icarus

Communications & Digital Technology Industries Committee
ABA Section of Antitrust Law

Winter 2011

Contents

2 Committee Leadership

3 From the Editors

4 The FTC's Use of Section 5 to Regulate Internet Password Security
Benjamin R. Dryden

17 State Sovereignty in the 21st Century: Limitations on Class Action Fairness Act Removal Jurisdiction
Adam Miller

33 Summary of Roundtable Discussion of *United States v. AT&T*
Travis H. Mallen

The FTC's Use of Section 5 to Regulate Internet Password Security

Benjamin R. Dryden
bdryden@foley.com

Foley & Lardner LLP[1]

On June 15, 2011, the Federal Trade Commission issued an administrative complaint and consent order against Lookout Services, a company that provides software and data hosting to help businesses verify their employees' eligibility to work in the United States.[2] The complaint arose out of an incident in which a customer tried several, low-tech means to test Lookout's security, such as entering the username "test" and password "test" to see if they worked.[3] To her surprise, she discovered that this combination was a valid credential for another Lookout customer and that, by entering the two codes, she was able to view the names, addresses, and Social Security numbers of some 11,000 people.

The FTC charged Lookout with two separate violations of Section 5 of the FTC Act.[4] Lookout's alleged violations included failing "to establish or enforce rules sufficient to make user credentials (i.e., user ID and password) hard to guess;" failing "to require periodic changes of user credentials, such as every 90 days;" and failing "to suspend user credentials after a certain number of unsuccessful login attempts."[5]

It was surely risky of Lookout to allow a customer to use "test" as both a username and password; nonetheless, the FTC may be overreaching by claiming authority under Section 5 to regulate Internet password security. Section 5 only authorizes the FTC to take action against "unfair" practices so long as the potential harms from the practices are not "reasonably

---

1 Benjamin R. Dryden is an associate with Foley & Lardner LLP and is a member of the firm's Antitrust, Business Litigation & Dispute Resolution, and Distribution & Franchise Practices.

2 *In the Matter* of Lookout Services, Inc., FTC File No. 102 3076.

3 Complaint, *In the Matter of Lookout Services, Inc.*, FTC File No. 102 3076, ¶ 10. The customer was also able to access information about other customers' employees by guessing URLs that bypassed the login process altogether.

4 15 U.S.C. § 45.

5 *Id.* ¶ 7(a)-(c). The consent order requires Lookout to develop "a comprehensive information security program," to be monitored by an independent third party (at Lookout's expense) for the next 20 years. *See* Decision and Order, *In the Matter of Lookout Services, Inc.*, FTC File No. 102 3076, at §§ II-III.

avoidable by consumers themselves and are not outweighed by countervailing benefits."[6] At first glance, Internet password security seems to be a classic example of a practice that falls out of this authority: consumers only get out of passwords what they put into them, and a consumer might rationally choose to forgo a strong password in exchange for one that is easy to remember. However, the FTC is increasingly using its Section 5 powers to sue Internet companies that employ subpar password privacy practices when company's stated privacy policy is "deceptive" or there is substantial injury to consumers due to a security breach. This article explores the evolution of these enforcement actions and argues that, although the FTC's enforcement actions have grown in scope and ambition, there are important limitations on the FTC's authority that should prevent the FTC from turning into the federal password police.

FTC Enforcement Actions

The FTC's complaint against Lookout Services is only the most recent in a series of administrative actions the FTC has brought in the area of password security.[7] In all of these actions, including the *Lookout* case, the FTC negotiated the same essential relief: a consent order requiring the offending company to develop and implement "a comprehensive information security program" and to retain an independent third party to audit the program every other year for the next 20 years.

