for them to investigate further, rather than just to hand the device back to the child without further inquiry.[115]

Again, the immediate point is not which side is correct, but simply that the FTC's debate over whether to open (and then immediately close) an investigation does not address these doctrinal questions in the way that a common law process would.

Orkin (1988)

In explaining their position in Apple, Commissioners Ramirez and Brill place great weight on the Eleventh Circuit's 1988 *Orkin* decision on several grounds. (The court upheld the FTC's administrative order finding Orkin had violated Section 5 by unilaterally raising a pre-set annual renewal fee on 200,000 termite warranties it had signed with its customers."[116]) Mostly, the court validated should have been apparent from the Unfairness Policy Statement Itself (which Wright accepts): "although the actual injury to individual customers may be small on an annual basis, this does not mean that such injury is not "substantial.'"[117]

---

[114]

[115] Wright Apple dissent at 10.

[116] 849 F.2d 1354 (11th Cir. 1988).

[117] Id. at 1365.

The court also said that "a practice may be found unfair to consumers without a showing that the offending party intended to cause consumer injury,"[118] but as we have seen, this is not exactly the concern Wright raised.

Ramirez and Brill seem to cite Orkin as evidence that the Commission need not undertake a rigorous assessment of unfairness. The court does refer to the statute in broad terms:

> Of course, the Commission's three-part standard does little to isolate the specific types of practices and consumer injuries which are cognizable. But "the consumer injury test is the most precise definition of unfairness articulated by either the Commission or Congress"; consequently, we must resolve the validity of the Commission's order "by reviewing the reasonableness of the Commission's application of the consumer injury test to the facts of this case, and the consistency of that application with congressional policy and prior Commission precedent." A.F.S., 767 F.2d at 972; see also Indiana Federation of Dentists, 106 S.Ct. at 2016.

But *Orkin* says little about how cost-benefit analysis should be performed in less clear-cut cases. The court noted that, "because '[t]he increase in the fee was not accompanied by an increase in the level of service provided or an enhancement of its quality,' the Commission concluded that no consumer benefit had resulted from Orkin's conduct." [119] The injury in this case was plain: "Orkin's breach of its pre-1975 contracts generated, during a four-year period, more than $7,000,000 in revenues from renewal fees to which the Company was not entitled." And Orkin's arguments about countervailing benefits were so feeble that Orkin did not even press them on appeal.

The Court agreed with the FCC on avoidability that:

> "neither anticipatory avoidance nor subsequent mitigation was reasonably possible for Orkin's pre-1975 customers." Anticipatory avoidance through consumer choice was impossible because these contracts give no indication that the company would raise the renewal fees as a result of inflation, or for any other reason.
>
> As for mitigation of consumer injury, the Commission concluded that the company's "accommodation program" could not constitute an avenue for avoiding injury because relief from Orkin's conduct was available only to those customers who complained about the increases in the renewal fees. [120]

---

[118] Id. at 1368.

[119] Id. at 1365.

[120] Id. at 1365-6.

Yet in the FTC's "common law" *Orkin* is supposedly the basis for explaining how to weigh the factors of unfairness against each other. *Orkin* and the FTC's reliance upon *Orkin* in cases like *Apple* simply demonstrates the doctrinal thinness of the FTC's supposed "common law."

Pereira (1999)

So what happens when the FTC actually has to go into court?

Let us return to the historical development of unfairness that eventually produced *Apple*. Cramming unauthorized charges is not the only practice the Commission has successfully litigated against in federal court. More relevant to privacy and data security cases is the FTC's 1999 motion for an injunction against Pereira.[121] Commissioner Leary summarized the case in his 2000 speech on the "Internet and Unfairness":

> the Commission challenged two Internet technology frauds, "pagejacking" and "mousetrapping." The defendants, located in Portugal and Australia, had captured unauthorized copies of U.S.-based websites, including those of Paine Webber and the Harvard Law Review. They produced look-alike versions that were indexed by major search engines. Consumers, expecting to visit these or others sites, found themselves at one of the defendants' pornographic sites. This "pagejacking" part of the scheme was challenged as a deceptive misrepresentation of the true identity of the defendants' web sites. Once there, consumers either were prevented from leaving the site or were diverted to a sequence of pornography sites which also could not be exited. This is the "mousetrapping" part of the scheme, which was attacked as unfair.[122]

Because these websites were overseas, the FTC could not simply settle the matter, as it usually did: The only way it could shut down the websites was to convince a Federal court to issue a temporary restraining order that the FTC could use to get Network Solutions, operator of the .COM registry, to suspend the domain names at issue.

The misrepresentation element of the deception claim required little explanation, since it was so obvious, yet the FTC explained it anyway – and analogized the case to a legal concept specifically referenced in the Deception Policy Statement.[123] The FTC's explanation of

---

[121] http://www.ftc.gov/sites/default/files/documents/cases/1999/09/990922memo9923264.shtm#Subject

[122] Leary 2000 speech.

[123] "The evidence demonstrates that in order to induce consumers to go to their adult sites, defendants have expressly misrepresented the true identity of their Web sites. Search engine descriptions for their hijacked Web pages are virtually identical to descriptions of original Web pages created by unrelated third parties. [Forbes Dec. at 3, 4; Exh. 1, Attachs. A-E.] When consumers click on a search result describing a Web page for the movie "Saving Private Ryan" or some other subject, consumers are not carried to a site about movies, World War II or some other innocuous topic. Rather, consumers are redirected to defendants' own graphic adult Web sites. [Exh. 1, Attach. A.] In this way, defendants' pagejacking creates deceptive "door openers" on the Internet. Such

materiality was short, but at least they offered one, which is more than can be said for most FTC enforcement actions:

> defendants' pagejacking is deceptive and material to any reasonable consumer. Consumers act reasonably when they go to a search engine to find information on the Internet. Pagejacking materially undermines consumers' ability to find quality Web sites and can drastically affect where they go when they click on specific search results.

On unfairness, the FTC offered far greater analysis. It alleged four clear forms of potential injury:

> One consumer who performed a routine Internet search at work was taken to an adult site as a result of defendants' pagejacking, and then he was trapped there. Accessing adult sites at his place of employment violated his employers' policies and subjected him to possible dismissal. [Exh. 1, Attch. P.] Another consumer owned a business that was targeted by defendants' practices and undermined the value of his Internet company at a time that when he was trying to sell it. [Exh. 3 ¶¶ 2, 3.]…
>
> In many cases, the only way to escape from defendants' mouse trap is to immediately shut off one's computer; consequently, defendants' practices also could cause consumers to lose valuable data, or damage their computers or Internet browsers. Finally, defendants' practices prevent consumers from locating the Web sites they desire to visit, thereby diminishing the usefulness of the Internet and impairing the growth of e-commerce as a whole. [Exh. 1, Attach. P.]

