PSYCHICS, RUSSIAN ROULETTE, AND DATA SECURITY: THE FTC'S HIDDEN DATA-SECURITY REQUIREMENTS

Gerard M. Stegmaier and Wendell Bartnick[*]

INTRODUCTION

Data breaches continue to grab headlines. According to a recent report published by Verizon, there were at least 855 data breaches affecting over 174 million data records in 2011 across the globe.[1] According to the report, most data breaches involved malicious activity by outsiders.[2] In other words, most of the entities with a reported data breach are victims of criminal activity.

Poor data-security practices may contribute to data breaches. The Verizon report concluded that nearly 80 percent of the data breaches for which it had information showed a victim that had easily exploitable weaknesses.[3] While entities have business incentives to protect the information they collect, there are no broad federal laws requiring data security. Instead, the law has focused on criminalizing unauthorized access. This is not surprising given that 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 considered public debate has led to a consensus that increased information protection was required.[4] Generally, in the United States, state-enacted breach notification requirements constitute the primary regulatory mechanisms used to encourage data

---

[*] Gerard M. Stegmaier is an adjunct professor at George Mason University School of Law where he created and has taught one of the first information privacy courses for over a decade. He is also an attorney in private practice who regularly appears before the Federal Trade Commission and assists technology and related businesses with all aspects of their privacy and information-governance concerns. Wendell Bartnick is an attorney who practices with Mr. Stegmaier in these same areas. The views contained in this Essay represent solely the views of the Authors in their individual and private capacities and are not necessarily the views of their firm or of any particular client.

[1] VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT 2 (2012), *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

[2] *Id.* at 3.

[3] *Id.*

[4] There are no less than six data-security bills moving through Congress. *See* Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011); Data Security Act of 2011, S. 1434, 112th Cong. (2011); SAFE Data Act, H.R. 2577, 112th Cong. (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011); Data Accountability and Trust Act (DATA) of 2011, H.R. 1841, 112th Cong. (2011); Data Accountability and Trust Act, H.R. 1707, 112th Cong. (2011).

stewardship.[5] Most states require entities to notify affected individuals when certain personal information is affected by a breach.[6]

Given the lack of a comprehensive federal regulatory scheme, and the increasing awareness of security breaches following state notification schemes, it is not surprising that the Federal Trade Commission ("FTC," "Commission," or "agency") has begun requiring reasonable data security for entities not covered by existing, industry-specific federal regulations over the last decade. The agency is the federal government's largest consumer protection agency. The Commission routinely investigates publicly reported data-related incidents with the threat of subsequent litigation. Since 2000, the FTC has brought forty-two data-security cases.[7] Further, the FTC recently agreed to a consent order with HTC America, after the FTC alleged that HTC America's mobile device security vulnerabilities potentially exposed sensitive information.[8] The complaint did not allege any actual data compromise.

The FTC bases its authority over data security on the broadly-worded Section 5 of the Federal Trade Commission Act ("FTC Act"). Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[9] "Unfair" practices are defined as those 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."[10] Usually, the FTC makes a deceptive practices claim when an entity has a data breach after publishing statements that it secures data.[11] Less frequently, the FTC alleges unfair

---

5 However, some states, such as California, have some data-security statutes. *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.").

6 *See State Security Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last updated Aug. 20, 2012). Only Alabama, Kentucky, New Mexico, and South Dakota do not have such laws, though the Texas law may require notification to the residents in those states. *See* TEX. BUS. & COM. CODE ANN. § 521.053 (West 2012).

7 *See* Plaintiff's Response in Opposition to Whyndham Hotels and Resorts' Motion to Dismiss at 7, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-PHX-PGR (D. Ariz. Aug. 9, 2012) [hereinafter Wyndham FTC Response]. Since the date of this complaint, the FTC investigated HTC America as well.

8 Complaint at 16-18, *In re* HTC Am., Inc., No. 122 3049 (Feb. 22, 2013), *available at* http://www.ftc.gov/os/caselist/1223049/index.shtm.

9 15 U.S.C. § 45(a)(1) (2006).

10 *Id.* § 45(n).

11 *See* Wyndham FTC Response, *supra* note 7, at 7 (noting that thirty-six data-security cases were brought under the FTC Act).

practices in data-security cases.[12] However, nothing in Section 5 mentions data security, which begs a practical question: Because the Constitution requires that fair notice be provided to entities so they are able to reasonably understand what behavior complies with the law, can the investigation and prosecution of entities under Section 5 in data-security cases violate entities' constitutional rights to fair notice?

Generally, the fair notice doctrine reflects society's expectations of "fundamental fairness"—that entities should not be punished for failing to comply with a law about which they could not have known.[13] The doctrine restrains law enforcement officials' discretion by requiring the procedural step of clarifying laws before enforcing them.[14] The issue is whether a law "describes the circumstances with sufficient clarity to provide constitutionally adequate warning of the conduct prohibited."[15]

The fair notice doctrine initially took root in the context of criminal defense,[16] but in 1968, the U.S. Court of Appeals for the District of Columbia Circuit ("D.C. Circuit") acknowledged the applicability of the doctrine in the civil administrative context.[17] 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."[18] Otherwise, the court stated tongue in cheek, penalizing a regulated entity for a reasonable interpretation of a law not matching the agency's unclear interpretation would require the entity to exercise "extraordinary intuition" potentially requiring "the aid of a psychic."[19] Indeed, the D.C. Circuit previously described the situation as resembling "Russian Roulette."[20]

The fair notice doctrine is not a trivial, academic legal theory with little bearing on the practice of law. On the contrary, it is directly relevant in the current regulatory climate, given the FTC's broad discretion under Section 5 of the FTC Act, the FTC's aggressive enforcement stance in the data-

---

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

13 McBoyle v. United States, 283 U.S. 25, 27 (1931). The fair notice doctrine is consistent with the legal principle that "ignorance is no defense," where enforcement of a clear law is permitted even when a defendant lacks knowledge of the law. *See* 22 C.J.S. *Criminal Law* § 113 (2012). However, if the law is unclear so as to create no clear description of compliant behavior, the fair notice doctrine may be a proper defense. *Id.*

14 Kieran Ringgenberg, Comment, United States v. Chrysler*: The Conflict Between Fair Warning and Adjudicative Retroactivity in D.C. Circuit Administrative Law*, 74 N.Y.U. L. REV. 914, 928 (1999).

15 Gates & Fox Co. v. OSHRC, 790 F.2d 154, 155 (D.C. Cir. 1986) (Scalia, J.).

16 *See* United States v. Nat'l Dairy Prods. Corp., 372 U.S. 29, 32-33 (1963) (citing United States v. Harriss, 347 U.S. 612, 617 (1954)).

17 Radio Athens, Inc. v. FCC, 401 F.2d 398, 404 (D.C. Cir. 1968).

18 Gen. Elec. Co. v. EPA, 53 F.3d 1324, 1328-29 (D.C. Cir. 1995).

19 United States v. Chrysler Corp., 158 F.3d 1350, 1357 (D.C. Cir. 1998).

20 Satellite Broad. Co. v. FCC, 824 F.2d 1, 4 (D.C. Cir. 1987) (internal quotation marks omitted).

security context, and the FTC's declination to use its existing rulemaking authority to clarify its data-security expectations. In light of the agency's current approach toward data-security enforcement, challenges to FTC actions under the fair notice doctrine may very well become increasingly justified. This Essay contends that although the FTC has undertaken significant efforts to develop and improve notice of its interpretation of Section 5, the nature, format, and content of the agency's data-security-related pronouncements raise equitable considerations that create serious due process concerns. In short, this Essay questions whether actual notice, which may exist in many of these cases, is an appropriate substitute for fair notice, which we believe due process requires. In essence, this Essay asks: If an entity cannot ascertain what the law is, how can it know what it must do—especially where liability most commonly arises out of the malfeasance of others?

This Essay's analysis begins by explaining the fair notice doctrine and the various tests courts use to analyze whether fair notice exists. Next, this Essay looks at the potential sources of notice used by the FTC to communicate its interpretation of Section 5 in the data-security context. This Essay then reviews the fair notice doctrine as it relates to the FTC's enforcement efforts by reviewing the first data-security case brought under Section 5 in which a defendant challenged the FTC's conduct in this area. The FTC's current process likely provides some notice to entities, but the Essay concludes that constitutionally required *fair notice* may be lacking due to the agency's use of an unclear standard and the lack of authoritative guidance.

Even if the FTC has provided enough notice to meet constitutional requirements, this Essay proposes that its current efforts are inadequate. The Essay evaluates alternative means by which the agency may construe and articulate its interpretation of Section 5 and any additional data-security requirements the FTC maintains the law requires. Specifically, the Essay explores formal rulemaking, formal adjudicatory processes, and the use of advisory opinions or other interpretive statements as alternatives to the agency's current practice. The FTC's current practice, this Essay believes, relies heavily upon the publication of negotiated resolutions that consist of draft complaints coupled with consent agreements, as well as the release of reports and other interpretive guidance that blend best practices with law. The result is that legal requirements are generally shrouded in mystery and uncertain risk of enforcement discretion. Finally, this Essay argues that a standard based on "reasonableness" grounded solely in settlements raises its own questions of whether constitutionally adequate fair notice was provided. Such a standard seems unfair and problematic to those tasked with assisting entities in avoiding unfair and deceptive trade practices.

I. FAIR NOTICE DOCTRINE

A. *What Is the Fair Notice Doctrine?*

The fair notice doctrine requires that entities should be able to reasonably understand whether or not 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 the entity to conform, the agency has not provided fair notice.[21] According to the courts, the doctrine is supported by both constitutional and administrative law underpinnings: "Traditional concepts of due process incorporated into administrative law preclude an agency from penalizing a private party for violating a rule without first providing adequate notice of the substance of the rule."[22] Due process protections are likely even more strongly implicated when an agency has not promulgated a formal rule and, instead, uses its enforcement conduct to define the contours of its broad discretion.[23]

1. Constitutional Underpinnings

The D.C. Circuit observed that the due process clauses support the fair notice doctrine:[24] "Procedural due process imposes constraints on governmental decisions which deprive individuals of 'liberty' or 'property' interests within the meaning of the Due Process Clause of the Fifth or Fourteenth Amendment."[25] Typically, these constraints include requiring a government agency to provide adequate notice.[26] In essence, due process prohibits the application of a law "that fails to give fair warning of the conduct it prohibits or requires."[27]

---

21 *Gen. Elec.*, 53 F.3d at 1329 (citing Diamond Roofing Co. v. OSHRC, 528 F.2d 645, 649 (5th Cir. 1976)). This is the D.C. Circuit's test. This Essay will describe this and other tests in greater detail below. *See infra* Part I.B-C.

22 *Satellite Broad.*, 824 F.2d at 3 (citing Gates & Fox Co. v. OSHRC, 790 F.2d. 154, 156 (D.C. Cir. 1986)).

23 *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.").

24 *Chrysler Corp.*, 158 F.3d at 1351. Some commenters have observed that the D.C. Circuit "has backpedaled" from its constitutional foundation and instead has rested the doctrine on administrative law principles. *See* Ringgenberg, *supra* note 14, at 927.

25 Mathews v. Eldridge, 424 U.S. 319, 332 (1976).

26 *Id.* at 348; Goldberg v. Kelly, 397 U.S. 254, 267-68 (1970).

27 *Gates & Fox*, 790 F.2d at 156 (Scalia, J.).

2. Administrative Law Underpinnings

The Administrative Procedures Act ("APA") prescribes the baseline rules for administrative rulemaking and adjudication.[28] The APA includes several explicit notice requirements as part of the process.[29] Under the APA, a court may set aside an agency action that is "arbitrary or capricious," and the D.C. Circuit has used this power in cases where adequate notice was not provided.[30] While courts have rarely theorized that the APA supports the fair notice doctrine,[31] the D.C. Circuit has stated that it is a "well-established rule in administrative law that the application of a rule may be successfully challenged if it does not give fair warning that the allegedly violative conduct was prohibited."[32] Further, the court has observed that "full and explicit notice is the heart of administrative fairness."[33] Therefore, the D.C. Circuit has concluded that fair notice is integral to proper agency action.

Constitutional due process requirements and administrative law require adequate notice of laws and regulations before agency enforcement occurs. In defending itself against agency enforcement, a defendant may raise the fair notice defense when it believes it has not received adequate notice of the contours of a law such that it can be reasonably expected to comply with the law.[34]

---

28 5 U.S.C. §§ 553-54 (2006).

29 *Id.* §§ 553(b), (d), 554(b) (requiring general notice of proposed rulemaking published in the Federal Register, publication of a final rule at least 30 days before becoming effective, as well as notice of an agency hearing).