1. *CardSystems Solutions and Solidus Networks, Inc.*

In 2006, the FTC brought a landmark administrative action against CardSystems Solutions, Inc. and it successor company for violations of Section 5.[8] CardSystems operates an Internet service that allows merchants to obtain authorizations for credit and debit card transactions. The case arose out a hacker's breach of this service; at the time, it was the largest

---

6 15 U.S.C. § 45(n) ("The Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice 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.").

7 In addition to the actions listed here, see also Complaint, *In the Matter of the TJX Companies, Inc.*, FTC File No. 072 3055, ¶ 8(c) (mentioning failure to "require network administrators and other users to use strong passwords or to use different passwords to access different programs, computers, and networks" among grounds for claim of unfair privacy practices).

8 *In the Matter of CardSystems Solutions, Inc. and Solidus Networks, Inc. d/b/a Pay By Touch Solutions*, FTC File No. 052 3148.

breach of financial data ever.[9] The breach caused "several million dollars in fraudulent credit and debit card purchases" and forced issuing banks to cancel and re-issue untold thousands of credit and debit cards.[10]

The FTC alleged that CardSystems's security practices were so gravely flawed that they constituted an unfair practice in violation of Section 5. It listed several categories of security failures that CardSystems had made which, "taken together," allegedly violated Section 5. The FTC emphasized that CardSystems created unnecessary risks by storing data in a vulnerable format for longer than was necessary; that it failed to take reasonable steps to anticipate commonly known or reasonably foreseeable hacking devices; and, relevant here, that CardSystems "failed to use strong passwords."[11]

The complaint made no attempt to explain what the term "strong passwords" meant. In fact, the breach of CardSystems's network had nothing to do with the company's password security practices. Instead, the hacker exploited a security flaw in the CardSystems application's login prompt code that allowed the hacker to bypass the login process altogether.[12] In other words, the hacker did not breach the CardSystems database by obtaining another user's password; rather, the hacker injected a logic string into the CardSystems web application that allowed him to avoid entering a password in the first place. Nevertheless, for the first time, the FTC had brought password security underneath the Section 5 umbrella.

2. *Reed Elsevier and Seisint*

In 2008, the FTC brought its first enforcement action that hinged squarely on password security. The case was brought against Reed Elsevier Inc. (the parent company of LexisNexis) and a subsidiary. The matter involved an identity verification service that compiles information about individuals from sources such as credit agency reports and motor vehicle records. Reed Elsevier packages its analysis into a sophisticated identity verification database, marketed under the LexisNexis brand, which professional organizations such as insurance companies, law firms,

---

9 Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (preliminary report Dec. 2010), at B-3.

10 Complaint, *In the Matter of CardSystems Solutions, Inc. and Solidus Networks, Inc. d/b/a Pay By Touch Solutions*, FTC File No. 052 3148, ¶ 8.

11 *Id.* ¶ 6.

12 The attack method is known as an "SQL injection attack." *Id.* ¶ 7. SQL injection attacks exploit vulnerabilities in the logic of Structured Query Language commands. For a technical explanation, see generally http://blogs.sitepoint.com/sql-injection-attacks-safe/.

debt collectors, and government agencies pay to access.[13] These customers access the service through a website secured by a username and password.

Beginning in 2003, hackers managed to obtain the usernames and passwords of several customers.[14] As a result, the hackers obtained the highly sensitive information — including names, dates of birth, Social Security numbers, and past and present addresses — of some 316,000 consumers.[15] The hackers used this information to open credit accounts and intercept credit cards in the names of some of these individuals, which they then used to make fraudulent purchases.[16]

The FTC came down hard on LexisNexis's password security practices. The complaint identified nine separate failures, including:

- allowing customers to choose the same word — "including common dictionary words" — as both the username and password;
- failing to require periodic changes to credentials, "such as every 90 days;"
- failing "to suspend user credentials after a certain number of unsuccessful log-in attempts;" and
- allowing users to reset their credentials "without confirming that the new credentials were created by customers rather than identity thieves."[17]

According to the FTC, these failures, "taken together," constituted an unfair act or practice. Thus, for the first time, the FTC claimed that Section 5 could be violated by password security failures alone.