While the Commission did not undertake an empirical study, this evidence sufficed to convince the court.

More complicated was the FTC's theory of injury to children. The FTC offered an example: "When one child was searching the Internet for more information about the country of Kosovo, defendants' trapped him in one of their sexually explicit Web sites, and the child's father had to

---

"door openers" are deceptive by law, even where the truth is made known prior to a purchase. The evidence demonstrates that in order to induce consumers to go to their adult sites, defendants have expressly misrepresented the true identity of their Web sites. Search engine descriptions for their hijacked Web pages are virtually identical to descriptions of original Web pages created by unrelated third parties. [Forbes Dec. at 3, 4; Exh. 1, Attachs. A-E.] When consumers click on a search result describing a Web page for the movie "Saving Private Ryan" or some other subject, consumers are not carried to a site about movies, World War II or some other innocuous topic. Rather, consumers are redirected to defendants' own graphic adult Web sites. [Exh. 1, Attach. A.] In this way, defendants' pagejacking creates deceptive "door openers" on the Internet. Such "door openers" are deceptive by law, even where the truth is made known prior to a purchase.

intervene. Unfairly and deceptively marketing to children, who are recognized as a vulnerable group in the marketplace, violates § 5 of the FTC Act." The FTC cited to its three cases involving marketing of 900 numbers to children.[124] While tricking children into viewing pornography sites *is* a form of marketing: after all, the purpose of this racket was, presumably, to get some customers to pay for pornography, or provide credit card information that could be used to make fraudulent charges. But the FTC did not actually explain what, exactly, the injury here was. Instead, it essentially cited its past settlements as creating a presumption of injury to a protect class as a "vulnerable group in the marketplace." Arguably, as Swindle argued in *Touch Tone*, this violated Section 5(n) by resting a claim of unfairness on FTC enforcement actions as evidence of public policy, something the 1994 amendments to Section 5 specifically prohibit being the "primary basis for such determination."[125]

Of course, since the FTC sought only a temporary restraining order, the court's decision does not evaluate this question. It says nothing other than that the FTC had met the standard for issuing a TRO: "There is good cause to believe that the defendants have engaged and are likely to engage in acts and practices that violate Section 5(a) … and that the Commission is therefore likely to prevail on the merits of this action."[126]

The Commission provided far more analysis of countervailing benefits, something generally mentioned only in passing in FTC complaints:

> The practice of trapping consumers at Web sites they never wanted to visit has few if any public benefits -- either economic or otherwise. The only benefits derived from this scheme are to defendants who likely receive revenues for each site visit or click through. Defendants' scheme denigrates the integrity of the Internet and benefits no one except themselves. [Exh. 2 ¶¶ 13, 14.] Indeed, this practice is detrimental to commerce on the Internet. According to PaineWebber, defendants hijacked dozens of the company's sites which resulted in consumers being taken to defendants' sexually-explicit Web sites instead of PaineWebber's financial Web sites. [Exh. 4, Attach. A.] Such practices clearly denigrate consumers' confidence in both providers of the information (here, PaineWebber) and search engines (here, AltaVista).

The FTC's analysis of reasonable avoidability was even stronger:

> The injury caused by defendants' mouse trapping is not reasonably avoidable because consumers have no advance warning of what is about to happen to them, [Exh. 2 ¶ 6; Exh. 3 ¶ 2; Exh. 4, Attach. B; Forbes Dec. at 4.], nor can they do anything about it once they learn their browser does not function properly. Once

[124] [Cite]

[125] See supra at ___.

[126] http://www.ftc.gov/sites/default/files/documents/cases/1999/09/990922tro9923264.shtm

> hijacked to defendant WTFRC's adult sites, consumers cannot avoid being trapped in the site. The transfer to defendants' Web sites is practically unseen by consumers. And, because defendants have overridden the normal Internet browser functions, neither the "back" or "X" buttons function in the way in which they were intended. Consumers (including children) are trapped looking at pornography, and trying to escape only makes the problem worse.

The point of this case is that the FTC can, when pressed, explain its analysis.

Public Policy Considerations under Section 5(n)

Much of the normative argument made by Solove and Hartzog in defense of the FTC's current approach, and of an even more active FTC, rests on their claim that: "The FTC is able to consider a more complete range of concerns than much of contract and tort law, and it is thus able to come to a balance that is more subtle and comprehensive of everything at stake."[127] They quote the 1980 Unfairness Policy Statement: "Sometimes public policy will independently support a Commission action. This occurs when the policy is so clear that it will entirely determine the question of consumer injury, so there is little need for separate analysis by the Commission."[128] But they do not mention that Congress narrowed the FTC's ability to weigh public policy considerations when it amended Section 5 in 1994.

The Supreme Court's broadly worded 1972 decision in *Sperry & Hutchinson* affirmed the approach to unfairness the FTC began in 1964, relying on three separate factors, in order of importance: "(1) whether the practice injures consumers; (2) whether it violates established public policy; (3) whether it is unethical or unscrupulous."[129] Armed with this power, the Commission set off on a series of rulemakings and enforcement actions that prompted a dramatic confrontation with Congress in 1980. The FTC was briefly defunded, and was able to negotiate its way out of the situation only by issuing the Unfairness Policy Statement that has become, at least nominally, the bedrock of the FTC's subsequent approach to unfairness. The FTC eliminated entirely the "unethical or unscrupulous" prong while narrowing the "public policy" prong:

> Although public policy was listed by the *S&H* Court as a separate consideration, it is used most frequently by the Commission as a means of providing additional evidence on the degree of consumer injury caused by specific practices. … Sometimes public policy will independently support a Commission action. This occurs when the policy is so clear that it will entirely determine the question of consumer injury, so there is little need for separate analysis by the Commission. … To the extent that the Commission relies heavily on public policy to support a

---

[127]

[128] S&H at 34, UPS.