30 Satellite Broad. Co. v. FCC, 824 F.2d 1, 4 (D.C. Cir. 1987); *see also* 5 U.S.C. § 706(2)(A) (2006) ("The reviewing court shall . . . hold unlawful and set aside agency action, findings, and conclusions found to be . . . arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law."); United States v. Chrysler Corp., 158 F.3d 1350, 1354 (D.C. Cir. 1998) (citing Gen. Elec. Co. v. EPA, 53 F.3d 1324, 1328, 1330 (D.C. Cir. 1995)); Rollins Envtl. Servs. Inc. v. EPA, 937 F.2d 649, 654 (D.C. Cir. 1991).

31 *See* Albert C. Lin, *Refining Fair Notice Doctrine: What Notice Is Required of Civil Regulations?*, 55 BAYLOR L. REV. 991, 998-99 (2003).

32 *Chrysler Corp.*, 158 F.3d at 1355; *see also Rollins*, 937 F.2d at 655 (Edwards, J., dissenting in part and concurring in part).

33 Radio Athens, Inc. v. FCC, 401 F.2d 398, 404 (D.C. Cir. 1968).

34 *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."); Lin, *supra* note 3131, at 998 ("[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

B. *Distinction Between* Chevron *Deference and the Fair Notice Doctrine*

Under what is known as *Chevron* deference, courts defer to agencies' reasonable interpretations of the statutes they enforce when such statutes are ambiguous.[35] *Chevron* deference means that courts accept agency interpretations regardless of whether there are other plausible interpretations.[36] A key rationale for such deference is the presumed "technical expertise" of agencies and Congress's vesting of "political authority [to administrative agencies] to carry out statutory mandates."[37] However, where an agency has made an interpretation that is manifestly wrong or clearly erroneous, arbitrary, or unreasonable, a court will not follow an agency's interpretation.[38]

The difference between the applicability of *Chevron* deference and the fair notice doctrine can be subtle. An agency benefits from *Chevron* deference when it reasonably interprets an ambiguous statute. A defendant in an agency enforcement action may use the fair notice doctrine to argue that the agency's interpretation of a statute, although reasonable under *Chevron*, has not been made public or is ambiguous. If a court upholds the fair notice defense in relation to an agency interpretation, the court will dismiss the claims stemming from that interpretation.[39] Thus, if *Chevron* deference represents a powerful sword in the hands of the administrative state when a statute is ambiguous, the fair notice doctrine provides an unusual type of shield—one that arguably protects the individual from blows from behind caused by unpredictable agency action.

If an agency interpretation is unclear, entities may use the fair notice doctrine to claim that they should not be held accountable for noncompliance. In such a case, the court would not look at the reasonableness of the agency's "intended interpretation, but at the clarity with which the agency made that intent known."[40] The permissibility of the agency's interpretation of a disputed law does not matter if it does not give "fair warning" of the

---

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.").

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

36 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).

37 *Gen. Elec.*, 53 F.3d at 1327 (citing *Chevron*, 467 U.S. at 864-66).

38 2 AM. JUR. 2D, *supra* note 36, § 77.

39 Gates & Fox Co. v. OSHRC, 790 F.2d 154, 156 (D.C. Cir. 1986) (Scalia, J.) ("Where the imposition of penal sanctions is at issue, . . . the due process clause prevents that deference from validating the application of a regulation that fails to give fair warning of the conduct it prohibits or requires.").

40 McElroy Elecs. Corp. v. FCC, 990 F.2d 1351, 1358 (D.C. Cir. 1993).

conduct it prohibits or requires.[41] Put simply, the attack itself is not reviewed, but rather whether the individual received warning that there was something they should or should not be doing to avoid the attack in the first place is reviewed.

Applying these judicial rules to our subject matter, if the FTC published a rule interpreting Section 5 to require that entities implement specific data-security safeguards and a defendant attempted to argue that Section 5 was ambiguous, courts would likely grant *Chevron* deference if the FTC's interpretation was reasonable. However, if the FTC did not publish an authoritative data-security interpretation or published an ambiguous interpretation of Section 5, an entity that allegedly did not comply with these requirements would be able to use the fair notice defense to escape liability.

In the absence of any rule or regulation, 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"[42] 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."[43] Courts have historically given the agency wide latitude to determine whether the practices of regulated entities are unfair or deceptive, but whether *Chevron* deference is given is unclear.[44]

C. *The Fair Notice Test as Applied by the D.C. Circuit*

As the fair notice doctrine is a creature of judicial creation, much like the common law doctrines of unconscionability, the exclusionary rule, and

---

41 *See* Rollins Envtl. Servs. Inc. v. EPA, 937 F.2d 649, 654 (D.C. Cir. 1991).

42 15 U.S.C. § 45(a)(1) (2006).

43 *Id.* § 45(n).

44 Precedent is somewhat unclear as to what level of deference courts give the FTC's legal standards under Section 5, but they do not seem to regularly use the *Chevron* analysis. Daniel A. Crane, *A Neo-Chicago Perspective on Antitrust Institutions*, 78 ANTITRUST L.J. 43, 62-63 (2012). In fact, the Supreme Court has stated "[t]he legal issues presented—that is, the identification of governing legal standards and their application to the facts found—are, by contrast, for the courts to resolve, although even in considering such issues the courts are to give some deference to the Commission's informed judgment that a particular commercial practice is to be condemned as 'unfair.'" FTC v. Ind. Fed'n of Dentists, 476 U.S. 447, 454 (1986). The Eleventh Circuit, relying on such precedent, recently stated, "[w]hile we afford the FTC some deference as to its informed judgment that a particular commercial practice violates the FTC Act, we review issues of law de novo." Schering-Plough Corp. v. FTC, 402 F.3d 1056, 1063 (11th Cir. 2005) (citing *Ind. Fed'n of Dentists*, 476 U.S. at 454). Courts generally do not afford *Chevron* deference to the FTC's interpretations of Section 5 in the antitrust context. Daniel A. Farber & Brett H. McDonnell, *"Is There a Text in this Class?" The Conflict Between Textualism and Antitrust*, 14 J. CONTEMP. LEGAL ISSUES 619, 656 (2005).

the good faith exception, it has different incarnations in different courts. The Supreme Court has not yet spoken on the nature and meaning of the fair notice doctrine, and, as demonstrated below, a uniform conception has not yet emerged. However, courts are increasingly familiar with the doctrine and its application. In particular, the D.C. Circuit has the most developed jurisprudence in this area and provides the strongest precedent, as the court has reviewed and accepted the fair notice defense in several instances. The doctrine as construed in the D.C. Circuit seems to best serve the doctrine's underlying purposes, namely, the protection of those regulated from being penalized after the fact for conduct whose legality likely could not be determined predictably at the time of the alleged violation. Other federal appellate courts seem to provide less protection.[45] For example, the Tenth Circuit seems to suggest that entities should be able to correctly adjust their behavior based solely on knowing the policy objectives of the law even when the agency's interpretations are unclear.[46] However, as this Essay discusses below in Part II, given the literal breadth of Section 5 and the FTC's efforts to foster best practices, in most cases entities subject to potential enforcement are confronted by a minefield where it can be nearly impossible to distinguish between advisable and required data-security behavior.

---

45 The Seventh Circuit observed, "[t]he regulations, while not models of clarity, should not have been incomprehensively vague to [the entity]." Tex. E. Prods. Pipeline Co. v. OSHRC, 827 F.2d 46, 50 (7th Cir. 1987). The court seems to require that when entities are faced with ambiguous interpretations, they should follow the more precautionary definition and interpret a regulation using a "common sense" approach even when the interpretation is unclear. *Id.* at 50; *see* Lin, *supra* note 31, at 1008-09. The Second, Ninth, and Tenth Circuits have used a test that asks whether "a reasonably prudent person, familiar with the conditions the regulations are meant to address and the objectives the regulations are meant to achieve, has fair warning of what the regulations require." Rock of Ages Corp. v. Sec'y of Labor, 170 F.3d 148, 156 (2d Cir. 1999); *see also* Walker Stone Co. v. Sec'y of Labor, 156 F.3d 1076, 1083-84 (10th Cir. 1998); Stillwater Mining Co. v. Fed. Mine Safety & Health Review Comm'n, 142 F.3d 1179, 1182 (9th Cir. 1998). The Tenth Circuit has indicated that entities should review the text and purpose of the law and consider the meaning of industry terms. *See Walker Stone*, 156 F.3d at 1082-84. However, the Fifth Circuit may be consistent with the D.C. Circuit and seems to have originated the "ascertainable certainty" test adopted by the D.C. Circuit. *See Gen. Elec.*, 53 F.3d at 1329 (citing Diamond Roofing Co. v. OSHRC, 528 F.2d 645, 649 (5th Cir. 1976)). The Fifth Circuit has also used a "reasonably clear" test: the government "must give an [entity] fair warning of the conduct it prohibits or requires, and it must provide a reasonably clear standard of culpability to circumscribe the discretion of the enforcing authority and its agents." *Diamond Roofing*, 528 F.2d at 649. For a detailed review of the tests, see Lin, *supra* note 31, at 1009-10.

46 *See Walker Stone Co.*,156 F.3d at 1083-84.

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

In *General Electric Co. v. EPA*,[47] the D.C. Circuit recognized that fair notice requires that a party must be able to determine with "ascertainable certainty" the agency's expectations. Fair notice requires that "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."[48] It also dictates that "[i]f, by reviewing the regulations and other public statements issued by the agency," such certainty exists, "then the agency has fairly notified a petitioner of the agency's interpretation."[49] Commentators suggest that the "ascertainable certainty" test of the D.C. Circuit provides almost as much protection to defendants in a civil context as that found in criminal cases.[50] This seems consistent with other due process considerations, given the deference afforded to agency interpretations under *Chevron*.

This Essay will discuss the factors the D.C. Circuit considers when applying the test, but the words "ascertainable certainty" themselves are not particularly clear. As Albert Lin observes, the word "ascertainable" may arguably imply that an entity has a duty to try to understand what is required, perhaps requiring an inquiry of the agency.[51] However, the court cases do not impose such a requirement. Rather, the D.C. Circuit reviews whether an agency has published an interpretation but not whether an entity has taken steps to resolve any lack of clarity with the agency. "Certainty" suggests "a level of definiteness,"[52] that the interpretation must be "fixed" or "settled." The court seems to focus on whether an agency has settled on an interpretation or has published conflicting interpretations. In all, the D.C. Circuit seems to focus on four factors when determining whether fair notice exists, which are each discussed below.

2. Factors of the D.C. Circuit's "Ascertainable Certainty" Test

Given that the D.C. Circuit has likely provided the most thorough review of the doctrine, this Essay will focus upon precedent from that court to analyze fair notice. Although the body of precedent interpreting "ascertainable certainty" continues to develop, several D.C. Circuit cases shed light on factors that influence a successful fair notice defense. The D.C. Circuit

---

47 53 F.3d 1324 (D.C. Cir. 1995).

48 *Id.* at 1329 (quoting *Diamond Roofing*, 528 F.2d at 649.).

49 *Id.* at 1329 (citing *Diamond Roofing*, 528 F.2d at 649.).

50 Lin, *supra* note 31, at 1011 ("[T]he fair notice test currently applied to civil regulations by the D.C. Circuit and the Fifth Circuit is nearly as stringent . . . as that in criminal cases.").

51 *Id.* at 1003.

52 *Id.*

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 had conflicting interpretations; and (4) the entity faces a serious penalty. The cases do not seem to require that an entity seek out any agency's interpretation, particularly when the agency itself has provided conflicting interpretations.[53]

a. *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 in determining a successful fair notice defense is whether a careful reading of the language of the law provides the necessary notice of the law's meaning.[54] "[W]here the regulation is not sufficiently clear to warn a party about what is expected of it"[55] the fair notice doctrine protects a party from government sanction. The language of the regulation provides proper notice only if it was "'reasonably comprehensible to people of good faith.'"[56] Where the law is silent or ambiguous and multiple interpretations exist, the D.C. Circuit has used the fair notice doctrine to protect parties from government sanctions in much the same way that it has used the *Chevron* doctrine to respect reasonable agency interpretations.

Several cases demonstrate that the D.C. Circuit reviews whether the law's text is silent or ambiguous and whether the interpretation made by the party subject to enforcement is plausible. A number of the cases reflect challenges to actions by the Federal Communications Commission ("FCC"). In particular, the D.C. Circuit has reviewed three FCC licensing cases where entities challenged the clarity of the FCC's license application rules. In each of the cases, the D.C. Circuit concluded that the text's interpretation was silent or ambiguous and that the entity's interpretation was a plausible one.[57] In other contexts, the D.C. Circuit also reviewed whether the rule or regulation and explanatory information was silent[58] or ambigu-

---

53 The FTC has had the authority to provide interpretive guidance in relation to some of the laws it enforces. For example, until recently the FTC could issue interpretive guidance related to the Fair Credit Reporting Act. Press Release, Fed. Trade Comm'n, FTC Issues Report: "Forty Years of Experience with the Fair Credit Reporting Act" (July 20, 2011), *available at* http://www.ftc.gov/opa/2011/07/fcra.shtm. Entities can petition the FTC to initiate a rulemaking proceeding, but to the Authors' knowledge, the FTC has not issued an interpretive guidance related to unfair acts or practices under Section 5.