3. *Twitter*

On March 11, 2011, in the FTC's first foray into the social media sector,[18] the FTC obtained relief against the social media site Twitter.[19] The complaint arose from two incidents

---

[13] Complaint, *In the Matter of Reed Elsevier Inc. and Seisint, Inc.*, FTC File No. 052 3094, ¶¶ 5-7.

[14] *Id.* ¶ 12. The Complaint does not specify how the hackers obtained these users' credentials.

[15] *Id.*

[16] *Id.* ¶ 13.

[17] *Id.* ¶ 10.

[18] *See Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 8, at B-5.

in 2009 in which hackers obtained the credentials of Twitter site administrators, allowing the hackers to take control of individual users' accounts. One hacker accomplished the breach by infiltrating a Twitter employee's personal email account, where he found passwords to other websites stored in archived emails; based on these other passwords, the hacker was able to surmise the employee's administrative credentials for Twitter.[20] The other hacker used a combination of luck and brute force; he ran "an automated password guessing tool to derive an employee's administrative password, after submitting thousands of guesses into Twitter's public login webpage. The password was a weak, lowercase, letter-only, common dictionary word."[21]

As a result, the hackers obtained administrative control of Twitter. They seized individual users' accounts, viewed private messages stored in personal archives, and reset individual users' passwords. One especially intrepid hacker took control of the Twitter account of then-President-Elect Obama. The imposter posted a tweet, ostensibly from the President-Elect, "that offered his more than 150,000 followers a chance to win $500 in free gasoline, in exchange for filling out a survey."[22]

The FTC recited many of the same password security lapses that it raised in the *Reed Elsevier* action: Twitter had allowed its employees to use dictionary words as passwords; it failed to require periodic changes of passwords; and it failed to suspend login attempts after a number of unsuccessful attempts.[23] To this list, the FTC added some new twists: for example, Twitter had failed to "require that such passwords be unique — *i.e.*, different from any password that the employee uses to access third-party programs, websites, and networks;" and it had failed to establish policies against "storage of administrative passwords in plain text in personal email accounts."[24]

However, unlike its previous enforcement strategies, the FTC did not allege that Twitter's security failures constituted an "unfair" act or practice. Rather, the FTC's theory was that Twitter violated Section 5 by making "deceptive" statements on its website assuring users that Twitter would employ reasonable security measures to prevent unauthorized access and

---

19 *In the Matter of Twitter, Inc.*, FTC File No. 092 3093.

20 Complaint, *In the Matter of Twitter, Inc.*, FTC File No. 092 3093, ¶ 12(b).

21 *Id.* ¶ 12(a).

22 *Id.*

23 *Id.* ¶ 11.

24 *Id.*

keep private messages "away from the public eye."[25] Because these statements were false or misleading — as the hacker's breaches proved — the FTC alleged that Twitter had violated Section 5 through "deceptive" acts or practices, as opposed to "unfair" ones.

Doubts About the FTC's Authority

Even though the FTC is increasingly using its powers to regulate Internet privacy generally — and password security specifically — it is far from clear where the FTC derives the lawful authority to do so. The FTC's powers under Section 5 date back before World War II:[26] Section 5's key provision authorizes the FTC to take limited actions to protect consumers against "[u]nfair methods of competition . . . and unfair or deceptive acts or practices" that are in or that affect commerce.[27] A practice cannot be "unfair" unless it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[28]

Weak privacy practices cause substantial injury to consumers and competition. Each year, as many as 9 million Americans fall victim to identity theft.[29] Those who detect the crime may spend countless hours and out-of-pocket costs repairing the damage; those who do not detect the crime may lose money and suffer lasting harm to their credit reports.[30] However, it does not necessarily follow that weak privacy practices are necessarily "unfair" within the meaning of the FTC Act. Many weak privacy practices are "reasonably avoidable by consumers

---

25 *Id.* ¶¶ 10, 13-17.

