The Heritage Foundation

LEGAL MEMORANDUM

No. 137 | SEPTEMBER 10, 2014

The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?

Alden F. Abbott

Abstract

Over the past decade, the Federal Trade Commission, the federal government's primary consumer protection agency, has pursued over 50 enforcement actions against companies that it deemed had "inadequate" data security practices. However, data security costs due to FTC actions will be passed on at least in part to consumers and should be weighed against the benefits in reduced data breaches. The FTC should carefully consider whether its current policies in this area are cost-beneficial and whether specific reforms would advance the public interest in enhancing data protection in a less burdensome, more welfare-enhancing fashion. The focus should be on punishing data thieves, not on imposing excessive regulatory burdens on legitimate businesses—burdens that could weaken the private sector and impose unwarranted costs on consumers.

Background: The Online Data Security Problem

While the phrase "identity theft" typically brings to mind stolen credit cards and false identity badges, another key area where privacy violations can occur is less visible but equally insidious: corporate data breaches. Companies' online data protection practices have a major impact on consumer privacy. Target's 2013 security breach, for example, involved up to 40 million credit and debit cards,[1] and Wyndham Hotel and Resorts LLP's (Wyndham) infiltration by hackers in 2012 resulted in $10.6 million of fraudulent charges to consumer accounts.[2] Every 79 seconds, personal data are stolen to open false accounts, and businesses lose $22 billion a year from cybercrime, in addition to the economic and personal harm

This paper, in its entirety, can be found at **http://report.heritage.org/lm137**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Key Points

- The Federal Trade Commission can ferret out and prosecute deceitful and fraudulent activity related to data security, but it needs to do a much better job of confining its data security enforcement to cases of deceit or cases in which the costs of the businesses' practices clearly outweigh any benefits they may engender.
- The FTC should carefully consider issuing guidelines, rooted in cost-benefit analysis, that clarify its enforcement intention regarding data protections.
- Congress should seriously consider preempting state authority over data security, given the serious risk that new state enforcement actions and regulations in this area (which inherently implicates interstate commerce) will impose overlapping and prohibitively costly regulatory burdens on business without proven benefits to consumers.
- Appropriate reforms could reduce the excessive costs associated with current FTC policies while maintaining the FTC's essential role in combatting deficient business practices that lead to excessive data security breaches.

this causes their customers whose information is stolen or peddled online.[3]

This problem seems to be growing faster in the United States than in any other country. Fifty-nine percent of the data breaches investigated by the cybersecurity firm Trustwave in 2013 affected U.S. organizations, with the United Kingdom in second place at 14 percent.[4] From July 2013 to April 2014, private data theft increased from 11 percent to 18 percent of online adults, according to a Pew Research study.[5]

Personal information at risk online includes Social Security numbers**,** account passwords, medical records for insurance including blood type information, and financial records such as credit score and bank account access. The huge scale of this problem is mind-boggling: In August 2014, public news sources revealed that a Russian crime ring had stolen 1.2 billion user name and password combinations and over 500 million e-mail addresses, based on material gathered from 420,000 websites.[6]

What, if anything, can and should United States public law enforcement officials do to combat this scourge? Obviously, vigorous criminal prosecution of data thieves is essential. However, given the difficulties involved in finding and punishing these miscreants, who may quickly cross jurisdictions and change identities, this is an imperfect solution.

Do governments also have a role in incentivizing companies to prevent data security theft in the first place? If so, what should that role be?

As a matter of first principles, one may question the desirability of government regulation of data security. Firms have every incentive to avoid data protection breaches that harm their customers, in order to avoid the harm to reputation and business values that stems from such lapses. At the same time, firms must weigh the costs of alternative data protection systems in determining what the appropriate degree of protection should be.

Economic logic indicates that the optimal business policy is not one that focuses solely on implementing the strongest data protection system program without regard to cost. Rather, the optimal policy is to invest in enhancing corporate data security up to the point where the marginal benefits of additional security equal the marginal costs, and no further. Although individual businesses can approximate this outcome only roughly, one may expect that market forces will tend toward the optimal result as firms that underinvest in data security lose customers and firms that overinvest in security find themselves priced out of the market.