54 *See* McElroy Elecs. Corp. v. FCC, 990 F.2d 1351, 1353, 62 (D.C. Cir. 1993).

55 Gen. Elec. Co. v. EPA, 53 F.3d 1324, 1328 (D.C. Cir. 1995).

56 *Id.* at 1330-31 (quoting *McElroy Elecs.*, 990 F.2d at 1358).

57 *McElroy Elecs.*, 990 F.2d at 1360; Satellite Broad. Co. v. FCC, 824 F.2d 1, 2 (D.C. Cir. 1987); Radio Athens, Inc. v. FCC, 401 F.2d 398, 402-03 (D.C. Cir. 1968).

58 United States. v. Chrysler Corp., 158 F.3d 1350, 1355 (D.C. Cir. 1998).

ous such that the language "obscures the agency's interpretation of the regulations sufficiently to convince [it] that [the entity] did not have fair notice."[59]

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

Because the fair notice doctrine is grounded in due process, its application will invariably focus on agency conduct relating to and surrounding the underlying enforcement activity. Potentially, agencies will point to many activities that might be instructive on their views. Whether these activities are authoritative depends on their context. In short, "[i]n many cases the agency's pre-enforcement efforts to bring about compliance will provide adequate notice,"[60] and courts will review public statements and actions, such as notices published in the Federal Register,[61] adjudicatory opinions,[62] previous citations,[63] and policy statements[64] to determine whether fair notice of an interpretation was given.

Citations imposing a monetary penalty likely do not provide fair notice. In *General Electric Co. v. EPA*, the D.C. Circuit stated in dicta that an agency provides adequate pre-enforcement notice when it informs a regulated party directly of the need to perform a required act or by publishing explanatory statements.[65] However, not all pre-enforcement efforts provide constitutionally proper and "fair" notice. Specifically, the Supreme Court has suggested that the use of a citation or other punishment including a monetary penalty to announce a particular interpretation may not be proper.

---

59 *Gen. Elec.*, 53 F.3d at 1328, 1331-32 (determining that the language of the statute was not explicit and observing that both parties had trouble identifying the applicable provisions); *see also* Rollins Envtl. Servs. Inc. v. EPA, 937 F.2d 649, 652 (D.C. Cir. 1991) (stating that "EPA's interpretation would not exactly leap out at even the most astute reader" while ruling that the language of the applicable regulation and the agency's explanatory report was ambiguous, because both the agency's and the entity's interpretations were equally plausible); Gates & Fox Co. v. OSHRC, 790 F.2d 154, 156 (D.C. Cir. 1986) (Scalia, J.) (holding that the unclear safety regulation could plausibly be read in multiple ways and failed to give fair notice).

60 *Gen. Elec.*, 53 F.3d at 1329.

61 *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).

62 *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).

63 *Id.* (finding that notice was provided when the agency previously cited the defendant for regulation violations).

64 *Gen. Elec.*, 53 F.3d at 1333 (reviewing an agency policy statement and concluding that notice was unclear).

65 *Id.* at 1329.

In *NLRB v. Bell Aerospace Co.*,[66] the Supreme Court allowed an agency to change its rule via an adjudication, in part, because no fines or damages were involved.[67] In *Martin v. OSHRC*,[68] the Supreme Court stated in dicta that deference to an agency interpretation may not be reasonable when an agency announces an interpretation through a citation with a monetary penalty.[69] Given this precedent, courts may hold that a citation imposing a monetary penalty would not provide fair notice to the defendant.[70]

Crucially, in order to meet fair notice requirements, agency guidance must originate from the agency as a whole. In *Gates & Fox Co. v. OSHRC*,[71] the D.C. Circuit held that guidance in interpreting a law must come from the authority of the agency as a whole, and not some other source, such as the opinion of a representative of the agency who may not be speaking for the agency as a whole.[72] To our knowledge, the D.C. Circuit has not analyzed whether a consent decree or settlement with an agency constitutes a reviewable interpretive document as part of the "ascertainable certainty" test. A court would need to determine whether the FTC's published complaints, consent orders, and guidance came from the FTC as a whole. If they did not, a court would not consider them a source of notice.

The D.C. Circuit reviews public statements and other sources of information published by the agency when the text of the agency's interpretation of a law is silent or ambiguous to help determine whether an entity received fair notice of the interpretation. Therefore, courts may consider the FTC's best practices guidance, its complaints, and consent orders as part of the fair notice analysis, because, as discussed below, these means of disseminating interpretive information are authorized by the agency as a whole and are not communicated along with a monetary penalty. However, as this Essay also discusses in detail below, there are both practical and policy challenges to whether these types of communications provide the type of authoritative notice that fairness and due process considerations require.

---

66 416 U.S. 267 (1974).

67 *Id.* at 295.

68 499 U.S. 144 (1991).

69 *Id.* at 158 (stating that "the 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").

70 This prohibition may not affect the FTC's usual procedure of issuing complaints and obtaining settlements with entities pursuant to alleged Section 5 violations, even when they include monetary remedies. Settlement agreements are voluntarily accepted by the entities involved, and the FTC's complaints are not citations that impose a monetary penalty. Therefore, courts may conclude that complaints and consent orders are not equivalent to citations imposing fines, damages, or other monetary penalties and may provide adequate pre-enforcement notice.

71 790 F.2d 154 (D.C. Cir. 1986) (Scalia, J.).

72 *Id.* at 157 (holding that notice of a violation given by a nonagency 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)

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

Assuming a court determines that the law and other authoritative pre-enforcement communications are ambiguous, a fair notice inquiry will include review of evidence concerning the presence of an agency's conflicting interpretations of the law. To determine whether an agency inconsistently interpreted a law, the D.C. Circuit has reviewed whether the agency published inconsistent documentation,[73] provided inconsistent advice to entities,[74] or otherwise acted inconsistently.[75] In situations where an agency did not provide any notice at all, courts likely would not require an examination of this factor. In each of the D.C. Circuit cases reviewed above, the agency always provided some interpretational notice,[76] which gave the court a basis for exploring potential inconsistencies.

If a court concludes that the FTC's published communications are authoritative and capable of providing fair notice, it may look at whether the communications contain inconsistencies. Courts may also review whether the agency has provided inconsistent data-security-related advice to entities or acted inconsistently, such as by filing complaints in some data-security cases but not others when the facts appear to be similar. In cases where an interpretation sufficiently authoritative and a court does not find inconsistencies, the court will likely find that fair notice is present.

---

73 *See* Darrell Andrews Trucking, Inc. v. FMCSA, 296 F.3d 1120, 1130 (D.C. Cir. 2002) (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."); United States v. Chrysler Corp., 158 F.3d 1350, 1356 (D.C. Cir. 1998) (concluding a prior schematic illustrating testing procedures conflicted with the EPA's current interpretation of the testing standard and stating, "an 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").

74 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); Rollins 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).

75 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).

76 *See supra* notes 73-75 (discussing generally the agencies' interpretations).

d. *Imposition of a Serious Penalty*

Due process requires that parties receive fair notice before being deprived of property, such as through the imposition of a fine,[77] the denial of a license application,[78] or by requiring an entity to take costly action.[79] The D.C. Circuit has stated that "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."[80]

In cases involving Section 5, a reviewing court must ascertain whether the FTC's remedies constitute a serious penalty. The D.C. Circuit seems to have an inclusive view of this requirement. The case law reflects that the imposition of a direct monetary fine or an agency action that indirectly results in a loss of business or an expenditure of funds, such as the denial of a licensing application or a vehicle recall by an automobile manufacturer, constitutes a serious penalty that warrants fair notice analysis. Therefore, even though the FTC has limited remedial powers unless an entity has violated an order, a reviewing court would determine whether those powers can be used to enforce a serious penalty.

The fair notice doctrine seeks to ensure that regulated entities have a clear interpretation of applicable law to guide their compliance efforts where substantial penalties may apply. Although courts have differing tests for determining the existence of adequate fair notice, a fairly clear set of requirements for agency conduct appears to have emerged from D.C. Circuit precedent. That court's "ascertainable certainty" test provides a useful means of analyzing recent FTC activities in the area of information security and highlighting challenges and complications to the agency's exercise of its Section 5 authority.

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

In Section 5, Congress gave very broad powers to the FTC to protect consumers from deceptive and unfair trade practices. The FTC has begun

---

77 *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").

78 *McElroy Elecs.*, 990 F.2d at 1363; *Satellite Broad.*, 824 F.2d at 2; *Radio Athens*, 401 F.2d at 403.

79 United States v. Chrysler Corp., 158 F.3d 1350, 1355 (D.C. Cir. 1998) (ruling that a vehicle recall would have required expenditure of significant amounts of money depriving Chrysler of property).

80 *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))).

using its "unfairness" authority to investigate and punish what it believes are companies' faulty data-security practices.

The FTC recently filed a complaint against Wyndham Worldwide Corp. and its affiliates (collectively "Wyndham") alleging that Wyndham's failure to employ reasonable and appropriate data-security measures constituted an unfair act or practice in violation of Section 5.[81] Wyndham sought dismissal of the case arguing that the FTC's unfairness authority does not extend to data security.[82] Significantly, Wyndham also argued that the FTC had not previously provided fair notice of what data-security practices would meet the standards required by Section 5.[83]

This Essay will review the FTC Act and the FTC's public activity related to data security to illustrate fair notice considerations under the D.C. Circuit's "ascertainable certainty" test. The Essay will use the Wyndham case as a tool for the analysis[84] and assess whether the notice provided by the FTC is in fact "fair."

A. *The FTC's "Unfairness" Authority*

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[85] 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."[86] To be a substantial injury, it must be significant in magnitude and actual (i.e., the harm has occurred or is imminently threatened).[87] Consumer injury may involve either causing very severe harm to a small number of people or "a small harm to a large

---

81 First Amended Complaint for Injunctive and Other Equitable Relief at 19, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-PHX-PGR (D. Ariz. Aug. 9, 2012) [hereinafter Wyndham First Amended Complaint].

82 Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC at 6-10, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-PHX-PGR (D. Ariz. Aug. 27, 2012) [hereinafter Wyndham Motion to Dismiss].

83 *Id.* at 10-11.

84 The Authors understand that the *Wyndham* case currently resides in the New Jersey district court within the Third Circuit; however, because the fair notice doctrine is more mature in the D.C. Circuit, analysis under its test better serves this Essay's goals of highlighting existing challenges for companies and practitioners and exploring additional alternatives.

85 15 U.S.C. § 45(a)(1) (2006).

86 *Id.* § 45(n).

87 Letter from the FTC to Hon. Wendell H. Ford and Hon. John C. Danforth, Committee on Commerce, Science, and 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).

number of people."[88] The two forms of injury that generally qualify under the "unfairness" test are economic harm and harm to health or safety.[89]

1. The FTC's Use of "Unfairness" Authority

The law's breadth has been used by the FTC to regulate a wide range of business practices, such as the production of unsafe farm equipment,[90] online check drafting and delivery,[91] business opportunity scams,[92] weight-loss products,[93] sales techniques,[94] billing techniques,[95] and telephone billing processors.[96]

This Essay does not challenge the FTC's use of its unfairness authority in cases where the alleged unfair practices and harm to consumers are clear. For example, in *In re International Harvester Co.*,[97] the FTC found that tractors would "geyser" fuel in certain situations causing fires and human injuries and the defendants knew of the hazard for seventeen years.[98] More recently, the FTC has investigated companies that "crammed" charges onto consumers' telephone bills. In *FTC v. Inc21.com Corp.*,[99] the defendant allegedly "crammed" millions of dollars of unauthorized charges onto thousands of telephone bills.[100] In these cases, the FTC likely does not need to provide notice that knowingly selling farm equipment with hidden hazards or stealing money from others is "unfair." In addition, the alleged consumer injuries are clear and substantial.

The same cannot be said for "unfair" data-security practices. While the Authors can agree that entities do not likely need more notice that a complete lack of data security may be "unfair," what data security is necessary to make it "fair" is unknown. This is not as clear as concluding that "spewing gasoline is 'unfair,' and not spewing gasoline is 'fair,'" or "unauthorized charges are 'unfair,' and authorized charges are 'fair.'" In addition, the cases we reviewed above indicate easy to find consumer harm–burn injuries

88 FTC v. Neovi, Inc., 604 F.3d 1150, 1157 (9th Cir. 2010).

89 *Int'l Harvester*, 104 F.T.C. at 1086.