[129] UPS

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

Solove & Hartzog laud this compromise as allowing the FTC to continue evaluating public policy on its own, and thus taking a more activist approach to data protection. But they do not consider the effect of the 1994 codification of the Unfairness Policy Statement in to Section 5(n). The first sentence of subsection (n) incorporated the three-prong assessment of substantial injury, countervailing cost and avoidability. The second sentence allows the FTC to consider "established public policies as evidence to be considered with all other evidence," but the third sentence appears to narrow the FTC's discretion within what the Unfairness Policy Statement would have allowed: "Such public policy considerations may not serve as a primary basis for such determination." In other words, the Policy Statement allowed the FTC to define public policy if it is well-defined in other statutes and widely shared as a proxy for identifying substantial injury – but subsection (n) does not. Thus, for example, under the Unfairness Policy Statement, it might have been sufficient for the FTC to ground its approach to data protection on the Gramm-Leach-Bliley statute and the Data Safeguards rule issued by the FTC thereunder, but subsection (n) requires that this kind of extension of "public policy," however well recognized, is not sufficient on its own; indeed, it cannot even be the "primary basis" for the FTC's approach – precisely Swindle's point in *Touch Tone*.[130] The FTC must do more to assess three factors that are supposed to be the focus of unfairness: injury, benefit and avoidability. What, precisely, that inquiry should look like is not clear from the statute, but *something* more is clearly required.

Data Security

The FTC's approach to data security may be understood in essentially three phases:

- **2000-2005**: Enforcement actions premised on deception and, starting in 2002, essentially incorporation of the "Data Safeguards Rule" prescribing data security requirements for financial institutions under the Gramm–Leach–Bliley Act of 1999.
- **2005-2009**: Enforcement actions premised on unfairness as well as deception.
- **2009-2014**: A more aggressive approach to data security enforcement actions

[130] See __.

Phase I: Data Security through Deception

The FTC's first foray into data security regulation – often forgotten – was quite narrow: It punished the deliver to failure to a form of security specifically promised to customers. An online pharmacy had promised customers that their credit card information "is transmitted to us using a SSL secure connection," which was not, in fact, true.[131] This was an uncontroversial deception claim, with Commission Swindle dissenting on other grounds (whether the company had deceived consumers by emailing them, but not third parties, about more than just medical issues).

In 2002, the Commission began its current approach, treating Eli Lilly's more general promise as the basis for a deception claim:

> Our Web sites have security measures in place, including the use of industry standard secure socket layer encryption (SSL), to protect the confidentiality of any of Your Information that you volunteer; however, to take advantage of this your browser must support encryption protection (found in Internet Explorer release 3.0 and above). These security measures also help us to honor your choices for the use of Your Information."[132]

Commissioner Swindle did not dissent.[133] The case was uncontroversial because Eli Lilly's "data breach" was clear: a company employee inadvertently included all email addresses of Prozac patients in the "To" line of a mass email, thus disclosing both their email addresses and the fact that they were being treated for depression with Prozac. The Complaint focused on the company's failure to maintain appropriate "internal measures appropriate under the circumstances to protect sensitive consumer information," such as "appropriate training for its employees," "oversight and assistance for the employee who sent out the email," and "checks and controls on the process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the email."

Later in 2002, the FTC brought a similar action against Microsoft, but this time more clearly focused on the adequacy of the company's *technical* safeguards.[134] This time, Commissioner Swindle issued no statement at all.

---

[131] http://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogcomp.htm

[132] http://www.ftc.gov/sites/default/files/documents/cases/2002/05/elilillycmp.htm

[133] http://www.ftc.gov/sites/default/files/documents/cases/2002/01/lillyswindlestat.htm

[134] disclosure of personal information resulted from respondent's failure to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information. For example, respondent failed to provide appropriate training for its employees regarding consumer privacy and information security; failed to provide appropriate oversight and assistance for the employee who sent out the email, who had no prior experience in creating, testing, or implementing the computer program used; and failed to

The Commission issued, and settled, six more such complaints between 2003 and 2005, focused entirely on deception.[135] The enforcement action against Tower Records, for example, noted the company's promise to "use state-of-the-art technology to safeguard your personal information," while, in fact, the company's online checkout system allowed visitors to the website to harvest the credit card information of 5,225 consumers, much of which was posted online.[136]

Phase II: Data Security through Unfairness

In 2005, filed its first data security action premised on unfairness against BJ's Warehouse. Unlike past defendants, BJ's had, apparently, made no promise regarding data security on which the FTC could have hung a deception action.[137] Instead the Commission alleged:

> Respondent did not employ reasonable and appropriate measures to secure personal information collected at its stores. Among other things, Respondent (1) did not encrypt the information while in transit or when stored on the in-store computer networks; (2) stored the information in files that could be accessed anonymously -- that is, using a commonly known default user id and password; (3) did not use readily available security measures to limit access to its computer networks through wireless access points on the networks; (4) failed to employ sufficient measures to detect unauthorized access or conduct security investigations; and (5) created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business need to keep the information, and in violation of bank rules. As a result, a hacker could have used the wireless access points on an in-store computer network to connect to the network and, without authorization, access personal information on the network.[138]

The Complaint plead substantial injury as follows:

> banks began discovering fraudulent purchases that were made using counterfeit copies of credit and debit cards the banks had issued to customers. The customers had used their cards at Respondent's stores before the fraudulent purchases were made, and personal information Respondent obtained from their cards was stored on Respondent's computer networks. This same information was contained on counterfeit copies of cards that were used to

---

implement appropriate checks and controls on the process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the email.

[135] CartManager International, August 26, 2005; Nationwide Mortgage Group, April 15, 2005; Petco March 8, 2005; Sunbelt Lending Services, January 7, 2005; Tower Records, June 2, 2004; Guess, August 5, 2003.

[136] http://www.ftc.gov/sites/default/files/documents/cases/2004/06/040602comp0323209.pdf

[137] http://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter

[138] http://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf

> make several million dollars in fraudulent purchases. In response, banks and their customers cancelled and re-issued thousands of credit and debit cards that had been used at Respondent's stores, and customers holding these cards were unable to use their cards to access credit and their own bank accounts.

The Complaint concluded with what has become the familiar, conclusory statement:

> 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

The Complaint offered no further analysis, nor did the Commission's order,[139] nor did the Commission's "Analysis of Proposed Consent Order to Aid Public Comment."[140] Nowhere did the Commission perform any cost-benefit analysis, nor analyze whether consumers could reasonably have avoided the injury alleged. Given Commissioner Swindle's longstanding concerns about the use of unfairness, and the need for clear limiting principles to avoid repeating the mistakes made by the FTC in the 1970s, it is worth noting that the original complaint was approved by the Commission less than two weeks[141] before Commissioner Swindle's retirement from the Commission in June 2005.[142] While Swindle could, in theory, have expressed his concerns at that point, he had left the Commission by the time the Commission settled the matter in September.