There is no obvious "market failure" that suggests the market should not work adequately in the data security area. Indeed, there is a large (and growing) amount of information on security systems available to business, and there is a thriving labor market for IT security specialists to whom companies can turn in designing their security programs. Nevertheless, government is accelerating its efforts to oversee data security practices, and it is unrealistic to believe that it will cease to regulate in this area, at least for the foreseeable future. With that in mind, let us examine more closely the problems with existing government enforcement in this area, primarily undertaken by the U.S. Federal Trade Commission (FTC).

The FTC, the federal government's primary consumer protection agency, recently has sought to regulate companies' data security practices through informal business guidance and, most significantly, litigation. Over the past decade, the FTC has pursued over 50 enforcement actions against companies that it deemed had "inadequate" data security practices. Most of these cases resulted in consent decrees—binding agreements with the FTC in which

1. Jared Newman, *The Target Credit Card Breach: What You Should Know*, TECHLAND.TIME.COM (Dec. 13, 2013), http://techland.time.com/2013/12/19/the-target-credit-card-breach-what-you-should-know/.
2. Katy Bachman, *FTC Sues Wyndham Over Data Breaches*, ADWEEK.COM (June 26, 2012), http://www.adweek.com/news/technology/ftc-sues-wyndham-over-data-breaches-141450.
3. *45 Stories About Recovering from Identity Theft*, IDENTITY THEFT PROTECTION, http://www.identitytheftprotection.net/45-stories-about-recovering-from-identity-theft/ (last visited Aug. 26, 2014).
4. Sabrina Korber, *Data Breach! U.S. Tops List of Victims, Study Shows*, CNBC (May 21, 2014), http://www.cnbc.com/id/101690847#.
5. Dara Kerr, *Personal Data Theft Jumps from 11% to 18% in Six Months*, CBS INTERACTIVE, INC. (Apr. 14, 2014), http://www.cnet.com/news/personal-data-theft-jumps-from-11-to-18-percent-in-six-months/.
6. Nicole Perlroth and David Gelles, *Russian Hackers Amass Over a Billion Internet Passwords*, NEW YORK TIMES (Aug. 5, 2014), *available at* http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0.

the company agrees to specific reforms in its practices, subject to penalties for violation.

Data security undoubtedly is an important aspect of consumer protection. The FTC argues that closer regulation of data security practices is necessary to protect consumer information and avoid breaches of privacy, particularly as the larger issue of identity theft has expanded to harm 16.6 million Americans.[7] Businesses, however, are justifiably concerned about high regulatory burdens that stem from FTC requirements on top of consumer privacy policies already in place. Data security costs due to FTC actions will be passed on at least in part to consumers, and these costs should be weighed against the benefits in reduced data breaches. Overall welfare effects of FTC enforcement in this area are far from certain.

Accordingly, the FTC should carefully consider whether its current policies in this area are cost-beneficial and whether specific reforms would advance the public interest in enhancing data protection in a less burdensome, more welfare-enhancing fashion.

FTC Data Security Authority

The FTC enforces three targeted laws that oblige certain types of businesses to act reasonably in protecting consumer data.

- The commission's Safeguards Rule, which it adopted pursuant to the Gramm–Leach–Bliley Act, sets forth data security requirements for non-bank financial institutions.[8]
- The Fair Credit Reporting Act (FCRA) requires that consumer reporting agencies use reasonable precautions to ensure that the entities to which they disclose sensitive consumer information have a permissible scope for receiving that information[9] and imposes safe disposal obligations on entities that maintain consumer report information.[10]
- The Children's Online Privacy Protection Act (COPPA) requires reasonable security measures to safeguard children's information collected online.[11]

Most of the FTC's privacy-related work, however, is based on its core general authority to proscribe unfair or deceptive acts or practices under Section 5(a)(1) of the Federal Trade Commission Act.[12] Although deception and unfairness are covered in the same statutory section, they represent different concepts.

The FTC defines "deception" as involving a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[13] Thus, deception occurs only when business conduct causes tangible harm to consumers who acted reasonably and were misled.