90 *Id.* at 954.

91 *Neovi*, 604 F.3d at 1153.

92 FTC v. Stefanchik, 559 F.3d 924, 926 (9th Cir. 2009).

93 FTC v. Garvey, 383 F.3d 891, 893 (9th Cir. 2004).

94 *In re* Carpets "R" Us, Inc., 87 F.T.C. 303, 323 (1976) (labeling high pressure sales tactics as an unfair trade practice); *see also*, Tashof v. FTC, 437 F.2d 707, 709 (D.C. Cir. 1970) (describing "a 'bait and switch' maneuver" in an eyeglasses sales campaign).

95 *E.g.*, Direct Marketing Concepts, Inc., No. Civ.A.04-11136-GAO, 2004 WL 1399185, at *5 (D. Mass. June 23, 2004) (describing a scheme which billed credit cards without authorization).

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

97 104 F.T.C. 949 (1984).

98 *Id.* at 1051.

99 745 F. Supp. 2d 975 (N.D. Cal. 2010).

100 *Id.* at 982.

and stolen money. However, in the vast majority of data-security cases, the harm may be more difficult to determine. In fact, courts have wrestled with whether the loss of personal information constitutes a cognizable harm to consumers without evidence of actual damages.[101] Actual damages resulting from a particular data loss incident can be hard to ascertain. No harm may result even when credit card numbers are compromised because consumers are refunded for any fraudulent charges made to their account. Given that the harm is less clear, fair notice is even more essential.

2. The FTC's Section 5 Enforcement and Penalty Structure

When the FTC identifies an "unfair" practice, it has two choices for enforcing Section 5 against the party using the practice. The FTC can follow an administrative process and issue cease-and-desist orders, which commonly result in consent orders.[102] Alternatively, the FTC can file complaints in court seeking injunctions and consumer redress against defendants for alleged violations of Section 5.[103]

Most commonly, in the areas of privacy and data security, rather than litigate cases to a conclusion, the agency follows the administrative process to enter into consent orders with defendants. Consent orders must be approved by the full Commission and are subject to notice and public comment before they become effective.[104] The consent orders in the privacy and data-security context typically govern an entity's behavior for 20 years.

The FTC can seek a monetary penalty when a defendant violates a consent order to which it agreed pursuant to an alleged Section 5 viola-

---

101 In the class action context, plaintiffs have faced obstacles in meeting standing requirements when they claim 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. The Supreme Court recently enunciated a strict test for standing when plaintiffs allege a risk of future harm, stating that future harm must be "certainly impending" or at least pose a "substantial risk" for it to confer standing. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143, 1150 n.5 (2013). Moreover, the Court rejected the plaintiffs' efforts to alleviate the alleged risk of future harm as a basis for standing, stating that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.* at 1151. We expect *Clapper* to be cited in motions to dismiss in class action litigation involving data breaches for the foreseeable future. Federal 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 KJM-DAD, 2012 WL 174961, at *2 (E.D. Cal. Jan. 20, 2012), *and* Low v. LinkedIn Corp., No. 11-CV-01468-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).

102 15 U.S.C. § 45(b)-(c), (g) (2006).

103 *Id.* § 53(a)-(b).

104 16 C.F.R. § 2.34 (2012).

tion.[105] Any violation of a consent order can result in civil penalties of up to $16,000 per violation,[106] and "[e]ach separate violation . . . [is] a separate offense, except that in a case of a violation through continuing failure to obey or neglect to obey a final order of the Commission, each day of continuance of such failure or neglect shall be deemed a separate offense."[107] Under this violation calculus, violations and fines can accumulate quickly. In essence, entities have potentially ruinous penalties hanging over their heads for 20 years after entering into a consent order.

For example, the FTC recently 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.[108] The result was the FTC's largest fine ever for an order violation: $22.5 million.[109] In its complaint, the FTC alleged that each time Google made a misrepresentation to a user, Google violated the order.[110] 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. A $16,000 fine for each of a million users would result in a very large civil penalty. Clearly, these penalties are serious and fair notice on how to avoid them seems warranted.

B. *The FTC Uses Section 5 of the FTC Act to Investigate Alleged Lack of Proper Data-Security Safeguards*

Given that penalties are serious and "unfair" data-security practices are not as clear as in other actions the FTC takes using its "unfairness" authority, "fair notice" is even more important. Although authorized to do so under the FTC Act, the FTC has never used formal rulemaking to explain Section 5's application to data security. Generally, agencies have discretion to choose between rulemaking and enforcement to implement their statutory responsibilities when Congress gives them the powers.[111] The FTC Act

---

105 15 U.S.C. § 45(l).

106 Section 5(1) of the FTC Act, 15 U.S.C. § 45(1) (2006), as modified by the 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.

107 15 U.S.C. § 45(l).

108 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).

109 *Id.* at 2.

110 *Id.* at 7.

111 *See* SEC v. Chenery Corp., 332 U.S. 194, 203 (1947). Congress may limit or provide rulemaking and/or enforcement authority. *Id.* at 196, 207.

grants the FTC both rulemaking and enforcement authority under Section 5, although the agency's rulemaking authority is limited.[112] The FTC's rulemaking authority, which is commonly referred to as Magnuson-Moss rulemaking,[113] includes additional requirements that are more cumbersome than the more widely known APA process. For example, though not required under the APA, the FTC Act requires the FTC to "provide for an informal hearing" where interested parties are entitled to present oral testimony and potentially cross-examine witnesses.[114]

Due to this potentially inefficient and time consuming process, the FTC has not used its rulemaking authority to issue rules related to data security.[115] Instead, the agency has used an enforcement approach to implement its policy, and in at least some circles the agency's work in privacy and data security has been referred to as creating an emerging "common law" of privacy.[116]

Like formal rulemaking, the FTC has also declined to clarify Section 5's application to data security through formal adjudication. According to the FTC, it has brought forty-two data-security enforcement actions since 2000.[117] Seventeen of those actions alleged unfair practices.[118] The FTC publishes information about its enforcement activities, including the details of the complaints and consent orders.[119] However, none of the cases resulted in formal adjudications by the FTC or the courts. Instead, each resulted in a settlement agreement with the respective defendants.

While declining to make use of formal means of clarifying its interpretation of Section 5, the FTC publishes complaints and consent orders, which may provide some notice of its interpretive standard. The FTC's data-security-related complaints frequently use terms like "reasonable," "appropriate," "adequate," or "proper" to describe the security safeguards that the agency maintains are required under Section 5. There are no rules or regulations that explicitly define the type or nature of safeguards satisfying

---

112 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.").

113 *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).

114 15 U.S.C. § 57a(b)-(c).

115 *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 these rules in a more timely and efficient manner.").

116 *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/120427loyolasymposium.pdf.

117 Wyndham FTC Response, *supra* note 7, at 7. In addition, the FTC thereafter brought an action against HTC America.

118 *Id.*

119 *Id.*

those requirements. The FTC has, along with the general standards, included many detailed data-security-related allegations in its complaints which form the basis of the underlying consent orders. These complaints have alleged that Section 5 was violated due to a 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.[120] However, these complaints do not provide a blueprint for entities to follow because the FTC cryptically states that the failures "taken together" violate Section 5, and each complaint lists different data-security practices.

The FTC also typically requires entities subject to a consent order involving data-security matters to implement the data-security practices it announces in its consent orders.[121] These data-security practices may also give entities some notice of what the FTC believes is required by Section 5. Consent orders resulting from data-security investigations usually include a requirement for the defendant to implement a "comprehensive information security program."[122] The imposed program typically includes: designating employees responsible for data security; implementing reasonable safeguards to protect against identified security risks, including prevention, detection, and response to intrusions; implementing privacy controls appropriate for the business, data use, and sensitivity of the information; and regular testing, monitoring, and adjusting of privacy controls.

To reiterate, no formal rulemakings or adjudications related to data security have occurred to date, and the FTC seems to regulate data security primarily through complaints and consent orders. This method creates ambiguity because complaints and consent orders differ when identifying noncomplying practices and imposing data-security safeguards. It is unclear whether nonparties to the investigation should attempt to follow the complaint, the consent order, or both when complying with Section 5, or whether the failure to implement some or all of the measures would result in a prohibited unfair practice. Additionally, the complaints may lack clarity regarding the particular type and sensitivity of information involved, which

---

120 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).

121 *Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 111th Cong. 9-11 (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.").

122 *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, *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.

makes distinguishing between required and simply *advisable* actions more difficult for nonparties to ascertain.[123]

This inherent ambiguity can be dangerous for regulated entities due to the potentially serious penalties that can result. Under Section 5, the FTC can issue a cease-and-desist order or request that a court enter an injunction.[124] Either a cease-and-desist order or an injunction involving data security can dramatically affect businesses—particularly small Internet companies whose entire business is based on data.

C. *The FTC's Public Statements*

As discussed above, the FTC has not issued any formal regulations or rules related to data security under Section 5. However, 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."[125]

In addition to the complaints and consent orders described above, the FTC has issued guidance describing data-security practices. For example, in *Protecting Personal Information: A Guide for Business*, the FTC lists thirty-six detailed recommendations related to network security, password management, laptop security, firewall usage, wireless and remote access, and detection of data breaches.[126] Many of the recommendations listed in this publication also appear in the FTC's complaints, including the complaint filed against Wyndham.[127] The guidance also explains that "[s]tatutes

---

123 Notably, the Commission uses what is commonly referred to as "fencing-in" relief, to directly regulate the conduct of entities under order in a broad and comprehensive manner. "Fencing-in" relief allows the FTC to use orders to deal with more than just the entity's specific allegedly illegal action. The Commission can also include prohibitions of related actions that would violate Section 5. This expansion allows the Commission to obtain a monetary penalty for a violation of an order for activity similar to the original violation. *See generally* John E. Villafranco, Katie Bond & Raqiyyah R. Pippins, *The FTC's New Take on Health-Related Advertising: What Companies Facing FTC Enforcement Need to Know*, UPDATE MAG., Sept.-Oct. 2010, at 27-28. Therefore, understanding whether or not the breadth of such obligations within the broader "fence-line" of an order should be reasonably read to reflect requirements under Section 5 for nonparties can be daunting to businesses and their counsel.

124 15 U.S.C. § 53(b) (2006) (stating that the court may issue a temporary restraining order, preliminary injunction, or permanent injunction); Michael J. Pelgro, Note, *The Authority of the Federal Trade Commission to Order Corrective Advertising*, 19 B.C. L. REV. 899, 907 (1978).

125 Wyndham FTC Response, *supra* note 7, at 13.

126 FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS 9-17 (2011), *available at* http://business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf. The publication seems to have existed since 2007 and was most recently updated in November 2011.

127 Complaint for Injunctive and Other Equitable Relief at 10-12, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-PHX-PGR (D. Ariz. Aug. 9, 2012) No. 2:12-cv-01365-SPL (D. Ariz. June 26, 2012) [hereinafter Wyndham Complaint].

like . . . the Federal Trade Commission Act may require you to provide reasonable security for sensitive information"[128] although the statute neither refers to "security" nor provides any explanation of what "sensitive information" is.[129]

Beyond complaints, consent orders, and agency guidance in the form of reports, the FTC has also been a leader in using the Internet and social media to provide information regarding the law and best practices. For example, an FTC website 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 your security practices are reasonable will depend on the nature and size of your business, the types of information you have, the security tools available to you based on your resources, and the risks you are likely to face.[130]

In practice, as discussed in detail below, this standard provides very little, if any, information on what entities must do. It also fails to address a practical reality—implicitly recognized by the agency, nonetheless—that the ever-evolving nature of technology creates a moving target for agency enforcement *as well as* entity compliance.

D. *The* Wyndham *Case*

Amidst the FTC's ongoing efforts to focus on the emerging areas of privacy and data-security policymaking and law enforcement, many practitioners privately wrung their hands at their inability to identify and ascertain what security practices are required versus those which are simply advisable. Against this background of widespread uncertainty, the agency took an increasingly aggressive tack with entities as it sought to vigorously protect consumers in its role as the federal law enforcement agency directly responsible for consumer protection. Indeed, as FTC Chairman Jon Leibowitz stated at a workshop on the privacy implications of facial recog-

---

128 FED. TRADE COMM'N, *supra* note 126, at 5.

129 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.

130 Burke Kappler, *Protecting Personal Information–Know Why*, BUREAU OF CONSUMER PROT. BUS. CTR. (Oct. 2007), http://business.ftc.gov/documents/art08-protecting-personal-information-know-why.

nition, "[t]o be sure, the FTC will vigorously enforce the law if we see a violation [of people's privacy rights]."[131] Unfortunately, identifying both the concrete requirements of the law as well as the nature and scope of consumers' privacy rights remain daunting and problematic tasks for all involved parties.