In 2004 Congressional Testimony, Swindle endorsed, in principle, the use of unfairness in data security cases:

> To date, the Commission's security cases have been based on its authority to prevent deceptive practices, [but it] also has authority to challenge practices as unfair if they cause consumers substantial injury that is neither reasonably avoidable nor offset by countervailing benefits. The Commission has used this authority in appropriate cases to challenge a variety of injurious practices, including unauthorized charges in connection with "phishing.[143]

---

[139] http://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305do0423160.pdf

[140] http://www.ftc.gov/sites/default/files/documents/cases/2005/06/050616anal0423160.pdf

[141] http://www.ftc.gov/sites/default/files/documents/cases/2005/06/050616comp0423160.pdf

[142] http://www.ftc.gov/news-events/press-releases/2005/05/statement-federal-trade-commissioner-orson-swindle

[143] Prepared Statement of the FTC, *Protecting Information Security and Preventing Identity Theft*, presented by Commissioner Orson Swindle to House Comm. on Gov't Reform, Subcomm. on Tech.,Info. Policy, Intergovernmental Relations, and the Census, at 7, 14 n.24 (Sept. 22, 2004) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-

Still, looking back at the subsequent evolution of data security cases, one cannot help but wonder if Swindle would have been comfortable with *how* the FTC applied its data security authority in *BJ's Warehouse* and after.

Again, the immediate point is not that this was necessarily an inappropriate use of unfairness, but that the Commission made a major doctrinal leap with no explanation. So what might a dissent have looked like? Indeed, what might Commissioner Wright have asked had he been on the Commission at that point? Or what would actual litigation have looked like?

Clearly, in actual litigation, the Commission's conclusory allegations would not have sufficed. Even in the cramming and fraud cases discussed above, the Commission had to establish injury with greater precision and to explain its analysis of both avoidability and countervailing benefits.

A dissent might have argued, as Commissioner Wright did in Apple, that [FINISH]

Focus of the Commission's Approach

The Commission's data security cases were fairly clear-cut, focusing on data security vulnerabilities that few, if any, would really defend.

Data Safeguards Rule

The Commission grounded its approach, especially the remedies it imposed on companies in settlements, in the Data Safeguards Rule.[144]

What Was <u>Not</u> Unreasonable

As the Commission developed its unfairness "common law" of data security, it did, at least on one occasion, provide guidance as to what did *not* constitute data security so "unreasonable" that it was unfair. In 2007, the FTC issued a no-action letter closing its investigation into Dollar Tree Stores that offers considerable background on the issue: "PED skimming," the tampering with or left of the "PIN entry devices" (PEDs) used at checkout to allow customers to enter the PIN for their debit card.[145] This allowed hackers to steal customers' card information and thus make fraudulent purchases.

The FTC explained its decision to close the Dollar Tree Stores investigation at length:

---

commission-protecting-information-security-and-preventing-identity/040922infosecidthefttest.pdf) ("*Comm'r Swindle's 2004 Information Security Testimony*").

[144] [cite].

[145] http://www.ftc.gov/sites/default/files/documents/closing_letters/dollar-tree-stores-inc./070605doltree.pdf

Despite these concerns, the staff has determined to close the investigation. Among the factors we considered were the extent to which the risk at issue was reasonably foreseeable at the time of the compromise; the nature and magnitude of the risk relative to other risks; the benefits relative to the costs of protecting against the risk; Dollar Tree's overall data security practices; the duration and scope of the compromise; the level of consumer injury; and Dollar Tree's prompt response to the incident. Applying these factors, the circumstances in this matter contrast significantly with those in recent enforcement actions brought by the Commission. For example, in the Commission's actions against CardSystems Solutions, DSW, ChoicePoint, and BJ's Wholesale Club, we alleged multiple failures to address well-known vulnerabilities; failure to use readily available, and often inexpensive security measures; and substantial injury to consumers in the form of account fraud, time loss, and inconvenience.[3]

We continue to emphasize that data security is an ongoing process, and that as risks, technologies, and circumstances change over time, companies must adjust their information security programs accordingly. The staff notes that, in recent months, the risk of PED skimming at retail locations has been increasingly identified by security experts and discussed in a variety of public and business contexts. We also understand that some businesses have now taken steps to improve physical security to deter PED skimming, such as locking or otherwise securing PEDs in checkout lanes; installing security cameras or other monitoring devices; performing regular PED inspections to detect tampering, theft, or other misuse; and/or replacing older PEDs with newer tamper-resistant and tamper-evident models. We hope and expect that all businesses using PEDs in their stores will consider implementing these and/or other reasonable and appropriate safeguards to secure their systems.

Also essential was that the risk in this case was a particularly creative form of PED skimming:

[2] The PED skimming variant here appears to have involved a sophisticated criminal enterprise: an unauthorized individual apparently dismantled PEDs at several Dollar Tree stores; used a hidden memory chip to secretly capture personal information; and then later returned to the stores, removed (and possibly replaced) the PEDs, and used the information to create counterfeit payment cards.

In essence, the FTC drew a line between cases where the injury to consumers was reasonably foreseeable and could be mitigated at a relatively small expense and those where, because of the "sophisticated" nature of the threat, it was not reasonably foreseeable or could not be prevented by "reasonable" data security measures.

Phase III: Unfairness Cases (2009- 2014)

The change of administrations and thus of FTC Chairmen and Directors of the Bureau of Consumer Protection in 2009 set in motion major changes in the FTC's approach to data security. While most of its enforcement actions were consistent with those undertaken in the 2005-2009 period, four cases highlight these changes. Again, for our purposes, what matters is not the substantive merits of these cases, but what they say about the difference between the FTC's approach and a true common law.

http://www.ftc.gov/enforcement/cases-proceedings/102-3076/lookout-services-inc-matter

Closing Letters

Again, clarity as to what the law does *not* prohibit may a more important hallmark of a common law system than specificity to what it prohibits. The FTC has issued only one closing letter in standard data security cases since its 2007 letter in *Dollar Tree Store* – and, apparently, about the same issue: In 2011, the FTC issued latter closing its investigation of Michael's art supply stores.[146] The letter offers essentially no information about the investigation or analysis of the issue (in marked contrast to the Dollar Tree Stores letter), but based on press reports from 2011, the issue appears to have been the same: "crooks [had] tampered with PIN pads in the Michaels checkout lanes, allowing them to capture customers' debit card and PIN numbers."[147]

The fact that the FTC's 2012 letter on what appears to be the same issue says essentially nothing is itself indicative of how the change in chairmen has affected the FTC's willingness to provide guidance as to what is *not* a violation. But even more important is that this very issue – whether a particular technological threat was a reasonably foreseeable and should have been protected against prophylactically – underlies both the pending legal challenges to the FTC's approach to data security, the *Wyndham* district court litigation and *LabMD* administrative litigation discussed below.