By comparison, conduct is "unfair" if it involves "an act or practice [that] causes or is likely to cause substantial injury to consumers which is not reasonably avoided by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[14] This necessarily calls for cost-

7. *Data Breach on the Rise: Protecting Personal Information from Harm, Hearing Before the S. Comm. on Homeland Security and Govt. Affairs,* 113th Cong. (2014) (prepared statement of the Fed. Trade Comm'n) ("Prepared Statement"), *available at* http://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf (last visited Aug. 25, 2014). Statistics regarding the number of FTC data protection settlements under the commission's various statutory authorities (summarized in the following main text discussion) are drawn from this Prepared Statement.
8. 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).
9. U.S.C. § 1681e.
10. 15 U.S.C. § 1681w.
11. 15 U.S.C. §§ 6501–6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").
12. 15 U.S.C. § 45(a)(1).
13. FTC Policy Statement on Deception, Oct. 14, 1983, appended to Clifford Associates, Inc., 103 F.T.C. 110, 174 (1984), http://www.ftc.gov/ftc-policy-statement-on-deception.
14. 15 U.S.C. § 45n.

benefit analysis,[15] since it weighs potential efficiencies against consumer harm, which makes it a more stringent test than deception. As FTC Commissioner Joshua Wright (both an academic economist and a lawyer) recently put it, "[t]his [unfairness] standard calls for an economic analysis of the allegedly unfair business practice. The economic analysis it invites is an appropriately flexible one—incorporating not only the harms to aggrieved consumers but also any benefits to consumers or to competition more generally."[16]

FTC Data Security Cases

Since 2002, under its deception and unfairness authorities,[17] the FTC has filed and settled over 50 cases against private companies, arguing that they compromised consumers' security by using deceptive or ineffective (unfair) practices in storing their data. Among them were suits against Twitter; LexisNexis; ChoicePoint; GMR Transcription Services; GeneLink, Inc.; Accretive Health, Inc.; and mobile device provider HTC. These cases involved complaints that would have been adjudicated administratively within the commission had they not been settled. Settlements involve "consent decrees" under which a company agrees to cease practices the FTC deems unlawful and to take various "corrective measures" to prevent future harm. (The FTC may seek civil fines in federal court for a violation of a consent decree.)

As an example of decree-related obligations that the FTC imposes on companies, HTC was required to establish a comprehensive security program, undergo independent security assessments for 20 years, and develop and release software patches to fix security vulnerabilities.[18] HTC also agreed to detailed security protocols that would be monitored by a third party. The FTC did not cite any specific harmful security breaches to justify these sanctions; HTC was merely charged with a failure to provide reasonable and appropriate security in the design of its smartphone software. The decree did not explain, however, what specific steps short of the decree requirements would have been deemed "reasonable."

The HTC settlement exemplifies the FTC's "security by design" approach to data security. This approach informs firms after the fact what they should have done without exploring what they might have done to pass agency muster. It is inherently vague and puts the FTC in the position of being a "data security systems designer."[19]

The FTC's regulation of business systems by decree threatens to stifle innovation by companies related to data security and to impose costs that will be passed on in part to consumers. Missing from the consent decree calculus is the question of whether the benefits in diminished data security breaches justify those costs—a question that should be at the heart of unfairness analysis. There are no indications that the FTC has even asked this question in

15. *See, e.g.*, J. Howard Beales III, Director, Bureau of Consumer Protection, Fed. Trade Comm'n, The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection, Address before the Marketing and Public Policy Conference (May 30, 2003), *available at* http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection. Current FTC Commissioner Josh Wright also has stressed the importance of cost-benefit analysis. *See, e.g.*, Joshua D. Wright, Commissioner, Fed. Trade Comm'n, The Economics of Access to Civil Justice: Consumer Law, Mass Torts, and Class Actions, Remarks to the George Mason University Law & Economics Center and Alliance of California Judges (March 16, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/293621/140316civiljustice-wright.pdf.

16. Joshua D. Wright, Commissioner, Fed. Trade Comm'n, The Economics of Digital Consumer Protection: One Commissioner's View, Remarks to TechFreedom and the International Center for Law and Economics (July 31, 2014), at 13, *available at* http://www.ftc.gov/system/files/documents/public_statements/573061/010731techfreedom.pdf.

17. Over 30 involved claims of deception, and over 20 involved claims of unfairness. In addition, some cases alleged deception and unfairness, as well as violations of the Safeguards Rule, FCRA, and COPPA.

18. *See* FTC, "HTC America, Inc.; Analysis of Proposed Consent Order to Aid Public Comment," 78 Fed. Reg. 13,673 (Feb. 28, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130228htcfrn.pdf.