Until recently, the agency's enforcement actions had one of two outcomes: (1) the agency determined not to go forward with adjudication, in which case the public or others seldom learned anything about the nature or breadth of the agency's inquiries; or (2) a consent order was entered into under terms and conditions similar to those described above. Until Wyndham, no other outcome had emerged.[132] This dynamic of public and private pressure on investigated organizations, coupled with the nature and requirements of the consent orders, created an atmosphere that favored settlement for financial, public relations, legal, and related resource considerations. Nonetheless, private concerns and discussion persisted among companies and practitioners plagued with a simple recurring complaint: "How are we supposed to know what we are supposed to do without any notice or standard that we can understand?" Likely spurred by this frustration, the Wyndham matter suggests a new, third potential outcome, a litigated challenge to the agency's authority and practices.

Wyndham suffered three separate data breaches between April 2008 and January 2010.[133] After the parties were unable to resolve the matter successfully by either the FTC closing the investigation or the parties entering into a mutually acceptable consent order, the agency filed suit. The FTC's complaint alleges that the intrusions resulted in unauthorized access to personal information, including credit card numbers, stored on Wyndham's network.[134]

The complaint further alleges that Wyndham performed unfair acts or practices by "fail[ing] to employ reasonable and appropriate measures to protect personal information against unauthorized access" and that Wyndham's alleged failures "caused or are likely to cause substantial injury to consumers."[135]

---

131 Jon Leibowitz, Chairman, Fed. Trade Comm'n, Opening Remarks at Face Facts Forum: A Forum on Facial Recognition Technology 4 (Dec. 8, 2011), *available at* http://htc-01.media.qualitytech.com/COMP008760MOD1/ftc_web/transcripts/120811_FTC_sess1.pdf.

132 *See, e.g.*, Letter from Joel Winston, Acting Assoc. Dir., Fed. Trade Comm'n Bureau of Consumer Prot., to Christine Varney, Hogan & Hartson (Jan. 22, 2001) (closing investigation without consent order), *available at* http://www.ftc.gov/os/closings/staff/doubleclick.pdf; Twitter Decision & Order, *supra* note 122.

133 Wyndham First Amended Complaint, *supra* note 81, at 12. Wyndham disputes that it is liable for the acts of its franchises, which were the original victims of the data breach. For the purposes of this analysis, the Authors will assume "Wyndham" had a data breach.

134 *Id.* at 12-13, 18; *see supra* note 133.

135 Wyndham First Amended Complaint, *supra* note 81, at 19.

The FTC alleged that the following practices, "taken together," unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft:

* Failing to use readily available security measures to limit access between affiliate and franchise networks;

* Storing payment card information in clear readable text;

* Failing to implement adequate information security policies and procedures;

* Failing to remedy known security vulnerabilities;

* Using easy to hack passwords;

* Failing to adequately inventory computers connected to its network;

* Failing to employ reasonable measures to detect and prevent unauthorized access to Wyndham's network or to conduct security investigations; and

* Failing to adequately restrict vendor's access to the network.

Wyndham filed a motion to dismiss the FTC's complaint arguing, in part, that "the FTC is enforcing its vision of data-security policy through this selective, *ex post* enforcement action, which seeks to hold [Wyndham] liable without any fair notice as to what the law required."[136] Wyndham argued that this "approach . . . subject[s] businesses to vague, unpublished, and uncertain requirements."[137]

E. *Applying the Fair Notice Doctrine to the FTC's Interpretation of Section 5*

The Wyndham case's timing highlights the nature and role of the fair notice doctrine and its implications for (1) the FTC's authority and enforcement and (2) the agency's goal of achieving sustainable workable mechanisms for protecting consumers in the areas of privacy and data pro-

---

136 Wyndham Motion to Dismiss, *supra* note 82, at 3. Wyndham has two primary arguments: (1) the FTC does not have the authority under Section 5 to regulate data security at all; and (2) Wyndham clearly disclaimed liability for the data security of its franchises in its Terms of Service and so it cannot be liable for its franchises' lack of adequate data security. *Id.* at 5.

137 *Id.* at 3.

tection. This Essay points this out because it takes no position on the agency or industry's conduct, but rather focuses on the practical problem it perceives: The FTC's existing tools may be inadequate to address perceived data-security concerns in an effective and fair manner for all concerned. The Wyndham litigation is significant, as a policy matter, not because of its particular facts but because the agency chose to litigate the case and therefore test its authority in this area in light of its actions over the past decade. Many businesses, especially those subject to investigation, and those who advise them, are less than satisfied with current enforcement approaches because the resultant unpredictability confounds established risk management models.

Analyzing the facts of the Wyndham complaint under the D.C. Circuit's "ascertainable certainty" fair notice test represents, this Essay believes, the best lens through which to view the underlying difficulties faced by the agency and by those entities it regulates in figuring out whether and what protection of information is *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 had conflicting interpretations; and (4) the entity faces a serious penalty. This Essay will analyze Section 5 using the D.C. Circuit's test below to shed further light on the issue of fair notice in data-security cases.

1. Section 5 Is Silent on Data Security

The text of Section 5 prohibits "unfair or deceptive acts or practices in or affecting commerce."[138] Congress intentionally used broad language so the FTC could address unanticipated practices in a changing economy.[139] 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.

2. The FTC Publications Are Advisory and Unclear

The statutory language does not provide clarity on legally required data-security safeguards. Therefore, whether other agency statements or activities have provided fair notice takes on added significance. In particular, a reviewing court should not confine its inquiry to a limited search for the

---

138 15 U.S.C. § 45(a)(1) (2006).

139 *See* 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.").

existence of some document listing information that could be labeled "actual notice," because in most cases there will be some facts that suggest the existence of *some* notice. Rather, a reviewing court should focus upon whether the provision of notice through methods such as recommendations and consent orders constitutes *fair* notice and satisfies due process. The FTC's methods of providing notice do not necessarily provide fair notice.

The D.C. Circuit conducts a broad inquiry. Previously, it has reviewed regulatory guidance and notices of proposed rulemaking published in the Federal Register,[140] adjudicatory opinions,[141] and agency policy statements.[142] These methods of information dissemination are unquestionable statements by the agency about how it intends to interpret the laws it is obliged to enforce. These publications are also sources organizations may be expected to review. Conversely, providing information through settlements with individual parties and in a set of recommendations posted on an agency website does not seem to rise to the same level of importance and organizational awareness of these information sources is likely limited.[143]

a. *The FTC Has Not Published Notice in the Federal Register*

Although the D.C. Circuit will review notices published in the Federal Register, the FTC has not published any form of notice there. The Federal Register is the official publication that documents agency action.[144] It contains agency rules and regulations, proposed rules, and public notices and announcements.[145] In several cases, the D.C. Circuit reviewed information published in the Federal Register, including regulatory guidance and notices of proposed rulemaking.[146] The FTC has not issued any guidance or notices in the Federal Register to explain what it deems to be adequate data security under Section 5.

---

140 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).

141 *Darrell Andrews Trucking*, 296 F.3d at 1130-32.

142 Gen. Elec. Co. v. EPA, 53 F.3d 1324, 1333 (D.C. Cir. 1995).

143 More practically, the question of what types of agency activity should be deemed authoritative for purposes of fairness analysis has not been addressed by the courts in ways similar to *Chevron* and *Mead* regarding agency deference.

144 *Federal Register*, U.S. GOV'T PRINTING OFFICE, http://www.gpo.gov/fdsys/browse/collection.action?collectionCode=FR (last visited Mar. 17, 2013).

145 *Id.*

146 *See, e.g.*, *Darrell Andrews Trucking*, 296 F.3d at 1130-32.

b. *The FTC Has Used Only Informal Adjudicatory Processes*

Agency adjudications are formal actions by an agency, which are typically closely scrutinized by the entities regulated by that agency.[147] These adjudications may provide precedential value, and entities are aware that adjudications are policymaking tools for agencies. Therefore, entities may be expected to be aware of relevant agency adjudications.

The FTC has not issued any adjudicatory opinions expressing its view on what data-security practices are required under Section 5. Instead, as sources of notice, the agency points to the collection of published complaints and the attendant consent orders describing an entity's particular data-security practices the FTC has deemed inadequate.[148] The commissioners of the FTC vote to approve a complaint and consent order,[149] so a court may conclude that both sources are subject to consideration under the "ascertainable certainty" test as guidance from the agency as a whole. The complaints usually provide detailed descriptions of the allegedly faulty practices, such as the lack of a firewall, strong passwords, and an intrusion detection system. In fact, the Wyndham complaint repeats many, if not all, of the unfair data-security practices alleged in prior complaints. The consent orders published by the FTC describe what it believes are adequate information security programs; however, the discussion is not as detailed as the complaint.

The 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. Instead, the complaints simply list what the FTC believes are faulty data-security practices in one particular case. The circumstances of each case are different, and the FTC has not explained why data-security practices in one case may violate Section 5 while those same practices may not violate Section 5 in another case. The FTC apparently expects entities to piece together the complaints and consent orders in thirty-six cases,[150] without any authoritative commentary, to arrive at the FTC's interpretation of adequate data-security practices under Section 5. Moreover, the consent orders are settlement agreements among the parties and have no legal bearing, precedential or otherwise, on third parties. An agency can expect an

147 *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").

148 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 Mar. 17, 2013).

149 16 C.F.R. § 2.34 (2012).

150 Thirty-six data-security cases were brought under the FTC Act. Wyndham FTC Response, *supra* note 7, at 7.

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 concerns of fundamental fairness.

c. *The FTC Has Not Published Any Policy Statements*

In addition to not using the Federal Register or formal adjudication, the FTC has not made use of published policy statements. In *General Electric Co. v. EPA*, the D.C. Circuit reviewed an FCC policy statement as part of its analysis to determine whether fair notice had been provided.[151] The FCC's policy statements describe principles the agency would follow in its policy-making activities.[152] These policy statements are intended to notify entities of how an agency will view the entities' practices in light of the law. The FTC has not published any policy statements providing its interpretation of the data-security practices that Section 5 requires.

d. *Fair Notice Analysis of the FTC's Best Practices Guide*

The FTC has published an agency-authorized best practices guide for how businesses should protect data.[153] The guide provides thirty-six detailed recommendations. Generally, a subset of these recommendations is repeated in the FTC's complaints alleging faulty data-security practices. Of course, these are recommendations and not the law, and the FTC has not explicitly stated that the recommendations listed in the publication are the focus of its data-security investigations under Section 5.

Although the D.C. Circuit has not had an occasion to analyze whether an agency's best practices guide provides fair notice of unlawful conduct, it seems likely that a reviewing court might consider the FTC's best practices guide in its analysis. The D.C. Circuit has considered formal guidance published in the Federal Register and whether agency staff has provided advice inconsistent with the text of the law or with staff members. Given that the D.C. Circuit reviews "public statements issued by the agency,"[154] it would likely consider the FTC's informal guidance. However, courts may not give such guides great weight in determining whether the FTC has provided fair

---

151 Gen. Elec. Co. v. EPA, 53 F.3d 1324, 1333 (D.C. Cir. 1995).

152 *See, e.g.*, Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, 20 FCC Rcd. 14,986 (2005) (policy statement), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf.

153 FED. TRADE COMM'N, *supra* note 126, at 9-17.

154 *Gen. Elec.*, 53 F.3d at 1329.

notice of its expected data-security practices under Section 5, given that it is only a set of recommendations.

As an introductory matter, in *Gates & Fox Co. v. OSHRC*, the D.C. Circuit required that an interpretation capable of providing fair notice must be issued by the agency as a whole and not just be the opinion of a representative of the agency.[155] Given that the FTC, as an agency, authorized the publication of the guide, it likely passes this requirement.[156] Beyond a simple source check of the interpretation, *Gates & Fox Co.*, *Chevron*, and *United States v. Mead Corp*.[157] all hit on an important point.[158] An interpretation in and of itself is not necessarily sufficient to provide fair notice. The interpretation must come from a position of authority to truly provide fair notice. Unlike the guide which was authorized by the FTC as a whole, the staff attorney's Internet postings related to the guide; discussing data security does not represent the agency and would not likely be considered by a court in its fair notice analysis.

The guide would not likely warrant *Chevron* analysis, which further suggests that it is not a strong interpretational authority in the fair notice context. Although not precisely analogous, the nature and role of informal guidance and the deference and weight it should receive has been the subject of litigation. The Supreme Court in *United States v. Mead Corp*. discussed agencies' various methods of action, some of which explicitly or implicitly interpret laws.[159] Courts use a spectrum to determine how much

---

155 *See* Gates & Fox Co. v. OSHRC, 790 F.2d 154, 157 (D.C. Cir. 1986) (Scalia, J.).