Other FTC Activity & Guidance

Both FTC and Solove and Hartzog point to the various forms of guidance issued by the FTC, claiming they, in combination with the FTC's cases, provide what amounts to a common law. It is certainly true that the FTC has, since 2010, used reports to make policy. But that does not make them common law-like. Indeed, these reports differ fundamentally from the antitrust guidelines continually updated by the FTC and DOJ: The FTC's reports recommend best practices while the antitrust guidelines distill past common law into articulable legal doctrines.

FTC v. HTC (2013)

In May 2013, the FTC reached a settlement with HTC, the maker of Android smartphones and other mobile devices.[148] HTC's devices came with several HTC apps pre-installed. The Android operating system's security framework generally requires that users consent when one application attempts to access sensitive information or device functionality controlled by another. But HTC's pre-installed apps allowed third-party apps access such information or functionality without user permission. Thus, the Complaint alleged:

---

[146] http://www.ftc.gov/sites/default/files/documents/closing_letters/michaels-stores-inc./120706michaelsstorescltr.pdf

[147] http://abcnews.go.com/Business/ConsumerNews/debit-card-fraud-michaels-crafts-customers-info-captured/story?id=13593607

[148] http://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter

> any third-party application exploiting these vulnerabilities could command those HTC applications to access various sensitive information and sensitive device functionality on its behalf -- including enabling the device's microphone; accessing the user's GPS-based, cell-based, and WiFi-based location information; and sending text messages -- all without requesting the user's permission.
>
> HTC could have prevented this by including simple, well-documented software code - "permission check" code - in its voice recorder application to check that the third-party application had requested the necessary permission. ….
>
> Malware could exploit these vulnerabilities to, for example, surreptitiously record phone conversations or other sensitive audio, to surreptitiously track a user's physical location, and to perpetrate "toll fraud," the practice of sending text messages to premium numbers in order to charge fees to the user's phone bill.[149]

The Complaint alleged the following about substantial injury:

> Among other things, malware placed on consumers' devices without their permission could be used to record and transmit information entered into or stored on the device, including financial account numbers and related access codes or personal identification numbers, medical information, and personal information such as text messages and photos. Sensitive information exposed on the devices could be used, for example, to target spear-phishing campaigns, physically track or stalk individuals, and perpetrate fraud, resulting in costly bills to the consumer. Misuse of sensitive device functionality such as the device's audio recording feature would allow hackers to capture private details of an individual's life.[150]

The Complaint did not discuss any potential benefits from this design configuration, such as user convenience, except to say that "HTC could have implemented readily-available, low-cost measures to address these vulnerabilities." On avoidability, the Commission said only that "Consumers had little, if any, reason to know their information was at risk because of the vulnerabilities introduced by HTC."

However such an analysis might have played out in court, the case was, of course, settled. The private practitioners on whom Solove & Hartzog rely to compensate for the lack of adversarial process in the FTC's "common law" approach quickly denounced the decision. Chris Cwalina and Steven Roosa summarized their concerns:

---

[149] HTC Complaint at 3 http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf

[150] Id at 6.

> The HTC Complaint essentially announces a lower bar for noncompliance (basically a negligence standard on issues of security), formally enshrines the role of independent researchers with no affiliation with the FTC (something we've been talking about for some time now), and delves deeply into complex security areas where it has no special expertise--and which seems to fall significantly outside the FTC's delegated, consumer-centric jurisdiction from Congress—and finds violations where there has been no evidence of actual harm, compromise or loss.[151]

The complaint included an element not found in previous complaints, that among the reasons HTC's practice was unfair was that the company had:

> failed to implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents.[152]

In effect, noted Cwalina and Roosa, while the FTC had previously "outsourced… significant portions of the [Commission's] technical research and investigative function to talented private researchers… These independent researchers have now been structurally incorporated as a watchdog mechanism so as to become the eyes and ears of the FTC. Indeed, by way of the HTC decision, the FTC has put industry on notice that processes need to be in place that will ensure that the voices of independent researchers are heard as part of the cycle of software improvement and bug killing."[153]

More fundamentally, Cwalina and Roosa explained that the decision essentially announced a new *per se* standard for unfairness:

> [HTC's] engineering conduct at issue was not unethical or unscrupulous…. Instead, the FTC characterized HTC's conduct as a failure "to employ reasonable and appropriate security in the design and customization of the software on its mobile devices." In other words, there was no real conduct involving sharp marketing or sales practices, but rather an engineering mistake or mistakes, according to the FTC. In one stroke, the FTC has gone from regulating consumer transactions to policing engineering negligence.

---

[151] The FTC's HTC Action: The Most Significant FTC Case in 5 Years - See more at: http://www.hklaw.com/PrivacyBlog/The-FTCs-HTC-Action-The-Most-Significant-FTC-Case-in-5-Years-03-01-2013/#sthash.MyD1mxBZ.dpuf ,March 1, 2013 http://www.hklaw.com/PrivacyBlog/The-FTCs-HTC-Action-The-Most-Significant-FTC-Case-in-5-Years-03-01-2013/

[152] HTC Complaint at 2

[153]

> Second, as to whether HTC's conduct "caused, or was likely to cause" injury, the allegations pertain to between 12 million and 18 million devices, depending on the specific category of flaws alleged by the FTC in the HTC matter. The FTC's complaint, however, fails to recount even a single incident where the alleged failure translated into an actual exploit. There is no universe in which zero incidents over a baseline of 12 million devices translates into "likely" injury. In fact, if anything, it is compelling evidence that such exploits or compromise were "unlikely." For all practical purposes, the "caused or likely to cause" standard has vanished.
>
> Finally, because the FTC has failed to identify likely injury, one does not even get to the question of whether the potential injury would be substantial.

Thus, once again, the FTC had effected a major expansion in doctrine with no analysis or explanation whatsoever. As Cwalina and Roosa concluded, bitingly:

> In the absence of a successful judicial challenge in the intermediate terms to the FTC's new tack, it would appear that the new expanded purview of the FTC may be here to stay. And what an expansion it is.

Wyndham

After eleven years of FTC enforcement actions regarding "reasonable" data security, which *all* resulted in settlements, without a single litigation in either Federal court or even the FTC's own administrative process, Cwalina and Roosa's call for judicial review might have seemed hopelessly wistful but for the fact that, the previous summer, the FTC finally did sue Wyndham Hotels.[154]

Why did Wyndham fight back when every single other company had settled an FTC enforcement action? The exact reasons why settlement negotiations broke down may never be known, but two explanations seem likely.

