Prepared Statement of

Gerard M. Stegmaier
Partner, Goodwin Procter LLP
Adjunct Professor, George Mason University School of Law

"The Federal Trade Commission and its Section 5 Authority: Prosecutor, Judge, and Jury"

Before the

Committee on Oversight & Government Reform
United States House of Representatives

Washington, D.C.
July 24, 2014

Mr. Chairman Issa, Ranking Member Cummings, and Members of the Subcommittee, my name is Gerry Stegmaier, and I am a partner at Goodwin Procter LLP and an adjunct professor at George Mason University School of Law, where I created one of the first information privacy law courses and have taught courses relating to privacy, consumer protection, and constitutional law for the last 13 years. I regularly appear before the Federal Trade Commission and state attorneys general, and I assist businesses with all aspects of their privacy and information governance concerns. I appreciate the opportunity to appear before you today to talk about the Federal Trade Commission's data security enforcement efforts under Section 5 of the Federal Trade Commission Act.[1]

INTRODUCTION

In 2013, there were 63,437 reported security incidents and 1,367 confirmed data breaches affecting more than 44 million data records across the globe according to Verizon's 2014 Data Breach Investigation Report.[2] Most data breaches involve malicious criminal activity stemming from outsiders.

While entities have business incentives to protect the information they collect, there is no single broad federal law requiring data security. Instead, the law has focused on criminalizing unauthorized access. This is not surprising since the law generally favors open and broad accessibility of information. Congress has limited its data-security legislation to certain industries, such as finance and healthcare, where public debate led to a consensus that increased information protection legislation was required. Generally, in the United States, data stewardship

---

[1] The views contained in this testimony solely represent the views of myself in my individual and private capacity and are not necessarily the views of my firm, our clients, or any particular institution with whom I may be affiliated.

[2] *2014 Data Breach Investigations Report*, VERIZON, 11, *http://www.verizonenterprise.com/DBIR/2014/* (last visited July 21, 2014).

is encouraged primarily by state-enacted breach notification requirements.[3]

Over the last decade, the FTC has begun requiring reasonable data security for entities not covered by existing, industry-specific federal regulations. The FTC routinely investigates publicly reported data-related incidents and has brought more than 40 data-security cases since 2000.[4] The FTC has become increasingly aggressive, as demonstrated by an FTC consent order with HTC America after the company's mobile security vulnerabilities allegedly *potentially* exposed sensitive information, even though no *actual* data compromise was alleged.

The FTC bases its authority over data security on § 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[5] Usually, the FTC makes a deceptive practices claim when an entity experiences a data breach after publishing statements that it secures data.[6] Less frequently, the FTC alleges unfair practices in data-security cases.[7] However, § 5 does not mention data security, which begs a practical question: Because the Constitution requires that entities receive fair notice to reasonably understand what behavior complies with the law, does the investigation and prosecution of entities under § 5 in data-security cases violate entities' constitutional rights to fair notice? And. if so, how might these due process concerns be better addressed?

While the Fair Notice Doctrine began in the context of criminal defense, in 1968 the U. Court of Appeals for the District of Columbia Circuit acknowledged the doctrine's applicability

---

[3] Notably, some states, such as California, have data-security requirements. *E.g.*, CAL. CIV. CODE § 1798.81.5(b) (West 2006) ("A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.").

[4] *See* Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 13, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-CV-01887-ES-SCM (D. N.J. June 17, 2013) [hereinafter Wyndham FTC Response].

[5] 15 U.S.C. § 45 (a)(1) (2006).

[6] Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 7, *FTC v. Wyndham Worldwide Corp.*, No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 9, 2012).

[7] *Id.* (stating that seventeen of the thirty-six cases brought under the FTC Act alleged unfair practices).

in the civil administrative context.[8] The court observed, "Where the regulation is not sufficiently clear to warn a party about what is expected of it—an agency may not deprive a party of property by imposing civil or criminal liability."[9]

The fair notice doctrine is not a trivial, academic legal theory with little bearing on the practice of law. On the contrary, given the FTC's broad discretion under § 5 of the FTC Act, the FTC's aggressive enforcement stance in the data-security context, and the agency's reluctance to use its existing rulemaking authority to clarify its data-security expectations, the doctrine is directly relevant to the current regulatory climate.[10] Although the FTC has undertaken significant efforts to develop and improve notice of its interpretation of § 5, the nature, format, and content of the agency's data security-related pronouncements raise equitable considerations that create serious due process concerns.[11]

FAIR NOTICE DOCTRINE

WHAT IS THE FAIR NOTICE DOCTRINE?

The fair notice doctrine requires that entities be able to reasonably understand whether their behavior complies with the law. If an entity acting in good faith cannot identify with "ascertainable certainty" the standards to which an agency expects it to conform, the agency has not provided fair notice.[12] An agency using enforcement conduct, rather than less adversarial methods, to define the contours of its broad discretion likely raises greater due process

---

[8] *Radio Athens, Inc. v. FCC*, 401 F.2d 398, 404 (D.C. Cir. 1968).
[9] *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1328-29 (D.C. Cir. 1995).
[10] Fair notice is particularly important when courts defer to an agency's interpretation of the scope of its jurisdictional authority. When agencies may define the breadth of their authority under broadly-worded statutes, fair notice may be one of few constraints on arbitrary and capricious agency action. For example, in *City of Arlington v. FCC*, the Supreme Court reviewed the FCC's assertion of jurisdiction under the Communications Act over applications for wireless facilities. The Supreme Court concluded that a court should defer to any agency's interpretations of the statute that it enforces, even those regarding the extent of the agency's authority. *City of Arlington, Texas v. FCC*, 596 U.S. ___, 133 S. Ct. 1863 (2013).
[11] In its response to Wyndham's motion to dismiss, the FTC stated, "unreasonable data security practices are unfair." *See* Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 7, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-CV-01887-ES-SCM (D. N.J June 17, 2013). The FTC argues that Wyndham has notice from government and industry sources about what security practices are reasonable.
[12] *Gen. Elec.*, 53 F.3d at 1329 (citing *Diamond Roofing Co. v. OSHRC*, 528 F.2d 645, 649 (5th Cir. 1976)).

concerns.[13] Due process protections, like those provided by the fair notice doctrine, increase in importance in these circumstances. A defendant may raise the fair notice defense to defend itself against agency enforcement when it feels it has not received proper notice.[14]

DISTINCTION BETWEEN *CHEVRON* DEFERENCE AND THE FAIR NOTICE DOCTRINE

The fair notice doctrine can serve as an effective defense even when a statute passes *Chevron* deference. *Chevron* deference is a powerful legal doctrine based on the assumption that federal agencies are experts on the statutes they enforce.[15] Under *Chevron*, courts defer to agencies' reasonable interpretations of the statutes they enforce when such statutes are ambiguous.[16] However, if an agency interpretation is unpublished or unclear, entities can argue that an agency should not hold them accountable for noncompliance under the fair notice doctrine and if such an argument prevails, the court will dismiss the claims stemming from that interpretation, or lack thereof.

THE FAIR NOTICE TEST AS APPLIED BY THE D.C. CIRCUIT

The fair notice doctrine is a creature of judicial creation not yet reviewed or bounded by

---

[13] *See e.g.*, *Martin v. OSHRC*, 499 U.S. 144, 158 (1991) (citing *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 295 (1974)) ("[T]he decision [by an agency] to use a citation as the initial means for announcing a particular interpretation may bear on the adequacy of notice to regulated parties.").