26 As originally enacted in 1914, Section 5 prohibited "unfair competition." In 1931, the Supreme Court interpreted this language to severely limit the FTC's authority over deceptive conduct. In 1938, Congress responded in 1938 by bringing "unfair or deceptive acts or practices" into the ambit of Section 5. *See generally* Michael M. Greenfield, *Unfairness Under Section 5 of the FTC Act and its Impact on State Law*, 46 Wayne L. Rev. 1869, 1870 (2000).

27 15 U.S.C. § 45(a)(1).

28 15 U.S.C. § 45(n) ("The Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice 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.").

29 *See generally* Federal Trade Commission, *About Identity Theft*, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

30 *Id.*

themselves." A consumer who favors strong passwords would be well advised not to use "test" as his password and username.

Moreover, the benefits of optimal password practices might well be "outweighed by countervailing benefits to consumers and competition." Who among us has never been irritated by websites that require upper-and-lower-case, non-dictionary, alphanumeric passwords? Such password policies not only impose costs on consumers' time and satisfaction, but they can also be counterproductive. One study found that in workplaces with the weakest password policies, 9% of employees write their passwords down in case they forget them; by contrast, in workplaces with the strongest password policies, 55% of users write their passwords down.[31] Writing a password down, of course, is self-defeating; an optimally secure password written down in an unsecured location is far less secure than a decent password committed to the user's memory. Indeed, a similar failure contributed to the breach in *Twitter*: a site administrator had so many passwords to remember that he kept them archived in a relatively insecure, personal email account.

The Shifting Bases for FTC Enforcement Actions

To understand the FTC's actions in the password arena, they must be viewed against the backdrop of a broader debate in the FTC about the scope of its own authority to regulate Internet privacy practices. As the Internet burst into commerce in the 1990s, the FTC first sought to promote a "notice-and-choice" model, whereby websites would give consumers accurate information about the sites' privacy practices to allow consumers to make informed decisions about how their information would be used. This notice-and-choice model reflected an understanding about the limits of the FTC's Section 5 authority. In 1998, Robert Pitofsky, the Chairman of the FTC at the time, testified before a House subcommittee that the FTC's authority in the Internet privacy context is limited "to ensuring that Web sites follow their stated information practices."[32] In fact, the Chairman called on Congress to give the FTC specific authority to regulate consumer privacy, which he said would be "necessary" for the FTC to move forward.[33] Two years later, in an open letter to the EU Directorate-General, Chairman Pitofsky echoed this position by acknowledging that "it currently may not be within the FTC's power to broadly require that entities collecting information on the Internet adhere to a privacy

---

31 Daniel D. Houser, "Blended Threat Analysis: Passwords and Policy," *in* Harold F. Tipton & Micki Krause, eds., *Information Security Management Handbook*, at 853 (6th ed. 2007)

32 Prepared Statement of the Federal Trade Commission on "Consumer Privacy on the World Wide Web," before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce (July 21, 1998), *available at* http://www.ftc.gov/os/1998/07/privac98.htm.

33 *Id.*

policy or to any particular privacy policy."[34] However, the Chairman reaffirmed the FTC's authority to enforce the notice-and-choice model, because "a company's failure to abide by a stated privacy policy is likely to be a deceptive practice."[35]

In the early 2000s, however, the FTC started to move away from the position that a privacy practice had to be "deceptive" in order to be actionable under Section 5. In 2001, a new FTC Chairman, Timothy Muris, backpedaled from his predecessor's calls for Congress to enact new laws regulating privacy. In Chairman Muris's view, there was already "a great deal we can do under existing laws," and what the FTC needed was "more law enforcement, not more laws."[36] At the same time, the exponential growth of the Internet gave way to a recognition that it would be impractical and costly to expect consumers to scrutinize the privacy notices of every website they visited before engaging in commerce.[37] Instead, a better, more efficiency-enhancing solution would allow consumers a reasonable assurance that all websites would take appropriate precautions to protect them from the malicious use of their personal information. Thus, the FTC turned away from the notice-and-choice model and towards what it later called a "harm-based approach."[38] The harm-based approach "targeted practices that caused or were likely to cause physical or economic harm, or unwarranted intrusions in consumers' daily lives."[39]