First, the FTC sought to hold Wyndham Hotel & Resorts (WHR) liable for the allegedly unreasonable data security practices of its independent franchisees, even though WHR's privacy policy specifically applied only to WHR, and specifically disclaimed responsibility for franchisee's data security: "Each Franchisee collects Customer Information and uses the Information for its own purposes. We do not control the use of this Information or access to the

[154] http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation. Original complaint is available at http://www.ftc.gov/sites/default/files/documents/cases/2012/06/120626wyndamhotelscmpt.pdf; second amendment complaint is available at http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf

Information by the Franchisee and its associates."[155] This prompted the International Franchise Association to join as an amicus in defense of WHR, adding that "Holding WHR liable in the absence of control would stand basic principles of franchise liability on their head."[156]

Second, the FTC sought to impose a monetary penalty in the form of restitution or disgorgement. While the Commission did not specify an amount, its complaint alleges that Wyndham's "unreasonable" data security:

> resulted in…. the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss.[157]

The litigation has proceeded slowly, initially being filed in Arizona district court, then transferred to New Jersey.[158] After oral arguments last fall, a Federal District court in New Jersey is expected to rule imminently on Wyndham's motion to dismiss.[159] There are essentially three issues before the court.

Unfortunately, the one that has received most – in fact, nearly all – the public attention is the one least relevant to this paper: Can the FTC use Section 5 to police data security at all? Or does the fact that Congress has passed several statutes giving the FTC specific grants of authority to regulate data security in specific areas suggest that Congress did not understand Section 5 to be applicable to data security? Wyndham, most of its amici, and many of its public supporters have focused on this issue, noting that the FTC has essentially imposed the standards of the 2002 Safeguards Rule, which applies only to financial institutions under Gramm-Leach-Bliley, to every company under its jurisdiction. They rely on the Supreme Court's decision in *Brown & Williamson*.

We both filed an amicus brief with the court that specifically avoids this question.[160] Instead, we focus on two questions: First, has the FTC provided adequate guidance of what it will

---

[155] Amicus brief of International Franchise Association at 3 http://www.chamberlitigation.com/sites/default/files/cases/files/2013/IFA%20Amicus%20Brief%20in%20Support%20of%20Wyndham%20MTD%20--%20FTC%20v.%20Wyndham%20Worldwide%20Corp.%20Et%20al.%20%28U.S.%20Dist.%20Court%20for%20N.J.%29.PDF

[156] Id.

[157] Complaint at 17.

[158] Order granting transfer of venue http://www.chamberlitigation.com/sites/default/files/cases/files/2012/Order%20Granting%20Motion%20to%20Transfer%20Venue%20--%20FTC%20v.%20Wyndham.pdf

[159] Cite.

[160] http://www.chamberlitigation.com/sites/default/files/cases/files/2013/Tech%20Freedom%20Amicus%20Brief%

require through Section 5? Or should the FTC have to do more, systemically, to explain what is required?

Pleadings

In this particular case, did the FTC adequately plead a complaint on which a court can evaluate a Section 5 claim? We argue that the FTC has failed to satisfy the pleading standards set forth by the Supreme court in *Twombly* and *Iqbal* on each of the three required elements of unfairness.

First, the FTC does not clearly allege who bore the supposed $10.6 million in economic losses, a key question given the fact that U.S. consumers are not liable for credit card charges over $50 and industry practice is to reimburse *all* charges upon complaint. We note the concern raised by former FTC Chairmen Majoras and Kovacic in N-Data "that the Commission was inappropriately extending consumer protection law to sophisticated corporations."[161]

Second, on avoidability:

> The Commission "FTC fails to support the allegation that 'unreimbursed fraudulent charges' are not reasonably avoidable by consumers. In fact, consumers could do so by putting a hold on the credit card, requesting a new card number, purchasing credit monitoring services, or by notifying the card issuer of unauthorized charges. The FTC asserts that "consumers and businesses... expended time and money resolving fraudulent charges and mitigating subsequent harm" but fails to provide any facts to permit a "reasonable inference" (as required by Iqbal) that these costs were unreasonable. Indeed, the only reasonable inference that can be drawn from the FTC's factual allegations is that any effort spent avoiding injury is not "reasonable"—a claim which would negate one prong of analysis required."

Third, on benefits and trade-offs:

> It would be easy to assert that allegedly shoddy data security has no benefits, but this misses the point: This prong of unfairness requires the FTC to weigh the benefits of the legal burdens it would impose with their costs. However great the benefits of data security, they are not absolute—and still subject to tradeoffs. The FTC ultimately bears the burden of establishing not only a substantial injury, but also that possible benefits to consumers from the practice at issue do not

---

20in%20Support%20of%20Wyndham%20MTD%20--%20FTC%20v.%20Wyndham%20Worldwide%20Corp.%20Et%20al.%20%28U.S.%20Dist.%20Court%20for%20N.J.%29.PDF

[161] Majoras Dissent, N-Data, available at http://www.ftc.gov/os/caselist/0510094/080122majoras.pdf ("[T]he FTC has used its authority under Section 5 to protect small businesses against unfair acts and practices.... There is a clear qualitative difference between these entities and...computer manufacturers")

> outweigh that injury. It would be easy to assert that allegedly shoddy data security has no benefits, but this misses the point: This prong of unfairness requires the FTC to weigh the benefits of the legal burdens it would impose with their costs. However great the benefits of data security, they are not absolute—and still subject to tradeoffs

Further, we argue the FTC should be held to the heightened pleading standard of Federal Rule of Civil Procedure 9(b).

What's Next on Wyndham?

As expected from oral arguments, the district court denied Wyndham's motion to dismiss.[162] Wyndham and its amici (other than the brief I co-authored) had primarily emphasized their argument under *Brown & Williamson*, that the FTC lacked statutory authority to regulate data security at all.[163] The court decided, unsurprisingly, that the FTC does indeed have plenary authority to regulate consumer protection under Section 5(a), including data security. This is consistent with the Unfairness Policy Statement – but it is also why the *quality* of the FTC's process is so important. As the Policy Statement said:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review,6 in the expectation that the underlying criteria would evolve and develop over time. As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion.'"[164]

In other words, Congress expected the FTC to develop the meaning of unfairness (and, by extension, deception, as well, since deception is a subset of unfairness) – but the Commission has not done so. Unfortunately, the district court judge decided the motion to dismiss narrowly on the second question raised by Wyndham: Must the FTC use formal rulemaking under Magnuson-Moss in order to provide fair notice adequate to satisfy constitutional principles of due process? The court's decision cites Wyndham's motion on this point and quotes from Gerry Stegmaier's article on point,[165] but completely misses the point of the article: Formal regulation

---

[162] [cite]

[163] [Cite to Wyndham brief & Brown & Williamson]

[164] [cite]

[165] [Cite]

may be the *best* way to provide fair notice, but it is not the *only* way.[166] The question, really, is about the quality of the FTC's decisions.