[14] *See* Kenneth K. Kilbert & Christian J. Helbling, *Interpreting Regulations in Environmental Enforcement Cases: Where Agency Deference and Fair Notice Collide*, 17 VA. ENVTL. L.J. 449, 454 (1998) ("The fair notice principle mandates that persons may not be punished for failing to comply with a law of which they could not have known."); Albert C. Lin, *Refining Fair Notice Doctrine: What Notice Is Required of Civil Regulations?*, 55 BAYLOR L. REV. 991, 998 (2003) ("[D]ue process requires . . . that parties subject to administrative sanctions are entitled to fair notice because civil penalties result in a deprivation of property . . . ."); John F. Manning, *Constitutional Structure and Judicial Deference to Agency Interpretations of Agency Rules*, 96 COLUM. L. REV. 612, 669-70 (1996) ("[I]t is arbitrary and capricious for the government to deny benefits based on noncompliance with standards that a putative beneficiary could not reasonably have anticipated."); Jeremy Waldron, *Vagueness in Law and Language: Some Philosophical Issues*, 82 CALIF. L. REV. 509, 538 (1994) (describing the unfairness of imposing vague legal requirements); Jason Nichols, Note, *"Sorry! What the Regulation* Really *Means Is...*": *Administrative Agencies' Ability to Alter an Existing Regulatory Landscape Through Reinterpretation of Rules*, 80 TEX. L. REV. 953, 964 (2002) ("Armed with knowledge of the bounds of acceptable action, people will be better able to plan their actions and will know when the government unjustly trounces upon their liberties.").

[15] *Gen. Elec.*, 53 F.3d at 1327 (citing *Chevron, U.S.A., Inc. v. Natural Res. Def. Council*, 467 U.S. 837, 864-66 (1984)). For more information on *Chevron* deference, *see* Kristine Cordier Karnezis, Annotation, *Construction and Application of "Chevron Deference" to Administrative Action by United States Supreme Court*, 3 A.L.R. Fed. 2d 25, 39 (2005); 2 AM. JUR. 2d *Administrative Law* § 77 (2002).

[16] *Chevron, U.S.A., Inc. v. Natural Res. Def. Council*, 467 U.S. 837, 864-66 (1984); *Gen. Elec.*, 53 F.3d at 1327.

the Supreme Court. The D.C. Circuit, the federal appeals court most frequently confronted with important questions of administrative law, has the most developed fair notice jurisprudence.

"Ascertainable Certainty": The D.C. Circuit's Test

In a nutshell, fair notice requires that a party be able to determine an agency's expectations with "ascertainable certainty" in order to satisfy due process requirements. Fair notice exists when "a regulated party acting in good faith would be able to identify, with 'ascertainable certainty,' the standards with which the agency expects parties to conform."[17] "The regulations and other public statements issued by the agency"[18] should provide this ascertainable certainty.

What is "Ascertainable Certainty"?

The words "ascertainable certainty" are not particularly clear; four factors have been identified to apply the standard by the D.C. Circuit:

1. ***Does the Plain Text of the Law Provide Notice, and Is the Regulated Entity's Interpretation Plausible?***

The D.C. Circuit has held that the most important factor for a successful fair notice defense is whether a careful reading of the law's plain language provides the necessary notice of the law's meaning.[19] "[W]here the regulation is not sufficiently clear to warn a party about what is expected of it"[20] the fair notice doctrine protects a party from government sanction. The language of the regulation provides proper notice only if it is "reasonably comprehensible to people of good faith."[21] Where the law is silent or ambiguous and multiple interpretations exist,

---

[17] *Gen. Elec.*, 53 F.3d at 1329 (citing *Diamond Roofing*, 528 F.2d at 649).
[18] *Id.* (citing *Diamond Roofing*, 528 F.2d at 649).
[19] *See McElroy Elecs. Corp. v. FCC*, 990 F.2d 1351, 1353, 1362 (D.C. Cir. 1993).
[20] *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1328 (D.C. Cir. 1995).
[21] *Id.* at 1330-31 (quoting *McElroy Elecs.*, 990 F.2d at 1358).

the D.C. Circuit has applied the fair notice doctrine to protect parties from government sanctions.

2. Do "Authoritative" Pre-Enforcement Efforts by the Agency, Such as Public Statements, Provide Adequate Notice?

Courts will determine whether the conduct of the agency ensures adequate notice by reviewing the agency's public statements and actions, such as notices published in the Federal Register,[22] adjudicatory opinions,[23] previous citations,[24] and policy statements. To my knowledge, the D.C. Circuit has not analyzed whether a single-party consent decree or settlement with an agency constitutes a reviewable and authoritative interpretive document as part of the "ascertainable certainty" test.

Moreover, to meet fair notice requirements, agency guidance must be "authoritative" and originate from the agency as a whole.[25] Statements from some other source, like the opinion of agency staff or even a single commissioner who may not be speaking for the entire agency, are insufficient.[26] A court would need to determine whether an agency's public statements, such as published complaints, consent orders, and guidance came from the agency as a whole. If they did not, a court should not consider them as a source of notice. Regulated entities should be able to clearly determine which statements identify the law's requirements, and which do not. By limiting the authoritative source to agencies as a whole, courts relieve regulated entities from

---

[22] *See Darrell Andrews Trucking, Inc. v. FMCSA*, 296 F.3d 1120, 1130-32 (D.C. Cir. 2002) (concluding that the formal regulatory guidance and notice of proposed rulemaking published in the Federal Register were self-contradictory); *Chrysler Corp.*, 158 F.3d at 1356 (reviewing the Federal Register notice discussing the rule and concluding that the notice was silent on the matter).

[23] *Darrell Andrews Trucking*, 296 F.3d at 1130-32 (concluding that the agency's adjudicatory opinion in a prior case gave a "crystal clear" interpretation of the regulation).

[24] *Id.* (finding that notice was provided when the agency had previously cited the defendant for regulation violations).

[25] *Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 157 (D.C. Cir. 1986) (Scalia, J.) (holding that notice of a violation given by a non-agency safety inspector did not provide sufficient notice, because it was "not an authoritative interpretation of the regulation"); *see also United States v. Hoechst Celanese Corp.*, 128 F.3d 216, 230 (4th Cir. 1997).

[26] *Gates & Fox Co.*, 790 F.2d at 157 (D.C. Cir. 1986) (Scalia, J.) (holding that notice of a violation given by a non-agency safety inspector did not provide sufficient notice, because it was "not an authoritative interpretation of the regulation"); *see also United States v. Hoechst Celanese Corp.*, 128 F.3d 216, 228, 230 (4th Cir. 1997) (holding fair notice only occurs if the agency's authoritative interpretation is provided to the entity), *cert. denied*, 524 U.S. 952 (1998).

having to parse the statements of agency staff or individual commissioners to determine what the law is.[27]

3. Did the Agency Inconsistently Interpret the Law or Inconsistently Apply Its Interpretation?

A fair notice inquiry will look for an agency's conflicting interpretations of the law, *i.e.*, published inconsistent documentation,[28] provided inconsistent advice to entities,[29] or otherwise acted inconsistently.[30] When an agency provided no notice at all, courts would likely exclude this factor.

4. Imposition of a Serious Penalty

Finally, the regulation must be sufficiently clear to warn a party of what is expected of it, otherwise, an "agency may not deprive a party of property by imposing civil or criminal liability."[31] The D.C. Circuit seems to view this requirement broadly. According to the court, due

---

[27] In the litigation context, the FTC also has not clearly stated what features of its consent orders are legal requirements. The FTC states that certain data security activities must be *evaluated*, but it does not state that the activities must be implemented. Wyndham FTC Response, *supra* n. 4, at 19 ("Although every situation is different, the consent orders in these matters provide industry, including Wyndham, with notice of different features of data security that must be evaluated in order to maintain a reasonable data security program.").

[28] *See Darrell Andrews Trucking, Inc.*, 296 F.3d at 1130 (stating that the "self-contradictory 'clarifying' utterances" in an agency's formal guidance "could have left [an entity] confused about what was required of it"); *Chrysler Corp.*, 158 F.3d at 1356 (concluding a prior schematic illustrating testing procedures conflicted with the EPA's current interpretation of the testing standard and stating, "[A]n agency is hard pressed to show fair notice when the agency itself has taken action in the past that conflicts with its current interpretation of a regulation."); *Satellite Broad. Co. v. FCC*, 824 F.2d 1, 2 (D.C. Cir. 1987) (finding other sections of the agency's rules "baffling and inconsistent").