19. Professors Daniel Solove and Woodrow Hartzog argue that FTC data security settlements create a "common law" framework of precedents that provide adequate guidance to industry. *See* Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014). Their analysis, however, does not adequately address the questions of whether the FTC is appropriately applying its Section 5 authority in finding unfairness and deception and whether it is imposing undue burdens on business by failing to provide any guidance beyond that found in fact-bound case-specific decrees.

fashioning data security consents, let alone made case-specific cost-benefit analyses. This is troubling.

Equally troubling is the fact that the FTC apparently expects businesses to divine from a large number of ad hoc, fact-specific consent decrees with varying provisions what they must do vis-à-vis data security to avoid possible FTC targeting. The uncertainty engendered by sole reliance on complicated consent decrees for guidance (in the absence of formal agency guidelines or litigated court decisions) imposes additional burdens on business planners.

Rather than accept onerous consent decree terms, why do almost no businesses litigate the validity of FTC complaints regarding their data security policies? The reason is simple: the high costs and unlikelihood of prevailing in administrative litigation. In particular, most firms will accede to onerous consent decree provisions that quickly settle a matter rather than absorb the high and uncertain costs of administrative investigations that may drag on for years, interfering with business operations and sullying corporate reputations.

The hazards of pursuing long-term administrative litigation against the FTC are exemplified by the case of LabMD, a small Atlanta, Georgia-based cancer detection lab. During the course of a protracted FTC investigation into whether the company's security practices were "unreasonable,"[20] LabMD absorbed enormous costs. In its most recent (and unsuccessful) motion to dismiss the administrative complaint against it, LabMD argued that the FTC failed to prove that harm to consumers was "likely" or "substantial" even after four and a half years of "investigation at taxpayer expense."[21] Although the FTC alleged that LabMD's lackluster security practices caused certain sensitive data to be exposed (including hundreds of customer names and Social Security numbers), not a single "identifiable victim of identity theft, medical identity theft, or fraud" could be found to have resulted from that exposure.[22] However, due to the burden of the investigation, LabMD was forced to wind down its operations, and it stopped accepting new patients in January 2014.

LabMD currently is seeking to enjoin the FTC's investigation in federal court, challenging the FTC's authority to regulate patient information data security practices that are also overseen by the U.S. Department of Health and Human Services.[23] The FTC's ability to drag out investigations in matters such as this, even where harm appears to be merely "abstract" and "speculative," creates a strong incentive for companies to avoid future pain by agreeing quickly to intrusive consent decree terms.

The LabMD case also suggests that FTC data security investigations carried out without regard to the scale or resources of the company under investigation have the potential to harm competition. Relatively larger companies (such as Twitter, LexisNexis, and other highly capitalized firms) may be much better able to absorb FTC investigation and litigation costs than are small firms such as LabMD. Thus, data security investigations that are not tailored to the size and capacity of the firm may impose competitive disadvantages on smaller rivals in industries in which data protection issues are paramount.

Moreover, it may be in the interest of very large firms to support costlier and more intrusive FTC data security initiatives, knowing that they can better afford the adoption of prohibitively costly data security protocols than their smaller competitors can. This is an example of a "raising rivals' costs"

20. *See* Press Release, Fed. Trade Comm'n, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy (Aug. 29, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers. This matter is still being actively litigated before an administrative law judge at the FTC, *see* FTC, *In the Matter of LabMD, Inc.* (last updated Aug. 11, 2014), http://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

21. Respondent's Motion to Dismiss, FTC, *In the Matter of LabMD, Inc.* (May 27, 2014), http://www.ftc.gov/system/files/documents/cases/140527respmtndismiss.pdf.

22. *See id*.

23. *LabMD Sues Federal Trade Commission*, Cause of Action (Mar. 20, 2014), http://causeofaction.org/labmd-sues-federal-trade-commission-2/. This case was filed in the Federal District Court for the Northern District of Georgia in March 2014. For all of the FTC-related federal court filings by the Cause of Action firm on behalf of LabMD (some of which raise a number of additional legal questions), *see* Related Documents: Federal Trade Commission v. LabMD, Cause of Action, http://causeofaction.org/related-documents-federal-trade-commission-v-labmd/ (last visited Aug. 26, 2014).

strategy,[24] which reduces competition by crippling or eliminating rivals. When successful, such a strategy harms ultimate consumers, who obtain costlier and less desired goods and services. The FTC, as a consumer watchdog agency, should keep this potential unintended consequence very much in mind when formulating its data protection initiatives and litigation practices.