The decision does not explicitly articulate a disturbing argument raised at oral arguments on the motion to dismiss, but to some extent, seems to endorse it—the notion that Fair Notice is a subjective standard (what Wyndham's employees knew or thought about the FTC's expectations) rather than an objective one (what a reasonable person could have divined based on guidance from the FTC). This would turn the Fair Notice doctrine on its head. Denying Wyndham's motion to dismiss allows the FTC can get more discovery about Wyndham's knowledge, such as by subpoenaing internal emails about what the company thought the FTC might require on data security.

But whatever the rationale, delaying resolution of Fair Notice question until the motion for summary judgment will effectively neuter Fair Notice as a potential source of analytical discipline that could improve the FTC's "common law" approach in two senses. First, if a defendant cannot make a Fair Notice argument until the Motion for Summary Judgment, it will have to incur the cost of discovery and endure the delay of a year or more simply to confront this key question. Given that it took a decade before a single company was willing to refuse to settle a data security action with the FTC, and that their primary argument (*Brown & Williamson*) is likely to lose, making it significantly more expensive for them to get to their second, stronger argument will significantly deter future litigation – perhaps completely. Thus, a subjective standard for Fair Notice could make an *actual* common law of data security impossible.

Removing Fair Notice as a realistic check on the FTC's discretion also removes whatever incentive the FTC might have had to plead its complaints, or explain its settlements, with a level of rigor beyond the minimal standard of a majority of Commissioners feel is required to show that they have "reason to believe" a Section 5 violation might have occurred, and that an investigation (or settlement) would be in the public interest. While it is possible that Fair Notice would only improve the quality of complaints in cases where the FTC believes a settlement is unlikely (the FTC often foes not file the complaint until it has already negotiated a settlement), or of those settlements that are more highly contested, even this would help to improve the analytical quality of the FTC's "common law" of unadjudicated complaints and consent agreements. Indeed, what matters is not that *every* case is better explained, but that the FTC better explains major doctrinal shifts. Even if the defendant in such a case is unwilling to litigate, regardless of the availability of a Fair Notice defense, the credible threat of a Fair Notice challenge to a subsequent case derived from that "precedent" may give the FTC a greater incentive to better explain that initial doctrinal shift so as to better protect its future "common law" decisions.

[166] [Cite]

Even if a Fair Notice inquiry were, in some sense, subjective, the FTC is not a normal plaintiff. While standard plaintiffs can only get discovery by first surviving a motion to dismiss, the FTC has broad subpoena power of its own (CIDs), which allows it to develop a rich factual record before ever suing. Thus, even under a subjective standard for Fair Notice, the FTC should bear the burden of showing why it had been unable to get the discovery it respond to Wyndham's fair notice defense.

The final issue our brief focused on, whether the FTC's pleadings are adequate, has received almost no attention in the discourse around the Wyndham case, and seemed an afterthought at oral arguments. Obviously, such arguments will matter little to a company like Wyndham, since even if the FTC loses on this ground, the FTC will simply refile their complaint. (By contrast, a victory on either of the other two issues would likely make further prosecution of Wyndham impossible.)

But here, once again, emerges the divergence between the interests of a private party and the public at large we mentioned at the outset.[167] A higher pleading standard could significantly improve the jurisprudential quality of the FTC's "common law" even if no further litigation occurs. It is, of course, possible that nothing would change, that the FTC would stick to its current "reason to believe" and "public interest" standard for the issuance of complaints and, if companies continue to be unwilling to litigate, the FTC could insist that, because these complaints are not actually Federal court pleadings, nothing has changed. But clearer Federal pleading standards would at least give private parties more leverage in settlement negotiations with the FTC, if only to require more rigorous complaints. Perhaps more importantly, they might change the dynamic among Commissioners. Suppose, for example, that Commissioner Wright had, in *Apple*, been able to frame his arguments in terms of satisfying federal pleading standards. He might well be able to convince other Commissioners that, as a matter of best practice, the FTC's complaints should more closely resemble what they would be required to file if they actually did litigate, at least regarding significant doctrinal shifts. It is also possible that such a decision would prompt greater Congressional attention to the difference between the real common law and what the FTC calls its "common law."

FTC v. LabMD (2013)

The FTC's enforcement action against LabMD, a small Georgia cancer diagnostics lab, has received less attention than *Wyndham* but is, in many ways more important. Where *Wyndham* involved essentially the same fact pattern as most of the FTC's prior data security enforcement actions (with the important twists of franchisee liability and the FTC's insistence on a monetary penalty), LabMD involved two different fact patterns. First, and most importantly, a third party company, Tiversa, was able to obtain a single billing file containing patient billing records from a LabMD computer on which a LabMD employee had allegedly installed LimeWire, the peer-to-peer filesharing program. Tiversa used a special tool, funded by a federal research grant, to build what it called the "Google of P2P" networks to find files that contained certain kinds of

[167] See supra ___

information. Second, long after the FTC started its investigation of this issue, it obtained print-outs of LabMD billing records found by a police department in a bust of a criminal fraud operation.

Thus, the most important doctrinal questions in LabMD are: Did LabMD take reasonable precautions against the P2P vulnerability, given its small size? Was that vulnerability reasonably foreseeable at the time? And, more generally, is the FTC applying a *per se* standard, as Cwalina and Roosa warned regarding HTC?

Unlike the Wyndham litigation, which the FTC filed in Federal court, the FTC elected to prosecute LabMD using its internal administrative process – the first time this has *ever* happened in a data security case and the first time for any unfairness case since Orkin in 1988. LabMD has shut down operations, blaming the FTC investigation,[168] but it has not declared bankruptcy, so it appears the litigation will continue, and with a public interest firm representing the company, LabMD's CEO Mike Daugherty appears determined to press on.[169]

Commissioner Wright wrote the Commission's order denying LabMD's motion to dismiss, first rejecting the *Brown & Williamson* argument made by Wyndham in Federal district court. Commissioner Wright's ten page discussion of this issue will likely be repeated in significant part by the federal district court in *Wyndham*.[170]

Wright began by quoting from Commissioner Swindle's 2004 testimony on data security, which endorsed both deception and unfairness as bases for data security enforcement actions in principle, and noted, as quoted by Commissioner Wright: "information security is an ongoing process of assessing risks and vulnerabilities: no one static standard can assure appropriate security, as security threats and technology constantly evolve."[171] Wright continued,

> Such complex questions relating to data security practices in an online environment are particularly well-suited to case-by-case development in administrative adjudications or enforcement proceedings, given the difficulty of drafting generally applicable regulations that fully anticipate the concerns that arise over emerging business arrangements in this rapidly changing area

Wright then quoted *Chenery* at length about

---

[168] [cite]

[169] [cite]

[170] Joshua D. Wright, Commissioner Fed. Trade Comm'n, Order Denying Respondent LabMD's Motion to Dismiss In the Matter of LabMD, Inc., FTC File No. 112-9357, at 3-14 (Jan. 16, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf.