[29] *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1332 (D.C. Cir. 1995) (finding that different divisions of the agency disagreed about the meaning of the applicable regulations); *Rollin Envtl. Servs. Inc. v. EPA*, 937 F.2d 649, 653-54 (D.C. Cir. 1991) (finding that agency officials in different regions interpreted the regulation differently and gave conflicting advice to regulated entities); *Gates & Fox*, 790 F.2d at 155 (noting evidence showing that the agency's review board could not agree on the interpretation of the underlying regulation).

[30] *McElroy Elecs.Corp. v. FCC*, 990 F.2d 1351, 1362-63 (D.C. Cir. 1993) (finding that the FCC had "misinterpreted" its own order by telling the defendant it would accept the licensing applications if they were filed, accepting the applications initially, and subsequently rejecting the applications as improperly filed); *Radio Athens, Inc. v. FCC*, 401 F.2d 398, 403 (D.C. Cir. 1968) (noting that five FCC decisions showed that the agency used a different licensing rejection process prior to the process it used to reject the application in the case at hand).

[31] *Gen. Elec.*, 53 F.3d at 1328-29; *see also Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 156 (D.C. Cir. 1986) (Scalia, J.) ("If a violation of a regulation subjects private parties to criminal or civil sanctions, a regulation cannot be construed to mean what an agency intended but did not adequately express[.]" (quoting *Diamond Roofing Co. v. OSHRC*, 528 F.2d 645, 649 (5th Cir. 1976)).

process requires that parties receive fair notice before the government may deprive them of property, such as through the imposition of a fine,[32] the denial of a license application,[33] or by requiring an entity to take costly action, such as a product recall.[34] The D.C. Circuit's "ascertainable certainty" test provides a useful tool to analyze current FTC activities in the area of information security and highlight challenges and complications to the agency's exercise of its § 5 authority.

THE FTC ACT'S PROHIBITION OF "UNFAIR ACTS OR PRACTICES"

In § 5 of the FTC Act, Congress gave broad powers to the FTC to protect consumers from deceptive and unfair trade practices. The FTC has begun using its "unfairness" authority to investigate and punish what it believes are companies' faulty data-security practices. This authority needs to be balanced with the due process rights of entities by memorializing the fair notice doctrine in statute.

THE FTC'S "UNFAIRNESS" AUTHORITY

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[35] An unfair act or practice is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[36] To be a substantial injury, it must be significant in magnitude and actual (i.e., the harm has occurred or is imminently threatened).[37]

---

[32] *Gen. Elec.*, 53 F.3d at 1328 (concluding that because the agency action resulted in a violation and imposed a fine, fair notice must be reviewed); *Rollins*, 937 F.2d at 653-54 (ruling that a $25,000 fine would be an "imposition of a serious penalty").
[33] *McElroy Elecs.*, 990 F.2d at 1363; *Satellite Broad.*, 824 F.2d at 2; *Radio Athens*, 401 F.2d at 403.
[34] *Chrysler Corp.*, 158 F.3d at 1355 (ruling that a vehicle recall would have required expenditure of significant amounts of money depriving Chrysler of property).
[35] 15 U.S.C. § 45 (a)(1) (2006).
[36] *Id.* § 45 (n).
[37] Letter from the FTC to Hon. Wendell H. Ford and Hon. John C. Danforth, Committee on Commerce, Science and

Consumer injury may involve either causing very severe harm to a small number of people or "a small harm to a large number of people."[38] The two forms of injury that typically qualify under the "unfairness" test are economic harm and harm to health or safety.[39]

The FTC's Use of "Unfairness" Authority

The FTC may use its unfairness authority when the alleged unfair practices and harm to consumers are clear. The FTC has used the law's breadth to regulate a wide range of business practices, from the production of farm equipment[40] to telephone bill processing.[41] However, what constitutes "unfair" data-security practices is far from clear. The amount of data security necessary to make an entity's practice "fair" under § 5 is unknown. Traditionally, the FTC has exercised its unfairness authority when there is obvious and substantial consumer harm, i.e. burn injuries and stolen money. In the vast majority of data-security cases, however, the harm may be more difficult to determine and may not be "substantial." In fact, courts have wrestled with whether the loss of personal information constitutes a cognizable harm to consumers without evidence of actual damages.[42] Actual damages resulting from a particular data-loss incident can be difficult to ascertain.[43] For example, even when a breach compromises credit card numbers,

---

Transportation, U.S. Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), *reprinted in In re Int'l Harvester Co.*, 104 F.T.C. 949, 1070-76 (1984).

[38] *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1157 (9th Cir. 2010).

[39] *Int'l Harvester*, 104 F.T.C. at 1086.

[40] *Id*. at 954.

[41] *FTC v. Inc21.com Corp.*, 475 F. App'x 106, 107-08 (9th Cir. 2012).

[42] In the class action context, plaintiffs have faced obstacles in meeting standing requirements when they argue that data breaches result in a cognizable harm, going so far as to claim that paying for identity theft protection services to preempt identity theft is an economic harm caused by the breach. Lower courts have gone both ways on the standing question. *Compare Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011), *Whitaker v. Health Net of California, Inc.*, No. CIV S-11-0910 KJMDAD, 2012 WL 174961, at *2 (E.D. Cal. Jan. 20, 2012), *and Low v. LinkedIn Corp.*, No. 11-CV01468-LHK, 2011 WL 5509848, at *4 (N.D. Cal. Nov. 11, 2011), *with Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010), *Lambert v. Hartman*, 517 F.3d 433, 437 (6th Cir. 2008), *and Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007). However, the Supreme Court recently enunciated a strict test for standing when plaintiffs allege a risk of future harm, stating that to confer standing, future harm must be "certainly impending," or at least pose a "substantial risk." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143, 1150 n.5 (2013). Litigants likely will cite *Clapper* in motions to dismiss in class action litigation involving data breaches for the foreseeable future.

[43] The uncertainty of consumer injury in the data-protection context, and the difficulties inherent in identifying it, are discussed in

no harm may result because credit card companies refund consumers for any fraudulent charges made to their account. Given the complexity of data security, the less-than-clear harm, and the fact that third-party criminal activity typically leads to the harm, fair notice is even more essential in the data-security context as compared to other types of alleged unfair practices.

The FTC's Section 5 Enforcement and Penalty Structure

When the FTC identifies an "unfair" practice, it may enforce § 5 against the party using the practice through an administrative process and issue a cease-and-desist order, which commonly results in a consent order.[44] Alternatively, the FTC can file a complaint in court, seeking injunctions and consumer redress against defendants through adjudication and fact finding for alleged violations of § 5.[45]

In the areas of privacy and data security, the FTC has typically followed the administrative process and entered into consent orders with defendants. The full Commission must approve consent orders, and they are subject to notice and public comment before becoming effective.[46]

Any violation of a consent order can result in civil penalties of up to $16,000 per violation,[47] and "[e]ach separate violation . . . [is] a separate offense . . . [and] each day of continuance of such failure or neglect shall be deemed a separate offense."[48] Under this violation calculus, violations and fines can accumulate quickly, and entities face potentially ruinous penalties hanging over their heads for 20 years after entering into a consent order.

---

the briefs of amici curiae in the Wyndham Case.

[44] 15 U.S.C. § 45(b)-(c), (g) (2006).

[45] 15 U.S.C. § 53(a)-(b) (2006).

[46] 16 C.F.R. § 2.34 (2012).

[47] Section 5(1) of the FTC Act, 15 U.S.C. § 45(1) (2006), as modified by Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461 (2006), and Section 1.98(c) of the FTC's Rules of Practice, 16 C.F.R. § 1.98 (c) (2012), authorizes a court to award monetary civil penalties of not more than $16,000 for each such violation of a consent order.

[48] 15 U.S.C. § 45(l).