The FTC's actions against CardSystems and Reed Elsevier reflect the harm-based approach. Both rely on a theory that the respondents' failures to protect personal information caused or were likely to cause harm to consumers. On the other hand, the FTC backed away from the harm-based approach in the *Twitter* action, returning instead to its old "notice-and-choice" strategy, claiming that Twitter harmed competition by posting "deceptive" privacy notices that misled consumers. Significantly, the FTC's most recent action, *Lookout*, reflects both theories. The FTC brought two different claims against Lookout: one alleging that Lookout's privacy notices were "deceptive," and another alleging that its privacy practices were "unfair."

---

[34] Letter from Chairman Robert Pitofsky to Director General John Mogg (July 14, 2000), *available at* http://www.ita.doc.gov/td/ecom/ftcletterfinal.htm.

[35] *Id.*

[36] *Protecting Consumers' Privacy: 2002 and Beyond*, Remarks of Chairman Timothy J. Muris at the Privacy 2001 Conference, Cleveland, Ohio (Oct. 4, 2001), *available at* http://www.ftc.gov/speeches/muris/privisp1002.shtm.

[37] *Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 8, at 9.

[38] *Id.* (internal quotations and alterations omitted).

[39] *Id.* (internal quotations and alterations omitted).

Limitations on the FTC's Authority to Regulate Passwords

As these cases show, the FTC has claimed Section 5 authority to regulate Internet passwords in two circumstances: when a password practice would render a website's stated privacy policy "deceptive" (the notice-and-choice approach); or when a password practice is likely to cause substantial injury to consumers which is neither avoidable by consumers themselves nor outweighed by countervailing benefits (the harm-based approach). Some important limitations on the FTC's authority to regulate passwords are inherent in these grants of authority.

1. The "Unfairness" Power is Limited to Risks that Consumers Cannot Avoid

First and foremost, the FTC lacks the authority to declare a practice "unfair" unless it poses a risk of harm "which is not reasonably avoidable by consumers themselves."[40] Thus, absent unusual facts, the FTC likely lacks the unfairness power to sue websites that allow consumers to select "weak" passwords (*e.g.*, based on birthdays or dictionary words); or to sue websites that allow consumers to keep the same password indefinitely; or to sue consumer websites that lack policies against writing passwords down or using the same password for multiple websites. Presumably, consumers who follow bad password practices do so because they determine that the convenience of bad practices outweighs the burden of best practices.

Thus, it is significant that all of the password actions brought to date present special cases where consumers' personal information was kept in a third party's hands where they were helpless to keep it safe. In *Lookout*, the username "test" and password "test" were set by an employer who used Lookout's website to store the personal information of its employees. In *CardSystems*, accounts were set up by retailers to transmit the credit card information of their customers. In *Reed Elsevier*, accounts were set up by professional organizations and governments to view LexisNexis's massive database of personal information about consumers. And in *Twitter*, the hacked passwords belonged to site administrators.

In short, the FTC lacks the authority under its "unfairness" power to bring enforcement actions against websites for merely allowing consumers to employ bad password policies. If a consumer wants to use the username and password "test" to safeguard his own personal information, the FTC is powerless to punish a website for failing to stop him. However, the FTC may legitimately have authority to bring an unfairness action against a consumer website that fails to suspend user credentials after a reasonable number of login attempts, or that allows users to reset their credentials without taking steps to confirm that the new credentials are created by consumers themselves. In those cases, where the consumer can do nothing to protect himself, a consumer website runs a risk by failing to employ best practices.