156 *See id.*

157 533 U.S. 218 (2001).

158 *See id.* at 234 (holding an agency interpretation to be "beyond the *Chevron* pale"); Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 842-44 (1984); *Gates & Fox*, 790 F.2d at 156-57.

159 *Mead Corp.*, 533 U.S. at 235-36. Under *Mead*, regulations and rulings produced by express Congressionally-authorized rulemaking or adjudication deserve *Chevron* deference, but interpretations by agencies without such authorization do not deserve any deference. *Id.* at 229-30. Sometimes less formal interpretive procedures also deserve *Chevron* deference. *Id.* at 230-31. In such a case, courts should review whether Congress intended the agency to issue interpretations with the force of law. *Id.* at 231-32. Courts should also review whether a statutory interpretation binds just the parties to a ruling or binds all parties required to comply with the statute. *Id.* at 232-33. Finally, courts should consider whether the agency, as a whole, issued the interpretation or whether it was simply one of many made by agency staff. *Id.* at 233-34. The Court noted explicitly that "'interpretations contained in policy statements, agency manuals, and enforcement guidelines,'" as well as opinion letters do not deserve *Chevron* deference because they lack the force of law. *Id.* at 234 (quoting Christensen v. Harris Cnty., 529 U.S. 576, 587 (2000). Even if a court does not grant *Chevron* deference to an agency interpretation, the interpretation may still receive " respect," particularly when an agency has specialized experience regarding the matter. Skidmore v. Swift & Co., 323 U.S. 134, 140 (1944). The deference under *Skidmore* is based on "the thoroughness evident in its consideration, the validity of its reasoning, its consistency with earlier and later pronouncements, and all those factors which give it power to persuade." *Id*. In essence, whether or not an agency interpretation is entitled to deference under *Chevron* requires an inquiry into whether the interpretation carries (or should carry) the force of law.

deference to give to the agency's interpretation of the laws it enforces. On one end of the spectrum are formal rulemaking and adjudication and some informal actions where the agency is afforded *Chevron* deference.[160] On the other end of the spectrum are interpretations made by agencies that have not been given sufficient authority by Congress. Those interpretations are granted no deference.[161] To determine whether *Chevron* deference is appropriate for interpretations made outside of formal rulemaking or adjudications, courts look at: (1) whether Congress intended the agency to interpret the statute with the force of law; (2) whether the agency action binds individual parties to a ruling or whether it applies to third parties; and (3) whether the interpretation is made by the agency as a whole or by agency staff on an ad hoc basis.[162] The Court explicitly noted 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.[163]

For this Essay's purposes, *Mead* is instructive in analyzing the authority with which an agency speaks through its various methods of action. Courts will find that an agency acts with more authority when it publishes information through a formal rulemaking or adjudication process. As action becomes less formal, courts will weigh other factors to determine whether the agency is acting with authority that merits *Chevron* deference. The FTC's data-security best practices guide is not the result of a formal rulemaking or adjudication process. For this reason, a court would likely apply the factors in *Mead* to determine whether *Chevron* deference is appropriate. The FTC issued the best practices guide as part of its Section 5 authority, where Congress has given the agency the authority to interpret the statute with the force of law, and the guide is issued by the agency as a whole. However, a best practices guide does not bind any parties, as it is simply a list of recommendations. It is more like the policy statements, agency manuals, enforcement guidelines, and opinion letters that do not deserve *Chevron* deference. In light of these mixed factors and their similarity to the types of interpretations not deserving of *Chevron* deference, courts would not likely give *Chevron* deference to the interpretations in a best practices guide.[164] At most the guide may warrant a "'measure of respect'" but would not be strong authority for the agency's policy position.[165] Therefore, given

---

160 *Mead Corp.*, 533 U.S. at 229-30.

161 *See id.* at 231.

162 *See id.* at 231-34.

163 *Id.* at 234; *Christensen*, 529 U.S. at 587.

164 *See* Fed. Express Corp. v. Holowecki, 552 U.S. 389, 399 (2008) (granting an agency's policy statement a "'measure of respect'" (quoting Alaska Dep't of Envtl. Conservation v. EPA, 540 U.S. 461, 488 (2004))); Wash. State Dep't of Soc. & Health Servs. v. Guardianship Estate of Keffeler, 537 U.S. 371, 385 (2003) (holding agency operating manual "warrant[s] respect").

165 *See Holowecki*, 552 U.S. at 399 (quoting *Alaska Dep't of Envtl. Conservation*, 540 U.S. at 488). Under *Mead*, agency deference increases as the formality and use of Congressionally-authorized power

the lower level of court deference and the implication of lesser authority of the guide, the guide may not provide fair notice of what Section 5 requires.

e. *Concerns Stemming from the Lack of Concrete and Authoritative Notice*

Beyond its admittedly numerous consent orders,[166] the FTC's interpretive guidance to entities consists of little other than published guidance reports. In particular, the agency has not used its formal rulemaking authority and, in fact, has sought additional and specific notice and comment rulemaking authority in this area.[167] Further, the agency has not had any formal adjudication through which to communicate its interpretations. Entities are left with very little to go on. 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 nonauthoritative guidance, the central due process question remains whether such information provides "fair" notice adequate to address constitutional concerns.

It remains difficult to dispute that 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. A reviewing court may conclude that actual notice of the agency's interpretation of Section 5 exists, even though the agency's interpretations do not match the formality and importance of the communication methods reviewed by the D.C. Circuit in its prior cases. However, some notice is not fair notice. 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)—something

---

increases, *Mead Corp.*, 533 U.S. at 229-30, and a similar correlation seems to arise such that notice becomes "fairer" as the agency uses more formal and authoritative methods for communicating its interpretations.

166 Thirty-six data-security cases were brought under the FTC Act. Wyndham FTC Response, *supra* note 7, at 7.

167 *See Prepared Statement of the Federal Trade Commission on Data Security*, *supra* note 115, at 11 ("The Commission supports . . . the discussion draft [that] provides the agency with rulemaking authority in several areas, and authorizes it to use the standard notice and comment procedures required by the Administrative Procedure Act in lieu of the current rulemaking procedures prescribed in Section 18 of the FTC Act."); FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 36 (2000) [hereinafter FED. TRADE COMM'N, PRIVACY ONLINE] (stating that the Commission supports "legislation [that] would set out the basic standards of practice governing the collection of information online, and provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act").

that is not likely to be found in settlements with third parties or a list of nonmandatory agency recommendations.

3. The FTC Has Not Likely Published Conflicting Interpretations

Even if the agency has provided an interpretation of a law, under the D.C. Circuit's test, if the agency has provided conflicting interpretations, the fair notice doctrine may apply. Although some entities argue that the FTC has taken conflicting positions over time in relation to whether or not it has the ability to regulate data security,[168] the allegations in the agency's complaints do list repeatedly a subset of the FTC's recommended security practices published in its guide for businesses.[169] Independent of any allegations of inconsistency, the list of recommendations, the published complaints, and the consent orders may not provide fair notice because they are not authoritative interpretations of the law and because entities must, in many ways, guess at what data-security practices are required. In such a case, courts may not need to find interpretational inconsistencies in order to conclude that fair notice has not been provided to entities.

More generally, additional commentary or dissenting statements to agency guidance from FTC commissioners does occur. For example, Commissioner J. Thomas Rosch filed a dissenting statement to its recent privacy report that also constituted agency guidance.[170] In such situations, where the agency has not presented a uniform front, the validity of the guidance also comes into question. Were such commentary or statements available in the data protection guidance context, they would be applicable to a fair notice inquiry and could bolster the argument that fair notice did not exist.

4. A Section 5 Violation May Result in Serious Penalty

Under Section 5, the FTC cannot directly impose or request a monetary penalty. The FTC was given the sole remedy to issue an order requiring an entity to cease and desist certain conduct, in part, to avoid potential due process problems.[171] Moreover, if such cease-and-desist order is violated, a

---

168 Wyndham Motion to Dismiss, *supra* note 82, at 6-7. Wyndham argues that that FTC explicitly "*disclaimed* the authority to mandate data-security standards" in a 2000 report on information security. *Id.*

169 *Compare* Wyndham Complaint, *supra* note 127, at 10-12, *with* FED. TRADE COMM'N, *supra* note 126, at 11-13.

170 *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at app. C (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

171 Pelgro, *supra* note 124, at 907.

court can order a civil penalty, the rescission of contracts, restitution, refunds, and disgorgement.[172] Alternatively, the FTC can request that a court issue an injunction prohibiting certain behavior.[173] Just as the denial of a license or a vehicle recall can be a serious penalty, either a cease-and-desist order, and the potentially large penalty for noncompliance, or an injunction involving data security can dramatically affect a business, particularly small Internet companies whose entire business is based on data. Therefore, a violation of Section 5 could result in a substantial loss of property, implicating the fair notice doctrine and meeting the D.C. Circuit's test.

Given the relative paucity of authoritative agency interpretation, the FTC may not have provided fair notice under the D.C. Circuit's "ascertainable certainty" test. 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." Instead, it has communicated its policymaking choices by publishing complaints and consent orders as part of investigations against alleged Section 5 offenders and through agency guidance publications that include details of what the agency believes are reasonable data-security safeguards. While these types of communications may provide some notice of what the FTC thinks about data security, whether these communications should be deemed sufficiently authoritative to provide fair notice seems to be open to question.

III. CHALLENGES OF THE FTC'S APPROACH AND MOVING FORWARD

Even if the FTC is deemed to have provided legally required fair notice of required data-security practices under Section 5, the FTC's policy has not likely been effectively communicated. Ironically, an agency that calls on companies to be more transparent about their business practices has not been transparent about its data-security policy, seemingly constrained

---

172 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.").

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

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."[174] The FTC seems to agree that traditional APA rulemaking may be superior to adjudicative proceedings but has not yet undertaken to use the authority it already possesses. The FTC has supported federal legislation prescribing data-security requirements and recommended that the legislation be phrased 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."[175] The FTC stated that regulations could clarify the definition of "adequate security."[176]

The FTC has declined to use its rulemaking authority under Section 5 in the data-security context because it maintains that the procedures are too onerous.[177] However, the FTC has used rulemaking to implement other data-security-related laws, and, with less burdensome rulemaking requirements, may craft a practical and useful interpretation. Below, the Essay will look at some of the FTC's rulemaking efforts related to the Children's Online Privacy Protection Act ("COPPA") and the Fair and Accurate Credit Transactions Act ("FACTA") to demonstrate that rulemaking procedures may address fair notice concerns with existing enforcement approaches. This Essay evaluates at some of the reasons why rulemaking is likely a more effective tool to prescribe data-security requirements than enforcement actions have proven to be. However, rulemaking is not the only method to prescribe data-security requirements. Entities may also benefit from formal adjudications, policy statements, and advisory opinions. In the end, the method is less important than confronting persistent fairness concerns facing entities who are generally also victims in data-security cases.

---

174 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.").

175 FED. TRADE COMM'N, PRIVACY ONLINE, *supra* note 167, at 37.

176 *Id.* (internal quotation marks omitted).

177 *See Prepared Statement of the Federal Trade Commission on Data Security*, *supra* note 115, at 11 ("[E]ffective consumer protection requires that the Commission be able to promulgate these rules in a more timely and efficient manner.").

A. *Formal Rulemaking May Provide the Greatest Benefit.*

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

While the FTC has not used its rulemaking authority under Section 5 to clarify "unfair" data-security practices, Congress has directed the FTC to promulgate regulations under other laws, such as COPPA and FACTA.[178] As expected, entities have fully participated in the process.[179] In addition, the FTC has admitted that it altered its proposed rules based on the comments it received.[180] Even though entities may disagree with the final rules implemented by the FTC, such entities cannot argue that they did not have an opportunity to participate in the process and potentially affect the outcome. And, perhaps more importantly, the process and resulting rulemaking have proven far more likely to yield "ascertainable certainty" of the agency's interpretation.

a. *COPPA Rulemaking*

As the name implies, COPPA is intended to protect children when they use the Internet so that they do not provide personal information to websites without the permission of their parents. When Congress passed COPPA, it directed the FTC to issue regulations implementing the legislation.[181] Congress expected the FTC to issue a regulation to "require the operator of . . . a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[182] As a result, the FTC followed the typical procedures for APA rulemaking, including publishing a notice of proposed rulemaking, receiving 132 comments from outside entities which the FTC described as "extremely informative," in issuing the COPPA Rule.[183] In 2006, the FTC reviewed the COPPA Rule and again accepted "comments from various parties, including: trade associations,

---

178 *See* 15 U.S.C. § 1681m(e) (FACTA); *id.* § 6502(b)(1) (COPPA).

179 *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).

180 *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.

181 *See* 15 U.S.C. § 6502 (b).

182 *Id.* § 6502 (b)(1)(D).

183 Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,888.