For example, the FTC filed an action against Google for violating a consent order when Google allegedly used cookies for advertising purposes on Apple Safari users' browsers despite the language in its privacy policy.[49] The result was the FTC's largest fine ever for an order violation: $22.5 million.[50] In its complaint, the FTC alleged that each time Google made a misrepresentation to a user, Google violated the order.[51] Therefore, the FTC appears to have calculated the number of violations based on the number of people who saw the alleged misrepresentations. Considering the number of Google users, the number of people who potentially saw these alleged misrepresentations could be in the millions, and a $16,000 fine for each of a million users would result in a very large civil penalty. Given the potential seriousness of these penalties, the significance of fair notice cannot be understated.

THE FTC USES SECTION 5 OF THE FTC ACT TO INVESTIGATE AN ALLEGED LACK OF PROPER DATA-SECURITY SAFEGUARDS

The FTC Act grants the FTC both specialized rulemaking and enforcement authority under § 5, although the agency's rulemaking authority is limited.[52] The FTC's rulemaking authority, which is commonly referred to as Magnuson-Moss rulemaking,[53] includes additional requirements that are more cumbersome than the more traditional Administrative Proceedings Act (APA) process. For example, the FTC Act requires the FTC to "provide for an informal hearing" in which interested parties are entitled to present oral testimony and potentially cross-

---

[49] Order Approving Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 1-2, *United States v. Google Inc.*, No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012).
[50] *Id.* at 2.
[51] *Id.* at 7.
[52] 15 U.S.C. § 57a (a)(1)(B) ("[T]he Commission may prescribe . . . rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce . . . .").
[53] *See* Lydia B. Parnes & Carol J. Jennings, Through the Looking Glass: A Perspective on Regulatory Reform at the Federal Trade Commission, 49 ADMIN. L. REV. 989, 995 (1997).

examine witnesses.[54] Due to this potentially inefficient and time consuming process, the FTC has not used its rulemaking authority to issue rules related to data security.[55]

As with formal rulemaking, the FTC has also declined to clarify "fair" data security through formal adjudication. The FTC argues that its consent orders provide fair notice.[56] According to the FTC, it has brought more than 40 data-security enforcement actions since 2000.[57] At least seventeen of those actions alleged unfair practices.[58] However, none of the cases resulted in formal adjudications by the FTC or the courts.[59] Instead, each resulted in a settlement agreement with the respective defendants. The FTC publishes information about its enforcement activity, including the details of the complaints and consent orders,[60] in what some proponents of this approach increasingly refer to as an emerging "common law" of privacy.[61]

The FTC's settlement and consent decree-focused approach to date security consumer protection arguably creates some likelihood of potential actual notice of the agency's interpretation of § 5. The FTC's data-security-related complaints frequently use terms like "reasonable," "appropriate," "adequate," or "proper" to describe the security safeguards that the

---

[54] 15 U.S.C. § 57a(b), (c); *see also* Brief of Amici Curiae Chamber of Commerce of the United States of America, Retail Litigation Center, American Hotel & Lodging Association, and National Federal of Independent Business in Support of Defendants at 21, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-SCM (D. N.J. May 3, 2013) [hereinafter Chamber of Commerce Brief] (noting that "[b]y Congressional Design, [the agency's] rulemaking authority is more burdensome on the FTC than rulemaking authority normally provided to administrative agencies under the APA; among other restrictions, for example, the statute permits interested parties to cross-examine witnesses").

[55] Prepared Statement of the Federal Trade Commission on Data Security: Hearing Before the Subcomm. on Commerce, Mfg., and Trade of the H. Comm. on Energy and Commerce, 112th Cong. 11 (2011) (statement of Edith Ramirez, Comm'r, Federal Trade Commission) ("[E]ffective consumer protection requires that the Commission be able to promulgate rules in a more timely and efficient manner.").

[56] Wyndham FTC Response, *supra* n. 4, at 19.

[57] *Id*. at 13.

[58] *See also* Tech Freedom Brief at 4.

[59] In August 2013, the FTC filed a complaint against LabMD following an alleged data breach. The case was not resolved at the time of this writing. Press Release, Fed. Trade Comm'n, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy (Aug. 29, 2013), available at *http://www.ftc.gov/opa/2013/08/labmd.shtm.*

[60] *Id*.

[61] *See, e.g.*, Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at the 12th Annual Loyola University Chicago School of Law Antitrust Colloquium: Privacy, Consumer Protection, and Competition 1 (Apr. 27, 2012), available at *http://www.ftc.gov/speeches/brill/120427l**o**yolasymposium.pdf; see generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy* (Aug. 15, 2013), available at: *http://ssrn.com/abstract=2312913* (last visited Aug. 30, 2013) (contending that the "FTC's privacy jurisprudence is the functional equivalent to a body of common law," and examining it as such).

agency maintains are required under § 5.[62] These complaints, which form the basis of the underlying consent orders, alleged that § 5 was violated due to some combination of failing to: have an information security policy; implement system monitoring; fix known vulnerabilities; maintain firewalls and updated antivirus software; use encryption; implement intrusion detection and prevention solutions; store information only as long as necessary; and prepare for known or reasonably foreseeable attacks.[63] However, because the FTC cryptically states that the failures "taken together" violate § 5 and each complaint lists different data-security practices, these complaints do not provide an effective "data-security blueprint." The FTC's standard mode of operation is to issue non-authoritative suggested guidelines and deal with unfairness actions through settlement. Neither of these practices provide entities with reliable guidance useful in avoiding unfairness actions. Michael D. Scott, a "pioneer" in the field of high-technology law and public policy and graduate of MIT and UCLA School of Law, has criticized the FTC noting that "[t]he complaints and consent orders entered into in these cases provide limited guidance as to what a company should do (or not do) to avoid being the target of an unfairness action by the FTC if it experiences a security breach."[64]

The FTC's consent orders in data-security cases also require some specific data-security practices of those companies whose practices are now supervised directly by the agency,[65] such

---

[62] In its response to Wyndham's motion to dismiss, the FTC reiterated, "unreasonable data security practices are unfair." *See* Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 17, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-CV-01887-ES-SCM (D. N.J June 17, 2013). Some commentators may suggest that there is no security standard because good security varies based on too many factors. This article agrees with that conclusion, but the FTC does not. The FTC seems to be using a security standard when it chooses whether to file complaints against entities for their "unreasonable" security practices. The FTC has issued "guidance" that looks like a standard, but the agency has not communicated that it is the law. Communicating the legal standard to entities will help entities understand what "reasonable" security looks like before they receive the FTC complaint.

[63] Complaint at 2-5, *In re* ACRAnet, Inc., No. C-4331 (Aug. 17, 2011); Complaint at 2-3, *In re* Ceridian Corp, No. C-4325 (June 8, 2011); Complaint at 2-3, *In re* BJ's Wholesale Club, Inc., No. C-4148 (Sept. 20, 2005).

[64] Michael D. Scott, *FTC, the Unfairness Doctrine, and Data Security Breach Litigation*, 60 ADMIN. L. REV. 183 (2008).

[65] *Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 111th Cong. 9-11 nn.20-25 (2010) (testimony of Jon Leibowitz, Chairman, Federal Trade Commission) ("The Commission's robust enforcement actions have sent a strong signal to industry about the importance of data security, while providing guidance about how to accomplish this goal.").

as a requirement that the company implement a "comprehensive information security program."[66] The imposed program typically includes: (1) designating employees responsible for data security; (2) implementing reasonable safeguards to protect against identified security risks, including prevention, detection, and response to intrusions; (3) implementing privacy controls appropriate for the business, data use, and sensitivity of the information; (4) and performing regular testing, monitoring, and adjusting of privacy controls. These data-security practices also may give entities some notice of what the FTC believes § 5 requires but whether they are authoritative interpretive documents, given their negotiated, non-precedential nature, lack of judicial review, and agency statement of their non-binding nature, remains an open question.