The only other ongoing federal court challenge to the FTC's authority over data security involves the hotel chain Wyndham Worldwide. In June 2012, the FTC brought a civil enforcement action against Wyndham's data security practices in federal court.[25] The FTC stated that Wyndham erroneously told its customers it was using "commercially reasonable methods" to protect their information, a claim called into question when hackers stole data on more than 619,000 consumer credit-card accounts and charged $10.6 million fraudulently.

In April 2014, the U.S. District Court in New Jersey rejected Wyndham's effort to dismiss the FTC's lawsuit and upheld the FTC's authority to challenge defective "corporate data-security practices" without having to promulgate specific regulations in that area.[26] In June 2014, that court denied the request by Wyndham's parent company that it be dropped from the case. U.S. District Judge Esther Salas held that the parent company should be subject to sanctions as well because it could not be "separated from a third subsidiary whose systems were allegedly breached."[27] If the FTC's authority to bring suit to challenge "inadequate" data protection policies is upheld on appeal, firms' already strong incentives to settle FTC complaints quickly will grow even stronger.

Another recent consent agreement with potentially far-reaching implications is that of TRENDnet, the first "Internet-of-Things" case, in which in-home security video cameras were hacked and "left open to online viewing" of 700 consumers' live feeds.[28] Cameras are considered to be part of the "Internet-of-Things," a category of consumer products with their own interconnectivity to the Internet and other electronic devices.[29]

Like most other companies facing an FTC complaint over data security, TRENDnet promptly agreed to a consent agreement imposing a new security program requirement, outside audits, and a requirement to notify consumers about company security and software capabilities. TRENDnet must now provide free technical support for the next two years to affected consumers, and third-party assessments of its security programs are required every two years for the next 20 years.

As Internet access and commercial transactions via mobile electronic devices have become routine, the FTC's authority to regulate the "Internet-of-Things" will likely reappear in future cases. If handled inappropriately, without regard to costs and benefits, FTC enforcement in this area could harmfully restrict companies' ability to develop new Internet-of-Things-related products and services desired by consumers.

While the FTC should be careful to limit the negative effects of its data security investigations on innovation, it should continue to monitor companies that blatantly disregard security precautions. For instance, mobile app companies Credit Karma and Fandango were charged with compromising

24. *See generally*, *e.g.*, David T. Scheffman and Richard S. Higgins, *Twenty Years of Raising Rivals' Costs: History, Assessment, and Future*, 12 Geo. Mason L. Rev. 371 (2003), http://www.georgemasonlawreview.org/doc/12-2_Scheffman-Higgins.pdf.

25. Press Release, Fed. Trade Comm'n, FTC Files Complaint Against Wyndham Hotels for Failure to Protect Consumers' Personal Information (June 26, 2012), *available at* http://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect. For a compendium of FTC federal court filings against Wyndham, *see* FTC Cases and Proceedings: Wyndham Worldwide Corporation, http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation (last visited Aug. 25, 2014).

26. Brent Kendall, *Judge Backs FTC's Authority in Data-Breach Case*, The Wall Street Journal (Apr. 7, 2014), *available at* http://online.wsj.com/news/articles/SB10001424052702304819004579487832665956494.

27. Allison Grande, *Wyndham Can't Break from Unit in FTC Data Security Row*, Law360 (Jun. 23, 2014), http://www.law360.com/articles/550884/wyndham-can-t-break-from-unit-in-ftc-data-security-row.

28. *See* Press Release, Fed. Trade Comm'n, FTC Approves Final Order Settling Charges Against TRENDnet, Inc. (Feb. 7, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

29. *See*, *e.g.*, Maureen K. Ohlhausen, Commissioner, Fed. Trade Comm'n, The Internet of Things: When Things Talk Among Themselves, remarks at Internet of Things Workshop (Nov. 19, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen-ftc-internet-things-workshop/131119iotspeech.pdf.

customers' security, and they settled with the FTC in March 2014.[30]

According to the FTC, both companies engaged in "unfair business practices by failing to properly implement Secure Sockets Layer (SSL) encryption on their mobile apps." This increased their customers' risk of receiving "man-in-the-middle" attacks from data thieves. Both companies also acted deceptively. Credit Karma, a mobile app allowing customers to access their credit reports, had disabled SSL systems for testing and distributed the app without reinstalling them, despite its claim to consumers that it took "industry-leading security precautions."[31] Fandango also failed to test its security systems, despite its claim to customers that their data would be securely stored. Credit Karma was charged with exposing Social Security numbers, birthdates, and credit report information, while movie ticket app Fandango allegedly exposed credit card information. Only after the FTC contacted Credit Karma did the company run a security check, which revealed that although it knew about its iOS vulnerability, the company launched the Android version of its app with the exact same problem.