Web site operators, privacy and educational organizations, COPPA safe harbor programs, and consumers."[184]

In 2011, the FTC proposed to modify the COPPA Rule by issuing a proposed notice of rulemaking. The FTC received 350 comments, which triggered the agency's reconsideration of the proposed rule.[185] When the FTC released its revised proposed rule, it received ninety-nine more comments.[186] When the FTC released its final COPPA Rule, it contained modifications from its two proposed rules, attributable to the public participation in the rulemaking process. Thus, providing a forum for public participation resulted in extensive participation by stakeholders and, presumably, a better rule.

b. *FACTA Rulemaking*

FACTA amended the Fair Credit Reporting Act, which regulates activities related to credit. Similar to COPPA, when Congress enacted FACTA, it required the appropriate oversight agencies, including the FTC, to issue joint regulations "regarding the detection, prevention, and mitigation of identity theft, including special regulations requiring debit and credit card issuers to validate notifications of changes of address under certain circumstances" in what has been called the Red Flags Rule.[187] The agencies issued a notice of proposed rulemaking and received 129 comments from financial institutions, financial institution holding companies, trade associations, individuals, business entities, and consumers groups.[188] The agencies modified the proposed rules and guidelines in response to the comments.[189] The Red Flags Rule broadly requires regulated entities to implement a written Identity Theft Prevention Program.[190] In addition to the general rule, the FTC issued detailed guidelines as an appendix to the rules to help guide regulated entities.[191]

These two rulemakings show that the FTC has experience crafting rules and detailed guidelines related to data-related practices. As the above examples demonstrate, the FTC is no stranger to using rulemaking proceed-

---

184 Children's Online Privacy Protection Rule, 71 Fed. Reg. 13,247, 13,247 (Mar. 15, 2006) (codified at 16 C.F.R. pt. 312).

185 Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 3973 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312).

186 *Id.*

187 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); *see also* 15 U.S.C. 1681m(e)(1)(C).

188 Identity Theft Red Flags, 72 Fed. Reg. at 63,718-19.

189 *Id.* at 63,719.

190 *See* 16 C.F.R. § 681.1(d) (2008).

191 *Id.* § 681 app. A.

ings to craft regulatory standards. When the FTC uses its rulemaking authority, entities clearly indicate their desire to participate in rulemaking proceedings by submitting comments. Not only are entities heard, but the FTC also uses the information it receives to formulate regulations in a manner directed at providing fair notice. In addition, the FTC has demonstrated that it can provide detailed guidance about data-security-related topics when necessary.

This Essay is not assessing the quality of the rules promulgated by the FTC in these instances; it only points out that in these situations, entities expected to comply with the rules have not had the same lack of clarity about compliant behavior as those regulated under Section 5 in connection with data security. Entities at least have a fair chance to comply with the rule, even when the rule is of no higher quality than the rule formed through the informal settlement process currently used by the FTC. Below, this Essay will discuss some of the benefits of rulemaking over adjudication for implementing policy choices.

2. Rulemaking Provides Many Benefits

As discussed previously, agencies typically have discretion to choose between rulemaking and adjudications in implementing the statutes it is assigned to regulate.[192] The FTC has chosen informal adjudication in the data-security field. However, as this Essay demonstrates, while the FTC's actions may provide some notice, that baseline may not be enough for entities to know the proper level of data-security precautions to undertake. The FTC's current method is constitutionally suspect, as the agency has not illuminated a clear formulation of a data-security rule under Section 5 in a way that provides fair notice. Rulemaking likely is the best method for providing authoritative, detailed guidance so that entities know how to comply with the law.

As this Essay discussed above, courts have held that fairness dictates that regulated entities be warned of the kinds of activities that will be punished.[193] The FTC can use rulemaking procedures and public comment to craft rules that make sense and to provide practical guidance to regulated entities. Unclear requirements, such as those vaguely communicated through the FTC's complaints and consent orders, unnecessarily burden regulated entities. Such entities must expend resources to discover the contours of the requirements, which often burdens regulated entities with un-

192 SEC v. Chenery Corp., 332 U.S. 194, 202-03 (1947).

193 *See* Bunn et al., *No Regulation Without Representation: Would Judicial Enforcement of a Stricter Nondelegation Doctrine Limit Administrative Lawmaking?*, 1983 WIS. L. REV. 341, 343 (1983).

certainty and conflicts with the FTC, litigation, and the high costs of potential noncompliance.[194]

These burdens can also flow through to consumers. Without clear direction, entities may waste resources by over-investing in unnecessary security when they could instead benefit society by providing better products and services. Vague requirements can also result in entities' frequent noncompliance through confusion or easy evasion,[195] which results in consumers receiving less data security than they might receive with clear baseline standards. Finally, vague rules may benefit larger companies at the expense of smaller companies. Large companies can afford the legal work necessary to better understand the FTC's interpretation and gauge risk. They can also afford to overinvest in data-security safeguards, while small companies, including many start-up technology companies dealing with data, do not have the resources to waste and face greater risks of noncompliance and litigation.

Another benefit of rulemaking is the opportunity for public participation. Unlike adjudication, rulemaking procedures generally require an agency to propose the regulations to the public and accept and consider public comment. Rules can be more effective because an agency can acquire from the public the benefit of pertinent facts, arguments, and considerations that it otherwise may not have.[196] Rulemaking also allows all stakeholders to participate in the formation of the regulations. Regulation by adjudication, on the other hand, means that nonparties may not be able to protect the rights that are being altered by the policies pronounced through the adjudication.[197]

Not only does the interpretive rulemaking process benefit through public participation, but the public itself derives an informational benefit from the openness and transparency of the rulemaking process. Through rulemaking procedures, agencies provide notice to the public and to the entities they regulate regarding the policy choices they are making.[198] These published values can be monitored by the public. When regulating by adjudication, an agency is making policy choices behind closed doors, which can invite political favoritism, corruption, or other arbitrary decision making.[199] In addition, the public is hard-pressed to change a law about which it does not know.[200] On the other hand, a clear, published regulation separates the

---

194 *See* Colin S. Diver, *The Optimal Precision of Administrative Rules*, 93 YALE L.J. 65, 73-74 (1983) (listing four categories of administrative rule compliance costs).

195 *See id.* at 103.

196 *See Chenery Corp.*, 332 U.S. at 202; Brice McAdoo Clagett, *Informal Action—Adjudication—Rule Making: Some Recent Developments in Federal Administrative Law*, 1971 DUKE L.J. 51, 83-84.

197 *See* Clagett, *supra* note 196, at 83.

198 *See Chenery Corp.*, 332 U.S.at 202.

199 *See* Bunn et al., *supra* note 193, at 343; Clagett, *supra* note 196, at 56-57.

200 *See* Bunn et al., *supra* note 193, at 343-44; Clagett, *supra* note 196, at 54.

outcome from a decision maker's discretion, helps ensure equal treatment of similarly situated entities, and creates broader public awareness.[201]

Although drafting transparent rules can be costly and time consuming,[202] it can greatly lessen the eventual cost of compliance and agency enforcement. That is particularly true with the rulemaking procedures required by Section 5. As discussed above, the rulemaking procedures under Section 5 are more burdensome than those prescribed by the APA.[203] Beyond the procedural difficulty, usually the more detailed the regulation is, the more political capital is required to push such details into law.[204] For example, many people would support a cyber-security law to protect the nation's critical infrastructure. However, a bill doing just that failed twice in the Senate in 2012, because the political parties had conflicting priorities and could not agree on the proper method for implementing the shared goal.[205]

Despite these initials burdens, there are potentially significant cost savings after the regulation becomes law. First, when a regulation is clear, voluntary compliance is more likely because compliance is easier to determine.[206] Second, determining whether a regulated entity is noncompliant is much easier, because the agency has a clear standard to apply to the entities' behavior.[207] This is particularly important when the potential number of violators is large, as is the case with data security. Virtually every company stores data on computers. Therefore, the FTC does not have nearly the resources necessary to police all of these entities. The easier it is for the FTC to identify violators, the more likely it is that the FTC will identify and investigate them. Third, when an investigation occurs, if the FTC has a clear set of guidelines, litigation costs should shrink.[208] With clear guidelines, the entity has less ability to argue the gray areas of compliance, and the FTC can more quickly prove its case against violators.

The complexity of the data-security landscape complicates rulemaking, but defining a coherent standard is not impossible. Besides the slow-moving procedural aspects of rulemaking, drafting clear and effective rules can be difficult, particularly in complex or fast-changing industries.[209] The FTC does not believe it would "be possible to set forth the type of particularized guidelines" to describe proper data-security safeguards.[210] It has

---

201 Diver, *supra* note 194, at 71.

202 *Id.* at 73.

203 15 U.S.C. § 57a (2006).

204 Diver, *supra* note 194, at 73.

205 *See* Grant Gross, *Cybersecurity Bill Fails in U.S. Senate*, COMPUTERWORLD (Nov. 14, 2012, 7:48 PM), http://www.computerworld.com/s/article/9233656/Cybersecurity_bill_fails_in_U.S._Senate.

206 Diver, *supra* note 194, at 72, 75.

207 *Id.*

208 *Id.*

209 *See* Jonathan R. Siegel, *Textualism and Contextualism in Administrative Law*, 78 B.U. L. REV. 1023, 1070-71 (1998).

210 Wyndham FTC Response, *supra* note 7, at 12.

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.'"[211] 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."[212] The FTC's statements are mystifying for two reasons. First, if the FTC does not believe it can properly define "reasonable," how can the FTC state that entities have been provided fair notice about how to conform to such a standard of reasonableness?

Second, while the FTC may be correct that technology continually changes, the same can be said for all laws that exist in an ever-changing world. The FTC seems to have taken the stance that because technology changes frequently, drafting regulations would be fruitless. But drafting principles-based regulations would provide guidance to entities and would still apply as technology changes. Moreover, the complaints the FTC filed a decade ago look remarkably similar to the complaints filed today.[213] Therefore, the idea that regulations would be impractical or out of date as soon as they are published is not reflected by the facts.

The rapid rate of technological progress should be no bar to crafting definite, coherent regulations. A regulation can be refined and corrected over time as it is applied to specific cases.[214] As the facts of each case differ, principles-based regulations can be adjusted accordingly. 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. These factors should be crucial inputs when determining the data-security safeguards an entity should implement. However, under the current complaint and consent order regime of informal adjudication, the presence of these factors and their relevance cannot be discerned. As such, regulated entities and other interested parties cannot work together to develop better working rules.

As the foregoing explains, the FTC has demonstrated the ability to use rulemaking in the data-security context, and rulemaking has several advantages over adjudication, generally, and more specifically in the context of fair notice. Rulemaking can provide clear guidance to regulated entities, incorporate the thinking of additional stakeholders, prevent cynical specula-

---

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

212 *Id.*

213 *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).

214 Diver, *supra* note 194, at 98-101.

tion regarding agency decision making, and lessen enforcement and compliance costs. The FTC has not used its existing Section 5 rulemaking authority to clarify "unfair" data-security practices because of its impracticality.[215] Congress's authorization to use the standard notice and comment procedures prescribed in the APA[216] could substantially address constitutional concerns relating to fair notice. Further, improved notice of a clear rule likely will result in greater compliance.[217] Pending such congressional authorization, the FTC has other options for improved communication of its interpretation of Section 5.

B. *Formal Adjudication Can Provide Benefits*

While the Authors believe rulemaking may be the preferred method for the FTC to address fair notice concerns and better communicate what it believes are adequate data-security practices under Section 5, it is not the only method. Up to this point in time, the FTC has eschewed formal adjudication of Section 5 violations in favor of its settlement process.[218]

Similar to its currently preferred process, the FTC can challenge "unfair practices" by issuing a complaint setting forth its charges.[219] However, rather than settle the charges, a defendant may respond to the complaint in writing, and the agency will consider the defendant's response.[220] If the FTC determines that the defendant violated Section 5, "it shall make a report in writing in which it shall state its findings as to the facts and shall issue" a cease-and-desist order.[221] A defendant may petition to set aside the order.[222]

This formal adjudicatory process can help provide notice to entities in two ways. First, when the FTC uses the cease-and-desist process, the FTC must report its findings of fact. These findings of fact would clearly communicate, in a formal way, what data-security practices violate the FTC's interpretation of Section 5. This mode of operation is superior to the current complaint and settlement process because it puts the FTC on record and creates predictability for entities. Entities are no longer required to sift through alleged violations; instead, they have clear notice of what the FTC has determined *are* violations. Government agencies can expect entities

---

215 *Prepared Statement of the Federal Trade Commission on Data Security*, *supra* note 115, at 11 ("[E]ffective consumer protection requires that the Commission be able to promulgate these rules in a more timely and efficient manner.").

216 *See supra* note 167.