THE FTC'S PUBLIC STATEMENTS

Even though the FTC has not exercised its specialized hybrid-rulemaking authority to issue any formal data-security rules or regulations, the FTC argues that it "has been investigating, testifying about, and providing public guidance on companies' data-security obligations under the FTC Act for more than a decade"[67] and that companies have sufficient notice "from both government and industry sources," suggesting that companies can follow the NIST, PCI-DSS, or ISO standards.[68] The FTC also argues that its business guidance provides fair notice.[69]

In 2011, the FTC issued *Protecting Personal Information: A Guide for Business*, which lists 36 detailed recommendations related to network security, password management, laptop

---

[66] *E.g.*, Decision and Order at 6-7, *In re* UPromise, Inc., No. C-4351 (Mar. 27, 2012); Decision and Order at 3, *In re* Ceridian Corp., No. C-4325 (June 8, 2011); Decision and Order at 3-4, *In re* Twitter, Inc., No. C-4316 (Mar. 2, 2011) [hereinafter Twitter Decision & Order], available at *http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf.*
[67] *See* Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 7, *FTC v. Wyndham Worldwide Corp.*, No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 9, 2012).
[68] Wyndham FTC Response, *supra* n. 4, at 17-18.
[69] *Id*. at 18-19.

security, firewall usage, wireless and remote access, and detection of data breaches.[70] Many of the recommendations listed in this publication also appear in the FTC's complaints. The document also explains that "[s]tatutes like . . . the Federal Trade Commission Act may require you to provide reasonable security for sensitive information"[71] although the statute neither refers to "security" nor defines "sensitive information."[72]

The FTC has also been a leader amongst various agencies in using the Internet and social media to disseminate information about the law and best practices. For example, an FTC Web site posting by an FTC attorney states, "[T]he FTC has tried to develop a single basic standard for data security that strikes the balance between providing concrete guidance, and allowing flexibility for different businesses' needs. The standard is straightforward: Companies must maintain reasonable procedures to protect sensitive information. Whether a company's security practices are reasonable will depend on (1) the nature and size of the company; (2) the types of information the company has; (3) the security tools available to the company based on the company's resources; and (4) the risks the company is likely to face."[73] The crux of the constitutional question is when are these settlements, tweets, speeches and blog posts authoritative for interpretive purposes? And, assuming they can be, do they create "ascertainable certainty" the constitutional requires before penalizing a party?

---

[70] FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS, (November, 2011), available at *http://www.business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf.*
[71] *Id*. at 5.
[72] In fact, the troubling constitutional implications of having the government regulate how and what people can say about someone to protect privacy continue to present recurring problems. *See, e.g.*, *Bartnicki v. Vopper*, 532 U.S. 514, 534-35 (2001) (holding that the protections of the First Amendment to disclose information about a public issue trumps the protections against illegally intercepted communications under the Electronic Communications Privacy Act); *see generally* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1050-51 (2000). It is unclear whether the FTC considered these and other potential complications while creating federal "privacy" rights through its actions.
[73] Burke Kappler, *Protecting Personal Information - Know Why*, BUREAU OF CONSUMER PROT. BUS. CTR. (Oct. 2007), available at *http:// business.ftc.gov/documents/art08-protecting-personal-information-know-why*.

APPLYING THE FAIR NOTICE DOCTRINE TO THE FTC'S INTERPRETATION OF SECTION 5

The D.C. Circuit's "ascertainable certainty" fair notice test is a helpful way to examine the FTC's data security enforcement activities to see if what data protection may be *required as a matter of law*. In its fair notice analysis, the D.C. Circuit reviews whether: (1) the plain text of the law is silent or unclear, and the entity's interpretation is plausible; (2) the agency has published clarification of its interpretation or performed other actions providing notice; (3) the agency has made conflicting interpretations; and (4) the entity faces a serious penalty. As described more fully below, in a nutshell, the statutory text is silent, the agency's interpretations are often seemingly unknown or unknowable in the eyes of those prosecuted, the agency maintains it has clarified its interpretations and otherwise provided fair notice and, as a result of these interpretations serious penalties are faced by those prosecuted.

SECTION 5 IS SILENT ON DATA SECURITY

The text of § 5 prohibits "unfair or deceptive acts or practices in or affecting commerce."[74] But the practical difficulties confronting the agency and those subject to its regulation are readily apparent when one refers to the enabling text of the statute itself. The FTC Act prohibits "unfair or deceptive acts or practices,"[75] and leaves the agency with broad authority and discretion to regulate practices that "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."[76] Congress intentionally used broad

---

[74] 15 U.S.C. § 45 (a)(1) (2006).
[75] *Id.*
[76] *Id.* § 45(n).

language so the FTC could address unanticipated practices in a changing economy.[77] The language of the statute itself is plain and does not reference any kind of data security or applicable standards for computer software and hardware systems.

THE FTC PUBLICATIONS ARE ADVISORY AND UNCLEAR

When the statutory language does not provide clarity on legally required data-security safeguards, agency statements or activities take on added significance. In particular, a reviewing court should not confine its inquiry to a search for some document listing information that it could label "actual notice," because in most cases evidence will suggest that *some* notice existed. Rather, a reviewing court should focus on whether the provision of notice through methods, such as recommendations and consent orders, constitutes *fair* notice and satisfies due process. Under this analysis, the FTC's recent and historic notice methods in this area remain problematic under the fair notice doctrine, because they do not clearly distinguish the law from best practices or explain why legal requirements may apply in some cases and not others.[78]

The D.C. Circuit conducts a broad inquiry for sources of notice. Previously, it has reviewed regulatory guidance and notices of proposed rulemaking published in the Federal Register,[79] adjudicatory opinions,[80] and agency policy statements.[81] These methods of information dissemination represent statements by the agency about how it intends to interpret the laws it is obliged to enforce. These publications are also sources that organizations may be

---

[77] S*ee FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1194 (10th Cir. 2009) ("[T]he FTCA enables the FTC to take action against unfair practices that have not yet been contemplated by more specific laws.").

[78] The FTC argues in Wyndham that industry provides notice of reasonable security standards. Wyndham FTC Response, *supra* n. 4, at 17-18. The legal standard for fair notice reviews what *the agency* states is the law, not what an industry body suggests are best practices.

[79] *Darrell Andrews Trucking, Inc. v. FMCSA*, 296 F.3d 1120, 1130-32 (D.C. Cir. 2002); *United States v. Chrysler Corp.*, 158 F.3d 1350, 1356 (D.C. Cir. 1998).

[80] *Darrell Andrews Trucking*, 296 F.3d at 1130-32.

[81] *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1333 (D.C. Cir. 1995).

expected to review. Conversely, providing information through settlements with individual parties and recommendations posted on an agency website do not seem to rise to the same level of importance, and organizational awareness of these information sources is likely limited.[82]

The FTC Has Not Published Notice in the Federal Register or a Policy Statement

The FTC has not issued any guidance or notices in the Federal Register to explain what it views as adequate data security under § 5. In addition to not using the Federal Register or formal adjudication, the FTC has not published policy statements. As a practical matter, the agency has not yet taken the opportunity to use all of the tools it has to address a serious problem facing industry, who increasingly find themselves feeling twice-victimized.

The FTC Has Used Only Informal Adjudicatory Processes

Agency adjudications are formal actions by an agency, and entities regulated by that agency closely scrutinize them.[83] These adjudications may provide precedential value, and entities are aware that adjudications are policymaking tools for agencies. Therefore, agencies may expect entities to be aware of relevant agency adjudications.

The FTC has not issued any adjudicatory opinions expressing its view on what data-security practices § 5 requires. Instead, as sources of notice, the agency points to the collection of published complaints and the attendant consent orders describing one entity's particular data-security practices that the FTC has deemed inadequate.[84] Courts might consider both sources as

---

[82] More practically, courts have not addressed the question of what types of agency activity should be deemed authoritative for purposes of fairness analysis in ways similar to the analysis of agency deference in *Chevron* or *Mead*.

[83] *See* Steven P. Croley, *Theories of Regulation: Incorporating the Administrative Process*, 98 COLUM. L. REV. 1, 114 (1998) (noting that agency adjudications "sometimes have far-reaching, prospective effects on entire industries," and "often apply prospectively to similarly situated parties not part of the immediate adjudication process").