[171] Id at 14 (quoting Swindle Testimony, supra note 143 at 3).

> [P]roblems may arise . . . [that] must be solved despite the absence of a relevant general rule. Or the agency may not have had sufficient experience with a particular problem to warrant rigidifying its tentative judgment into a hard and fast rule. Or the problem may be so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule. In those situations, the agency must retain power to deal with the problems on a case-to-case basis if the administrative process is to be effective. There is thus a very definite place for the case-by-case evolution of statutory standards. And the choice made between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency.[172]

Wright concluded:

> The Commission has enforced Section 5's prohibition of "unfair . . . acts or practices" primarily through case-by-case adjudication and litigation from the time the statute was enacted. Indeed, numerous recent cases have condemned conduct that facilitated identity theft or involved misuse of confidential consumer information as unlawful "unfair . . . acts or practices," **although the practices were unprecedented and not covered by any preexisting rules**. Thus, even though the Commission had never promulgated any regulations governing the creation of online checks or bank drafts without adequate verification procedures, the Ninth Circuit, in *Neovi*, easily affirmed both the district court's holding that the defendants had committed "unfair acts or practices," 604 F.3d at 1155-58, and its requirement that the defendants disgorge all revenue from the unlawful conduct. *Id.* at 1159-60. Similarly, despite the absence of any regulation prohibiting online data brokers from gathering and selling consumers' confidential information gleaned from telephone records, the Tenth Circuit affirmed a district court decision finding that the defendants' conduct constituted "unfair acts and practices" and imposing an equitable disgorgement remedy. *See generally Accusearch*, 570 F.3d 1187.[173]

Wright concludes a discussion of four appellate cases by summarizing *Shell Oil Co. v. FERC*, 707 F.2d 230, 235-36 (5th Cir. 1983) as follows: "parties in administrative adjudicatory proceedings are not denied due process even when agencies establish new, binding standards of general application in such proceedings, so long as affected parties are given meaningful opportunities to address the factual predicates for imposing liability."[174] But this begs the important question for our purposes: what if defendants systemically fail to take advantage of those "opportunities" by challenging the FTC to litigate, either in court or in the FTC's administrative

---

[172] Motion denying LabMD order at 15, quoting *Chenery*, 332 U.S. at 202-03..

[173] Id at 15.

[174] Id at 16.

adjudicatory process? Indeed, how "meaningful" is their opportunity to litigate if the basic legal principles asserted by the FTC have been developed outside the adjudicatory process?

Wright argues that economic regulation is subject to a lower vagueness standard than is regulation of speech, citing *Trans Union Corp. v. FTC*, 245 F.3d 809, 817 (D.C. Cir. 2001) (quoting *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498-99 (1982)).[175] He does not respond to detailed scholarly arguments made on Fair Notice grounds by Gerry Stegmaier, about the adequacy of *how* the FTC uses its adjudicatory process as an alternative, within its discretion under *Chenery*, to formal rulemaking:

> An agency can expect an entity it regulates to comply with policy made through formal adjudication. However, requiring entities to review allegations contained in unfiled complaints with attendant settlement orders begs the question as to whether such actions are suitably authoritative to address fundamental fairness concerns.[176]

Wright concludes by embracing the "common law" analogy championed by Commissioner Brill and Chairman Ramirez:

> the three-part statutory standard governing whether an act or practice is "unfair," set forth in Section 5(n), should dispel LabMD's concern about whether the statutory prohibition of "unfair . . . acts or practices" is sufficient to give fair notice of what conduct is prohibited. In enacting Section 5(n), Congress endorsed the Commission's conclusion that "the unfairness standard is the result of an evolutionary process . . . . [that] must be arrived at by . . . a gradual process of judicial inclusion and exclusion." *Policy Statement on Unfairness*, 104 F.T.C. at 1072. This is analogous to the manner in which courts in our common-law system routinely develop or refine the rules of tort or contract law when applying established precedents to new factual situations. As the Supreme Court has recognized, "[b]roadly worded constitutional and statutory provisions necessarily have been given concrete meaning and application by a process of case-by-case judicial decision in the common-law tradition." *Northwest Airlines, Inc. v. Transp. Workers Union of Am*., 451 U.S. 77, 95 (1981). [177]

Wright concludes:

---

[175] Id at 16.

[176] Gerard M. Stegmaier and Wendell Bartnick, *Another Round In The Chamber: Ftc Data Security Requirements And The Fair Notice Doctrine*,

*

[177] Id at 16-17.

> LabMD's due process claim is particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care, and the contexts in which they make those fact-specific judgments are as varied and fast-changing as the world of commerce and technology itself. The imposition of such tort liability under the common law of 50 states raises the same types of "predictability" issues that LabMD raises here in connection with the imposition of liability under the standards set forth in Section 5(n) of the FTC Act. In addition, when factfinders in the tort context find that corporate defendants have violated an unwritten rule of conduct, they – unlike the FTC – can normally impose compensatory and even punitive damages. Even so, it is well-established that the common law of negligence does not violate due process simply because the standards of care are uncodified. There is similarly no basis to conclude that the FTC's application of the Section 5(n) cost-benefit analysis violates due process, particularly where, as here, the complaint does not even seek to impose damages, let alone retrospective penalties.

What does this mean? Is Commissioner Wright signing off on the FTC's approach, as Commissioner Swindle seemed to do in his last year at the Commission? To a degree, yes. But it is important to keep in mind that this was merely a motion to dismiss, not an adjudication of the merits of the case. Indeed, Wright's passing reference to "Section 5(n) cost-benefit analysis" may suggest that he expects the Commission to perform something like the kind of rigorous analysis he outlined in his *Apple* dissent. In other words, denying the Motion to Dismiss in no way precludes him from insisting that any Commission order or settlement should more rigorously assess the component elements of unfairness. (Both of the underlying issues here do not seem to present a real question of fact as to reasonable avoidability, so it makes sense that Wright would refer only to "cost-benefit analysis.") Thus, Wright may once again part way from the majority as to *how* the FTC goes about its "common law" approach, even if he agrees that, in principle, it could be a sound one.