---

[40] 45 U.S.C. § 45(n).

2. The "Unfairness" Power is Limited to Practices that Harm "Consumers"

Second, the FTC's authority to regulate "deceptive" conduct extends to all practices in or affecting commerce; by contrast, the FTC's authority to regulate "unfair" conduct only applies to practices that can harm "consumers."[41] This is an important distinction, and it suggests why the FTC has taken three different approaches in its password cases.

In *CardSystems* and *Reed Elsevier*, the victims of the security breaches were the consumers whose credit card and Social Security numbers were stolen; the actual customers of the two services — retailers and professional organizations — were not harmed or deceived in any way. Thus, the FTC brought the two cases under its "unfairness" power to cure the substantial harm suffered by consumers. In *Twitter*, by contrast, the relevant victims were the Twitter users whose accounts were breached by hackers posing as site administrators. Because Twitter is a free service, these users are not "consumers" in a meaningful sense of the word.[42] However, insofar as Twitter is a service involved in the interstate transmittal of messages for a profit, it is a service "in or affecting commerce," and thus subject to the FTC's authority over "deceptive" practices.[43]

Notably, the *Lookout* case presents an interesting jurisdictional challenge for the FTC. Unlike the consumer-oriented credit card records that Card Systems kept or the credit agency reports and motor vehicle records that Reed Elsevier compiled, Lookout stores personal information about companies' employees; and while these employees are no doubt "consumers" in the sense that they spend the money they earn, the database that was breached only contained information about them that had been collected in their capacity as "employees." Although the FTC has previously taken the position that it "has the same jurisdiction in the employment-related data situation as it would generally,"[44] it is far from clear whether this assertion would

---

41 15 U.S.C. § 45(n).

42 *See, e.g.*, *FTC v. IFC Credit Corp.*, 543 F. Supp. 2d 925, 937-938 (N.D. Ill. 2008) (noting that "consumer" is not defined in the FTC Act, but assuming that the term captures entities that make "transactions" for goods or services); *see also Black's Law Dictionary* (abridged 8th ed. 2005) ("A person who buys goods or services for personal, family, or household use, with no intention of resale; a natural person who uses products for personal rather than business purposes.").

43 *See* Letter to Commenter Thomason, *In the Matter of Twitter, Inc.*, FTC File No. 092 3093, at 2 (addressing commenter's concerns about FTC's jurisdiction over websites and social network operators).

44 *See* Letter from Chairman Robert Pitofsky to Director General John Mogg, *supra* note 33; *see also* Boris Segalis, "FTC Privacy Enforcement Update: Two Companies Allegedly Failed to

stand if challenged.[45] Meanwhile, the allegedly "deceptive" statements at issue in *Lookout* were tenuous at best: Lookout promised generally that it would "keep [customers'] data secure from unauthorized access," but it never promised anything concrete.[46] Thus, *Lookout* has forced the FTC to assert two different, dubious theories, in the (correct) hope that the respondent would rather cave on the merits than litigate the FTC's jurisdiction.

3. In All Cases, the FTC Seeks "Harm-Based" Relief

Even though the FTC brings password security cases under different theories, in all cases it seeks a remedy that reflects the "harm-based" enforcement approach. In the "harm-based" actions against CardSystems and Reed Elsevier, the consent orders require the respondents to develop "a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information," and to retain an independent monitor to perform biannual assessments of the program for a period of 20 years.[47] Similarly, in the hybrid "harm-based" and "notice-and-choice" action against Lookout, the consent order both requires an independently monitored "comprehensive information security program" and further bars Lookout from misrepresenting its privacy practices.[48]

In the pure "notice-and-choice" action against Twitter, however, the consent order does not merely bar Twitter from misrepresenting its privacy practices going forward: rather, the consent order still requires Twitter to develop a comprehensive information security program

---

Protect Sensitive Employee Data," *available at* http://www.infolawgroup.com/tags/segalis/ (making this connection).