[84] A collection of complaints and consent orders can be found on the FTC's website. *Legal Resources*, BUREAU OF CONSUMER PROT., *http://business.ftc.gov/legal-resources/29/35* (last visited Aug. 3, 2013). At least one commentator has observed that entities, and their attorneys, scrutinize the FTC's complaints and consent orders as though they were formal

guidance from the agency as a whole under the "ascertainable certainty" test.

Complaints and consent orders are not part of a formal adjudicatory process and do not contain reasoned analysis of the FTC's interpretation of the law.[85] Rather, the complaints list what the FTC believes to be faulty data-security practices in one particular case. The circumstances of each case differ, and, unlike formal adjudications, the FTC has not articulated why data-security practices in one case may violate § 5 while those same practices may not violate § 5 in another context. Moreover, the consent orders are settlement agreements among the parties and have no legal bearing, precedential or otherwise, on third parties.[86] For these reasons, there is little reason for a court to accept such statements as "authoritative" for purposes of evaluating whether they provide constitutionally required fair notice. If regulated entities cannot know with certainty that the complaints and consent orders are the law as applied to them, then the complaints and consent orders may not be sufficiently authoritative to provide fair notice.

An agency can expect an entity that 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.[87]

Fair Notice Analysis of the FTC's Best Practices Guide

Sadly, for whatever reason, the agency itself has done less than it could to help clarify

---

adjudications. Solove & Hartzog, *supra* n.61, at 25 (discussing that privacy attorneys view FTC settlements like cases interpreting statutes). However, even after careful scrutiny, privacy attorneys cannot definitively advise their clients on what they must do versus what they should do.

[85] *See* TechFreedom Brief at 8 ("Settlements (and testimony summarizing them) do not in any way constrain the FTC's subsequent enforcement decisions . . . [and] unlike published guidelines, they do not purport to lay out general enforcement principles and are not recognized as doing so by courts and the business community.").

[86] *United States v. ITT Cont'l Baking Co.*, 420 U.S. 223, 238 (1975) ("[A] consent decree or order is to be construed for enforcement purposes basically as a contract . . . ."); *United States v. Armour & Co.*, 402 U.S. 673, 681–82 (1971) ("Consent decrees are entered into by parties to a case after careful negotiation has produced agreement on their precise terms.").

[87] *See* Solove & Hartzog, *supra* n. 61, at 24-27 (arguing that the complaints and settlements are in many ways "the functional equivalent of common law").

which of its statements should have the force of law or otherwise provide guidance on the underlying legal requirements for data security. For example, the FTC describes its data security guide, *Protecting Personal Information: A Guide for Business*, as: "Practical tips for business on creating and implementing a plan for safeguarding personal information."[88] The guide suggests to "[u]se the checklists on the following pages to see how your company's practices measure up—and where changes are necessary."[89] The guide does not state that the items in the checklists are required by law or that an entity's compliance with the checklists will ensure that its data security is not an unfair practice. The guide further provides little instruction on when a particular recommendation is a legal requirement or otherwise is or would be a best practice.

Courts, including the D.C. Circuit, have not yet reviewed generally whether an agency's best practices guide provides fair notice of unlawful conduct. If a reviewing court finds that a best practices guide is "authoritative," the court likely would consider the FTC's best practices guide in its analysis.[90] However, there will be a question of the amount of weight a court will give such a guide since it is only a set of recommendations.[91]

Courts place agency action on a spectrum to determine how much deference to afford an agency interpretation of the laws that it enforces. On one end of the spectrum formal rulemaking and adjudication and some informal actions are afforded *Chevron* deference.[92] On the other end of the spectrum are interpretations made by agencies to which Congress has not given sufficient authority. Courts grant those interpretations no deference.[93] To determine whether *Chevron* deference is appropriate for interpretations made outside the context of formal rulemaking or

---

[88] FED. TRADE COMM'N, *supra* n. 70.
[89] FED. TRADE COMM'N, *supra* n. 70.
[90] The D.C. Circuit reviews "public statements issued by the agency." *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995).
[91] Distinguishing between what is required and what is advisory in these guides can be practically impossible without *authoritative* distinctions between the two, an issue frequently discussed among practitioners and agency staff and management.
[92] *Mead Corp.*, 533 U.S. at 229-30.
[93] *See id*. at 231.

adjudications, courts consider whether: (1) Congress intended the agency to interpret the statute with the force of law; (2) the agency action binds only individual parties to a ruling or also applies to third parties; and (3) the interpretation is made by the agency as a whole or by agency staff on an ad hoc basis.[94] The Supreme Court in *United States v. Mead* noted explicitly that interpretations contained in policy statements, agency manuals, enforcement guidelines, and opinion letters do not deserve *Chevron* deference because they lack the force of law.[95]

The FTC Data-Security Best Practices Guide is simply a list of recommendations; it is not the result of formal rulemaking or adjudication and does not bind any parties. It is more similar to the policy statements, agency manuals, enforcement guidelines, and opinion letters that courts have held do not deserve *Chevron* deference. For an interpretation to provide fair notice, it must come from a position of authority.[96] Similarly, staff attorney's Internet postings discussing data security do not represent the entire agency and are not authoritative. Accordingly, a court would probably not appropriately consider the FTC staff attorneys' Internet postings at all in its fair notice analysis. Doctrinally, *Mead* laid important groundwork regarding why much of what the FTC has been saying – especially given its chosen means – raises serious constitutional question of fair notice.

Concerns Stemming from the Lack of Concrete and Authoritative Notice

Consent orders,[97] the FTC's interpretive guidance to entities, consist of little more than published reports and its reliance on consent orders. In particular, the agency has not used its formal rulemaking authority and has not had any formal adjudication through which to

---

[94] *See id*. at 231-34.
[95] *Id.* at 234; *Christensen*, 529 U.S. at 587.
[96] *See Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 157 (D.C. Cir. 1986) (Scalia, J.).
[97] Thirty-six data-security cases were brought under the FTC Act. Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 7, *FTC v. Wyndham Worldwide Corp.*, No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 9, 2012).

communicate its interpretations. Thus, entities have very little guidance. They have: (1) lists of fairly detailed data-security practices published in single-party complaints; (2) consent orders with vague descriptions of comprehensive information security programs; and (3) published guidance in which the FTC *encourages rather than requires* entities to implement data-security safeguards. With such scant and non-authoritative guidance, the central due process question remains whether such information provides "fair" notice adequate to address constitutional concerns. To be sure, the FTC's published complaints, consent orders, and the aforementioned data-security guide identify many of the same data-security requirements it alleges investigation targets do not adequately maintain. Nevertheless, *some* notice is not *fair* notice—which is a practical constitutional question befuddling many individuals and begging the question: Does reasonable information security require an FTC and administrative law specialist to figure out what the law requires?

Due process requires examining the nature and quality of the notice to ensure entities have a clear description of required behavior from an authoritative source (i.e., fair notice)—which settlements with third parties and agency recommendations do not provide. Moreover, a *post hoc* review of whether sufficient authoritative notice existed *at the time* of the alleged violations is difficult considering an assessment of current requirements is impossible.

Section 5 Violation May Result in Serious Penalty

Under § 5, the FTC cannot directly impose or request a monetary penalty. Congress provided the FTC with the sole remedy to issue an order requiring an entity to cease and desist certain conduct, in part, to avoid potential due process concerns.[98] If a party violates a cease-and-

[98] Michael J. Pelgro, Note, The Authority of the Federal Trade Commission to Order Corrective Advertising, 19 B.C. L. REV. 899, 907 (1978).

desist order, a court can order a civil penalty, the rescission of contracts, restitution, refunds, and disgorgement.[99] Alternatively, the FTC can request that a court issue an injunction prohibiting certain behavior.[100] Few would seem to argue that a violation of § 5 could not result in a substantial loss of property implicating the fair notice doctrine.