217 Diver, *supra* note 194, at 72, 75.

218 *Prepared Statement of the Federal Trade Commission on Data Security*, *supra* note 115, at 11.

219 15 U.S.C. § 45(b) (2006).

220 *Id.*

221 *Id.*

222 *Id.* § 45(c).

subject to their jurisdiction to pay attention to interpretive rulings.[223] Second, entities can appeal the FTC's order, allowing both parties to argue before courts the applicability of Section 5 to data-security practices. The agency will be forced to articulate its interpretation in a way that makes sense to the court, benefiting third parties. The court can publish an opinion, possibly granting some level of deference to the FTC's Section 5 interpretation, which will further enunciate and clarify the FTC's interpretation.

Alternatively, as in Wyndham's case, the FTC can directly file suit in federal district court for injunctions.[224] Similar to the discussion above, the FTC will need to convince the court that a defendant is violating Section 5. To do that, the FTC will need to explain its interpretation of Section 5 and how the defendant's data-security practices violate Section 5. As a result, third parties may be able to better understand the FTC's interpretation. In addition, the court will be able to assess whether the FTC's interpretation is reasonable and discuss the merits of the FTC's interpretation. Judicial review may provide authority supporting the interpretation. Like rulemaking, this method of clarifying the FTC's interpretation can provide benefits, such as improving legal compliance and preventing entities from wasting resources by attempting to comply with unclear requirements.[225]

Adjudication may remain less desirable than rulemaking, because regulation by adjudication means that nonparties may not be able to protect their rights.[226] In addition, when regulating by adjudication, an agency is not as directly monitored by the public, inviting political favoritism, corruption, or other arbitrary decision making.[227]

While policymaking through adjudication has its own set of problems, it seems preferable to the current environment where entities often lack fair notice predicates on an authoritative set of data-security requirements imposed by Section 5.

C. *Advisory Opinions, Policy Statements, and Other Communications*

Policies made through formal rulemaking and adjudications are authoritative and can provide clear notice to entities. Advisory opinions, policy statements, and other similar communications are less formal and authoritative, but possibly more effective than the current complaint and settlement process and best practice recommendations.

---

223 Radio Athens, Inc. v. FCC, 401 F.2d 398, 404 (D.C. Cir. 1968) (noting that "[a]gencies, like courts, may rightly expect attention to be accorded their interpretive rulings).

224 15 U.S.C. § 53(b).

225 *See* Diver, *supra* note 194, at 72, 103.

226 *See* Clagett, *supra* note 196, at 83.

227 Bunn, et al., *supra* note 193, at 343; Clagett, *supra* note 196, 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)).

When entities regulated by the FTC request guidance about the FTC's enforcement intentions,[228] the FTC may respond with an agency advisory opinion or a staff advisory opinion.[229] The agency may issue an advisory opinion when: (1) the matter involves a substantial or novel question with no clear FTC or court precedent; and (2) the subject matter is of significant public interest.[230] The agency has also authorized its staff to provide advice when the agency believes an agency advisory opinion is inappropriate.[231] The agency could provide advisory opinions that fully describe data-security practices satisfying the data-security requirements of Section 5 because there is no clear precedent and it is a matter of significant public interest. In the past, the FTC has issued advisory opinions for subjects such as advertising, the Federal Credit Reporting Act, the Fair Debt Collection Practices Act, the Gramm-Leach-Bliley Act, and telemarketing.[232] However, the FTC may choose not to form a definite opinion when difficult factual issues exist or significant investigation is required.[233] In the Section 5 context, the FTC may not provide an opinion if it concludes that an opinion describing detailed data-security practices would necessarily be based on complex factual circumstances and require extensive investigatory efforts.

Although advisory opinions can provide some notice and limited guidance, they are not universally helpful. Advisory opinions are placed in the public record and thus provide notice.[234] However, advisory opinions are only marginally better than the existing best practices guidance and the complaints and settlements the FTC currently uses to communicate its data-security policy. First, an advisory opinion does not "prejudice" the FTC's right to reconsider the questions involved and rescind or revoke its opinion.[235] In other words, the FTC can change its mind at any time. Therefore, relying on an advisory opinion presents risk and unpredictability. Second, the FTC only grants protection for good faith reliance on an advisory opinion to the requesting party.[236] Therefore, the FTC is not required to act in accordance with its advisory opinion as it relates to third parties. Third, advice from staff may not be authoritative, as it may not represent the policy of the agency as a whole. The agency may choose to override staff opinions when determining whether to bring an enforcement action.

---

228 16 C.F.R. § 1.1 (2012); Judith A. Moreland, Att'y, Fed. Trade Comm'n, Overview of the Advisory Opinion Process at the Federal Trade Commission (Feb. 13-14, 1997), *available at* http://www.ftc.gov/bc/speech2.shtm.

229 16 C.F.R. § 1.1.

230 *Id.* § 1.1(a).

231 *Id.* § 1.1(b).

232 *Advisory Opinions*, FED. TRADE COMM'N, http://www.ftc.gov/ftc/opinions.shtm (last visited Mar. 17, 2013).

233 Moreland, *supra* note 228.

234 16 C.F.R. § 1.4.

235 *Id.* § 1.3(b).

236 *Id.*

Similarly, enforcement policy statements, while nonbinding on the FTC, can provide much needed clarity. The FTC has already issued an enforcement policy statement related to its "unfairness" authority. In 1980, the FTC responded to a Congressional inquiry to explain its application of its "unfairness" authority over consumer transactions.[237] Unsurprisingly, the policy statement does not discuss Section 5's application to data-security practices. In the statement, the FTC admitted that the concept of consumer unfairness was understandably not obvious and "has been honestly troublesome for some businesses."[238] As a result, the FTC "attempt[ed] to delineate . . . a concrete framework for future application of the Commission's unfairness authority."[239] In drafting the framework, the FTC reviewed its decisions and those from courts and stated, "it is possible to provide a reasonable working sense of the conduct that is covered [by the unfairness authority]."[240] In light of its experience in bringing data-security-related actions over the last ten years, the FTC should be able to provide a policy statement delineating a reasonable working sense of its data-security requirements.

In addition to advisory opinions and enforcement policy statements, other agency communications can provide some benefits. As the FTC has already done, it can provide some clarity with agency reports and guides. This Essay discussed above the problem with the FTC's data-security best practices guide. The guide contains recommendations and not requirements. Therefore, it does not provide the desired authoritative description upon which entities can rely. Nonetheless, there are benefits to having the FTC provide some explanation of its enforcement decisions through advisory opinions, policy statements, and other communications related to data-security violations of Section 5. The FTC can use these communications to clarify its expectations beyond simply listing recommendations. However, these statements are less authoritative than formal rulemaking and adjudication, and they leave questions about whether entities can rely upon them.

D. *To Provide the Greatest Benefit, the FTC's Interpretive Guidance Should Not Consist of Vague Generalities*

As this Essay has shown, the FTC has multiple methods of communication at its disposal through which it can provide much needed clarity regarding entities' data-security obligations. However, should the agency decide to publish authoritative guidance, the guidance needs to be practical and useful for entities.

---

237 *In re* Int'l Harvester Co., 104 F.T.C. 949, 1070-76 (1984).

238 *Id.* at 1071.

239 *Id.*

240 *Id.*

A "reasonableness" test absent additional principles-based authoritative guidelines or significant additional court-resolved litigation will remain problematic. The agency may continue its current practice of stating that data-security practices must be "reasonable and appropriate"[241] and that entities must use "readily available" security measures, have "adequate" information security and network-access policies and procedures, implement "reasonable measures" to detect and prevent unauthorized data access, and use "proper" incident response measures.[242] In other words, the FTC may offer an interpretation that does nothing to clarify the underlying uncertainty and to resolve the problem of fair notice. Moreover, 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."[243] The Authors do not believe that using the standards of "reasonable" and "appropriate" while taking into account the nature of the business and the kinds of information that is collected can ensure that *fair* notice occurs. Such standards would provide no useful guidance without substantial additional participation by stakeholders through the formal rulemaking process or the reasoned and thorough discussion of the standard in a formal adjudicatory opinion, policy statement, or advisory opinion.

Even were the FTC to employ formal rulemaking or adjudication, a reasonableness test seems to be less useful in contexts like data security, where the meaning of "reasonable" remains subject to ongoing technology evolution and prevailing data protection preferences. This can be seen now as society debates the balance of strong privacy protections against the societal benefits of the free flow of information.[244] There may be no such concept as "reasonable" privacy and data-security practices until more satisfactory societal consensus emerges. Even at a more detailed level, for example, the FTC itself does not seem to consistently define what information is "sensitive" and potentially deserves greater protection.[245] As such, at any

---

241 Wyndham First Amended Complaint, *supra* note 81, at 2.

242 *Id.* at 10-12

243 FED. TRADE COMM'N, *supra* note 126, at 23.

244 THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 5-6 (2012), *available at* http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf.

245 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* note 126, at 47 n.214. The privacy report also lists passwords as sensitive information. *Id.* at 8, 15, 37 n.174. 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* note 126, 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

given time, an entity would not be able to determine with precision what data-security practices are "reasonable." Given the lack of consensus 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" inserts arbitrariness and the risk that "reasonable" security is whatever the FTC says it is at any given moment in time. Entities have little hope of confidently ensuring that they have successfully complied with Section 5, thereby preventing litigation. This seemingly arbitrary standard creates due process challenges and a risk of post hoc rationalization. Therefore, the use of a "reasonableness" test without providing concrete guidance makes the relevance and significance of the application of the fair notice doctrine especially important in this emerging area of consumer protection.

Against the current backdrop of aggressive agency enforcement, the patent unfairness of the "reasonable" security standard is clear. Entities have not been given proper notice of what data-security practices are "reasonable" and "adequate." Given the lack of detailed clarity, entities are basically working under a strict liability framework where any data breach could result in an FTC enforcement action. It is common knowledge that 100 percent security does not exist.[246] Yet, entities are working in an environment of "Russian Roulette," just as the D.C. Circuit cautioned, where the next time they are victimized they may also face litigation. Given the reality that entities cannot provide 100 percent security, the FTC should undertake to evaluate the use of all the interpretive tools at its disposal in light of these concerns. In sum, "reasonable" data security cannot mean 100-percent security; yet, the FTC seems to be working with that expectation and has been unwilling to authoritatively articulate a more definite standard. This lack of notice is unfair.

Lack of notice is particularly inappropriate when the FTC is punishing an entity that has been the victim of a crime. Some of the FTC's data-security-related enforcement actions have involved alleged actions solely attributable to the defendant, such as improperly disposing of documents containing personal information.[247] In these matters, all of the facts and circumstances were entirely within the entities' control, and the entities allegedly committed some form of malfeasance. In contrast, in matters like Wyndham's, involving data breaches, the entities are investigated due to the

---

Consumers and Failed to Safeguard Sensitive Data It Collected (Oct. 22, 2012), *available at* http://www.ftc.gov/opa/2012/10/compete.shtm.

246 The Authors regularly see hackers victimize the Pentagon, where this Essay assumes information and computer security infrastructure is at its strongest. *See* Grace Wyler, *Pentagon Admits 24,000 Files Were Hacked, Declares Cyberspace a Theater of War*, BUS. INSIDER (Jul. 14, 2011, 4:35 PM), http://www.businessinsider.com/pentagon-admits-24000-files-were-hacked-declares-cyberspace-a-theater-of-war-2011-7.

247 *E.g.*, Complaint ¶ 7, *In re* Rite Aid Corp., No. C-4308 (Nov. 22, 2010), *available at* http://www.ftc.gov/os/caselist/0723121/index.shtm; Complaint ¶ 7, *In re* CVS Caremark Corp., No. C-4259 (June 23, 2009) *available at* http://www.ftc.gov/os/caselist/0723119/index.shtm.

actions of a criminal third party. The investigated entities did not directly cause the loss or unauthorized access to data; they simply failed to prevent a third party from accessing it. In situations where an entity is investigated and potentially liable as a direct result of being victimized by a criminal invasion, fundamental fairness may dictate that entities be clearly told what actions would insulate them from allegations of unfair and deceptive acts or practices.

CONCLUSION

This Essay argues that currently the FTC's enforcement and guidance practices may pose serious constitutional and practical concerns of providing fair notice of the data-security practices that violate Section 5. The FTC has several alternative methods for providing more useful and authoritative guidance to entities. Rulemaking seems to be the most promising to address these concerns, as it allows entities to participate in the regulatory process thereby improving the final rule. Formal adjudications, advisory opinions, and policy statements, though less effective than rulemaking, may also provide some much needed clarity. Given the current environment of aggressive enforcement against the victims of crimes that have unclear guidance on expected data-security practices, improved authoritative interpretations of Section 5 are crucial to improve compliance and provide entities with enough information to perform proper risk management.