[45] Chairman Pitofsky's letter cited a dictum from *United States v. American Building Maintenance Industries*, 422 U.S. 271, 277 n.6 (1975) in support of the assertion that Congress has given the FTC jurisdiction to the fullest extent allowed under the Commerce Clause. In 1994, however, Congress limited the FTC's Section 5 jurisdiction to regulate "unfair" practices by adding subsection (n), which provides that a practice is not unfair unless it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." *See generally* Greenfield, *supra* note 25, at 1876-77 (explaining legislative history of 1994 amendment).

[46] Complaint, *In the Matter of Lookout Services, Inc.*, FTC File No. 102 3076, ¶¶ 5-6.

[47] Decision and Order, *In the Matter of Reed Elsevier Inc. and Seisint, Inc.*, FTC File No. 052 3094, §§ I-II; Decision and Order, *In the Matter of CardSystems Solutions, Inc. and Solidus Networks, Inc. d/b/a Pay By Touch Solutions*, FTC File No. 052 3148, §§ I-II.

[48] Decision and Order, *In the Matter* of Lookout Services, Inc., FTC File No. 102 3076, §§ I-III.

and to hire a third-party monitor to perform biannual assessments for the next 20 years.[49] The *Twitter* order reveals that the FTC's ultimate concern in its password cases is to improve privacy practices: that is, even when it uses the notice-and-choice litigation strategy, the FTC will seek relief that reflects the "harm-based" enforcement approach.

4. The FTC Lacks Authority to Require Specific Privacy Practices

A final observation is that Section 5 of the FTC Act plainly does not confer the authority for the FTC to prescribe any specific privacy practices. Thus, the FTC cannot force websites to require passwords to change every 90 days; to suspend user credentials after three unsuccessful log-in attempts; or to prohibit the use of passwords that appear in the *Merriam-Webster Collegiate Dictionary*. The FTC can, however, claim that the combined failure to require passwords to change periodically, to suspend user credentials after a reasonable number of attempts, and to require "strong passwords," comprise a set of practices that "taken together" constitute a Section 5 violation.

Just as importantly, the consent orders do not require the respondents to adopt any specific privacy practices. Rather, the order require the respondents to establish "a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information." These programs will be assessed by third parties every other year for a period of 20 years, and the assessments must certify that the security program provides "reasonable assurance that the security, confidentiality, and integrity of personal information is protected." Such relief is a fitting exercise of FTC powers; far from prescribing the FTC's own determination of "best practices," it instead sets in place a flexible framework to ensure that the respondents' privacy practices evolve appropriately over the next 20 years.[50]

Conclusion

It is impossible to know what password best practices will look like in 20 years: one can easily envision a future where user credentials are replaced with retinal scans or even one where software is so sophisticated that passwords are no longer required at all. For now, it is important to recognize that the FTC expects websites to maintain reasonable password policies that are appropriate to safeguard the personal information they protect. However, it is equally important to recognize that the FTC's authority to regulate passwords is limited to countering "deceptive" conduct affecting commerce and "unfair" conduct that can harm consumers. Critically, the FTC cannot challenge the "fairness" of password failures that consumers are reasonably able to protect themselves from, such as using birthdays or common dictionary words to secure one's

---

[49] Decision and Order, *In the Matter of Twitter, Inc.*, FTC File No. 092 3093, §§ I-III.

[50] *See generally* Letter to Commenter Smith, *In the Matter of Twitter, Inc.*, FTC File No. 092 3093, at 1-2 (addressing commenter's concerns about FTC's authority and competence to prescribe "best practices").

own personal information. Insofar as the FTC brings cases that test the outer limits of this authority in the future — as *Lookout* case seems to do — jurisdictional challenges may become a fruitful area of litigation.