Given the relative paucity of authoritative agency interpretation, whether existing FTC activities have provided "fair notice" remains an open question. Section 5 of the FTC Act gives the FTC broad authority to combat "unfair trade practices." The statutory language does not provide notice of required data-security safeguards. The FTC has chosen not to issue regulations to explain what data-security practices are "unfair." While the agency's informal communications may provide some notice about the FTC's position, whether courts should deem these communications as sufficiently authoritative to provide fair notice is questionable. Perhaps more importantly, many businesses struggle with understanding what's required of them and are often stunned after a security incident to learn that the party mostly likely to be prosecuted is in fact the organization that held the underlying information—not the perpetrators.

CHALLENGES OF THE FTC'S APPROACH AND MOVING FORWARD

Even if a court concluded that fair notice of required data security practices exists, there seems to be little doubt that underlying legal requirements and the process of determining what is "reasonable" data security could be communicated more effectively. Ironically, an agency that

---

[99] 15 U.S.C. § 45(l) (2006) ("Any person, partnership, or corporation who violates an order of the Commission after it has become final, and while such order is in effect, shall forfeit and pay to the United States a civil penalty of not more than $10,000 for each violation . . . ."); *id.* § 57b(b) ("The court in an action under subsection (a) of this section [an action following a cease a desist order] shall have jurisdiction to grant such relief as the court finds necessary to redress injury to consumers or other persons, partnerships, and corporations resulting from the rule violation or the unfair or deceptive act or practice, as the case may be. Such relief may include, but shall not be limited to, rescission or reformation of contracts, the refund of money or return of property, the payment of damages, and public notification respecting the rule violation or the unfair or deceptive act or practice, as the case may be; except that nothing in this subsection is intended to authorize the imposition of any exemplary or punitive damages.").

[100] *Id.* § 53(b) (allowing the court to issue a temporary restraining order, preliminary injunction, or permanent injunction).

calls on companies to be more transparent about their business practices has not been transparent about its data-security policy, seemingly constrained by the practical difficulties of using investigations and enforcement actions to provide fair notice.

The D.C. Circuit recommended agency rulemaking instead of a series of adjudicative proceedings to explain a regulation because "full and explicit notice is the heart of administrative fairness."[101] The FTC seems to agree that traditional APA rulemaking may be superior to adjudicative proceedings, but it has not yet undertaken to use the modified APA rulemaking authority it already possesses. The FTC has supported federal legislation that would prescribe data-security requirements. The agency recommended that Congress phrase the legislation in general terms, using broad definitions, to allow the implementing agency to promulgate rules or regulations to "provide further guidance to Web sites by defining fair information practices with greater specificity."[102] The FTC stated that regulations could clarify the definition of "adequate security."[103]

FORMAL RULEMAKING MAY PROVIDE FAIR NOTICE BENEFITS

The FTC Has Issued Rules Pursuant to Other Data-Security Related Statutes

While the FTC has not used its current limited rulemaking authority under § 5 to clarify "unfair" data-security practices due to onerous rule-making proceedings, Congress has directed the FTC to promulgate regulations under other laws, such as COPPA and FACTA.[104] As

---

[101] *Radio Athens, Inc. v. FCC*, 401 F.2d 398, 404 (D.C. Cir. 1968) ("[T]he agency could and should have proceeded to accomplish its result by exercising its broad rulemaking powers.").
[102] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 37 (2000) [hereinafter FED. TRADE COMM'N, PRIVACY ONLINE].
[103] *Id.* (internal quotation marks omitted).
[104] *See* 15 U.S.C. § 1681m(e) (FACTA); *id.* § 6502(b)(1) (COPPA).

expected, entities have fully participated in the process.[105] In addition, the FTC altered its proposed rules based on the comments it received.[106] The process and resulting rulemaking have proven far more likely to yield "ascertainable certainty" of the agency's interpretation.

While the final rules the FTC implemented may result in inflexible requirements rather than adaptable principles, the quality of the rules promulgated by the FTC in these instances is beside the point for addressing fair notice concerns.[107] All parties received an opportunity to participate in a public and deliberative process and potentially affect the outcome. The rule-making process also leads to rule refinement outside the enforcement context, which may allow the parties to more objectively view and craft the rules. As it currently stands, recent agency data-security investigations reflect private non-public, refinement of statutory interpretations lacking transparency and clarity. This process runs the practical risk of creating a costly and vexatious guessing game for businesses constrained by a lack of consensus and clarity. The FTC clearly does not intend this consequence. Those subject to FTC data security requirements lack the benefit of any authoritative policy statements on these issues.

Fair Notice Benefits of Rulemaking

There are specific fair notice advantages to rulemaking over the prosecution and settlement approach used by the agency.[108] Rulemaking can provide regulated entities with clear

---

[105] *See* Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 3972-73 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312); Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,718, 63,718 (Nov. 9, 2007) (codified at 16 C.F.R. pt. 681).

[106] *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,889 (Nov. 3, 1999) (codified at 16 C.F.R. pt. 312); Identity Theft Red Flags, 72 Fed. Reg. at 63,719.

[107] Rulemaking is not a panacea. Inflexible rules in a fast-changing environment are problematic. However, the FTC can and should provide clear notice on what the law is. Rulemaking is one method to improve such notice. Rules are not inherently bad, and a principles-based data-security legal framework (rather than a detailed data-security standard) would be one workable solution. The FTC has already articulated 36 detailed recommendations in its guidance. FED. TRADE COMM'N, *supra* n. 70. The FTC has also pointed to the NIST and ISO standards for guidance. Wyndham FTC Response, *supra* n. 4, at 18. The agency holds companies accountable to some or all of these recommendations in some fashion. *Id.* at 17-19.

[108] *See* TechFreedom Brief at 9-10 (noting the ways in which rulemaking is preferable to case-by-case adjudication as a method

guidance, incorporate the thinking of additional stakeholders, prevent cynical speculation regarding agency decision-making, and lessen enforcement and compliance costs.[109] Further, improved notice of a clear rule would likely result in greater compliance.[110] The FTC has not used its existing § 5 rulemaking authority to clarify "unfair" data-security practices because of its alleged impracticality.[111] The FTC does not believe it would "be possible to set forth the type of particularized guidelines" to describe proper data-security safeguards.[112] It has stated that "[d]ata security industry standards are continually changing in response to evolving threats and new vulnerabilities and, as such, are 'so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule."[113] The FTC has also stated that "industries and businesses have a variety of network structures that store or transfer different types of data, and reasonable network security will reflect the likelihood that such information will be targeted and, if so, the likely method of attack."[114]

The FTC's statements are mystifying for two reasons. First, if the FTC does not believe that it can properly define "reasonable," fair notice of the reasonableness standard seems unlikely?[115] Second, the FTC seems to have taken the stance that, because technology changes

---

of developing agency-enforced law).

[109] Colin S. Diver, The Optimal Precision of Administrative Rules, 93 YALE L.J. 65, 73, 74 (1983); Brice McAdoo Clagett, Informal Action—Adjudication—Rule Making: Some Recent Developments in Federal Administrative Law, 1971 DUKE L.J. 51, 54-57, 83-84; Bunn et al., No Regulation Without Representation: Would Judicial Enforcement of a Stricter Nondelegation Doctrine Limit Administrative Lawmaking?, 1983 WIS. L. REV. 341, 343-44 (1983).

[110] *See* Diver, *supra* n. 109, at 72, 75.

[111] *Prepared Statement of the Federal Trade Commission on Data Security*, *supra* n. 55, at 11 ("[E]ffective consumer protection requires that the Commission be able to promulgate rules in a more timely and efficient manner.").

[112] Wyndham FTC Response, *supra* n. 4, at 20. At the same time, the White House and Department of Commerce have seemingly articulated an alternative view on prospects for standards development - at least for privacy. "Companies, industry groups, privacy advocates, consumer groups, crime victims, academics, international partners, State Attorneys General, Federal civil and criminal law enforcement representatives, and other relevant groups" have been called together to develop voluntary, enforceable privacy codes of conduct. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 7 (2012) [hereinafter WHITE HOUSE PRIVACY BILL OF RIGHTS], available at *http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_ paper.pdf.*

[113] *Id.* (quoting *SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947)).

[114] *Id*.

[115] *See* Chamber of Commerce Brief at 12 (noting that "it is *precisely because* the appropriate standards are difficult to ascertain that businesses cannot be held to a nebulous notion of 'reasonableness,' all without any formal guidance before they find

frequently, drafting regulations would be fruitless. However, drafting flexible, principles-based regulations would provide guidance to entities and would still apply as technology changes. The concept of drafting laws in an ever-changing world is nothing new. Moreover, the complaints that the FTC filed a decade ago look similar to the complaints that the agency is filing today.[116] Therefore, the FTC's own actions seemingly contradict that regulations would be impractical or out of date upon publication.

FORMAL ADJUDICATION MAY PROVIDE FAIR NOTICE BENEFITS

A formal adjudicatory process can help provide notice to entities in two ways. When the FTC seeks a formal adjudication, the FTC must report its findings of fact. These findings of fact would clearly and officially communicate, which data-security practices violate the FTC's interpretation of § 5. This mode of operation is superior to the current complaint and settlement process regarding confusion about legal requirements because it puts the FTC on record and may create greater predictability for entities subject to enforcement. To be effective, the agency would need to articulate its interpretation and rationale which the current investigation-complaint-settlement routine does not. Moreover, the FTC or court can publish an opinion, which will further enunciate and clarify the FTC's interpretation. Judicial review also may provide authority supporting the interpretation.

Like rulemaking, this method of clarifying the FTC's interpretation can provide additional benefits, such as improving legal compliance and preventing entities from wasting

---

themselves in violation of the law.").

[116] *Compare* Complaint for Permanent Injunctive and Other Equitable Relief, *FTC v. Wash. Data Res., Inc.*, No. 8:09-cv-02309-SDM-TBM (M.D. Fla. Nov. 10, 2009), *with* Complaint for Permanent Injunction and Other Equitable Relief, *FTC v. SlimAmerica, Inc.*, No. 0:97-cv-06072-DLG (S.D. Fla. Jan. 24, 1997).

resources by attempting to comply with unclear requirements.[117] Nevertheless, adjudication may remain less desirable than rulemaking because regulation by adjudication means that nonparties may not be able to protect their rights.[118] In addition, when regulating by adjudication, the public cannot directly monitor an agency.[119]

ADVISORY OPINIONS, POLICY STATEMENTS, AND OTHER COMMUNICATIONS

Policies made through formal rulemaking and adjudications are more definitively authoritative and can provide entities with clear notice. Advisory opinions, policy statements, analysis appended to proposed consent orders, and other similar communications are less formal and authoritative, but possibly more effective than the current complaint and settlement process and best practice recommendations, as they can communicate agency reasoning and principles.

CONCLUSION

No formal rulemakings or adjudications related to data security have occurred to date, and the FTC appears to regulate data security primarily through complaints and consent orders. This method creates ambiguity because complaints and consent orders are inconsistent or lack additional helpful information. It also is unclear whether nonparties to the investigation should attempt to follow the complaint, the consent order, neither, or both, or whether implementing some or all of the measures would result in "fair" data security. The FTC's position that "security standards can be enforced in an industry-specific, case-by-case manner"[120] provides little guidance. This inherent ambiguity poses dangerous and unnecessary compliance risks for

---

[117] *See* Diver, *supra* n. 109, at 72, 103.
[118] *See* Clagett, *supra* n. 109, at 83.
[119] *See* Bunn, *supra* n. 109, at 343; Clagett, *supra* n. 109, at 56-57 (citing *Holmes v. N.Y.C. Hous. Auth.*, 398 F.2d 262 (2d Cir. 1968); *Hornsby v. Allen*, 326 F.2d 605 (5th Cir. 1964)).
[120] Wyndham FTC Response, *supra* n. 4, at 22.

regulated entities due to the potentially serious penalties that may result from non-compliance.

The FTC's existing enforcement and guidance practices also pose serious constitutional concerns of providing fair notice. Given the current environment of aggressive enforcement against the victims of third-party criminal hacking who operate with no clear guidance what data security actions they should take to avoid allegations of unfair and deceptive acts and practices, improved authoritative interpretations of § 5 are crucial to improve compliance and provide entities with sufficient information to perform proper risk management.

The FTC has several alternative methods for providing more useful and authoritative guidance to entities, but simply stating a vague standard will not improve the situation if it does nothing to clarify the underlying uncertainty or to resolve the problem of fair notice. A "reasonableness" test absent additional, flexible principles-based authoritative guidelines or significant additional court-resolved litigation will remain problematic. As FTC guidance states, "[t]here's no one-size-fits-all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect from your customers."[121] In other words, data-security standards may differ as a function of the sensitivity of the data collected, the amount of data collected, and how the data is collected, used, and disclosed to third parties. Using the standards of "reasonable" and "appropriate," without accounting for the nature of the business and the kinds of information that are collected may not ensure that *fair* notice occurs. However, these factors should at least be considered as crucial inputs when determining the data-security safeguards an entity should implement. Nonetheless, such additional standards would still provide no useful guidance without substantial additional stakeholder participation or the reasoned and thorough discussion of the flexible standard in a formal adjudicatory opinion,

---

[121] FED. TRADE COMM'N, *supra* n. 70, at 23.

policy statement, or advisory opinion.

Moreover, even if the FTC employed formal rulemaking or adjudication, the reasonableness test without explanation as currently relied upon by the agency seems less useful in contexts like data security, where the meaning of "reasonable" remains subject to ongoing technological evolution and prevailing data-protection preferences. This is evident now as society continues to debate the balance of strong privacy protections against the societal benefits of the free-flow of information.[122] And notably, the FTC itself does not seem to consistently define what information is "sensitive," potentially deserving greater protection.[123] Thus, there may be no such thing as "reasonable" privacy and data-security practices until a more satisfactory consensus on these issues emerges.

Given the lack of agreement on what "privacy" is, what data should be protected, and what data-security practices should be used to protect that data, any rule based on "reasonableness" should also include explanation. Otherwise, the rule is entirely arbitrary, and "reasonable" security will be whatever the FTC dictates at that point in time. At any given time, an entity would be unable to determine with precision what data-security practices are "reasonable," and whether it could ensure successful compliance with § 5. This situation creates due process challenges and a palpable risk of post-hoc rationalization. For all of these reasons and those laid out above, the agency continues to have a unique opportunity to take up many of

---

[122] WHITE HOUSE PRIVACY BILL OF RIGHTS, *supra* n. 112, at 5-6.

[123] In its recent privacy report, "[t]he Commission defines as sensitive, at a minimum, data about children, financial and health information, Social Security numbers, and certain geolocation data . . . ." FED. TRADE COMM'N, *supra* n. 70, at 47 n. 214. The privacy report also lists passwords as sensitive information. *Id.* at 8, 15, 37 n. 17 4. In other guidance, the FTC includes names that identify customers or employees as sensitive information. FED. TRADE COMM'N, DOES YOUR ORGANIZATION COLLECT AND KEEP SENSITIVE INFORMATION? 1, available at *http://www.business.ftc.gov/sites/default/files/pdf/bus52.pdf;* FED. TRADE COMM'N, *supra* n. 70, at 5. A person's name can hardly be considered sensitive personal information, and the FTC has recently implied that passwords are not sensitive. Press Release, Fed. Trade Comm'n, Tracking Software Company Settles FTC Charges that It Deceived Consumers and Failed to Safeguard Sensitive Data It Collected (Oct. 22, 2012), available at *http://www.ftc.gov/opa/2012/10/compete.shtm.*

the tools it has at its disposal to address the practical problem that businesses face in being unable to determine better what data security measures are required as a matter of law and which practices are simply better or best.