Both Credit Karma and Fandango were made subject to independent audit requirements for the next 20 years and required to install "comprehensive information security programs." In light of the serious concerns these cases raised concerning consumer data security online, the companies' apparent failure to maintain even minimal security precautions, and the companies' deceptive claims regarding security, it appears likely that the FTC's enforcement initiative was cost-beneficial.

Other FTC Data Protection Initiatives

The FTC increasingly is pursuing non-litigation initiatives, including workshops, speeches, and testimony, to promote data security. For instance, in November 2013, the FTC hosted a public forum on mobile security issues and workshop on the "Internet of Things"[32] and created OnGuard Online to educate consumers about privacy when making online accounts and purchases.[33]

In the FTC's April 2, 2014, statement before the Senate Committee on Homeland Security,[34] Chairwoman Edith Ramirez stipulated that companies should keep track of their consumer information and who has access to it, "properly dispos[ing] of information that they no longer need." She pointed out the risks of "needless storage of data" and recommended "physical security, electronic security, employee training, and oversight of service providers." In addition, the FTC recommended legislation that would further empower it to enforce its policies, such as stronger "existing authority governing data security standards" and rules requiring companies to inform consumers of security breaches. The FTC also has organized a workshop to explore appropriate policies toward "big data," a term used to refer to advancing technologies that are dramatically expanding the commercial collection, analysis, use, and storage of data.[35]

One FTC Commissioner has suggested that the FTC proceed cautiously in pursuing data protection regulation that extends beyond core enforcement actions. In her keynote address at the Georgetown Law Center on April 22, 2014, Commissioner Maureen Ohlhausen pointed out important considerations that challenge traditional regulatory models, particularly with the advent of big data and online purchases. Due to the increasingly fluid nature of online data use, "companies cannot give notice at the time of collection for unanticipated uses."[36]

As with other regulations, the FTC should be careful that its attempts to improve security do

30. *See* Press Release, Fed. Trade Comm'n, Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers by Failing to Securely Transmit Sensitive Personal Information (Mar. 28, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers.

31. *Id.*

32. *See Internet of Things—Privacy and Security in a Connected World*, Fed. Trade Comm'n (Nov. 19, 2013), *available at* http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

33. *See* OnGuard Online, http://www.onguardonline.gov/ (last visited Aug. 25, 2014).

34. *See* Prepared Statement, *supra* note 7.

35. *See* Press Release, Fed. Trade Comm'n, *FTC Announces Agenda for Upcoming Big Data Workshop*, Federal Trade Commission (Aug. 8, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/08/ftc-announces-agenda-upcoming-big-data-workshop.

36. Mark MacCarthy, *Ohlhausen on Big Data and Consumer Harm*, SIIA Digital Discourse (Apr. 22, 2014), http://www.siia.net/blog/index.php/2014/04/ohlhausen-on-big-data-and-consumer-harm/.

not stymie innovative abilities. Ohlhausen argued that "strictly limiting the collection of data to the particular task currently at hand and disposing of it afterwards would handicap the data scientist's ability to find new information to address future tasks."[37] Despite the changes of advancing technology, Ohlhausen contended that the FTC "should use its traditional deception and unfairness authority to stop consumer harms that may arise from the misuse of big data"[38] instead of forming more stringent requirements that will prevent the flexibility necessary to use advancing technology.

Closely related to these data protection initiatives is the FTC's interest in the activities of data brokers, companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies. As the FTC explained in 2012 in launching a study of data brokers' privacy practices, "while data brokers collect, maintain, and sell a wealth of information about consumers, they often do not interact directly with consumers. Rather, they get information from public records and purchase information from other companies."[39]

In May 2014, the FTC issued a report based on this study, recommending that Congress consider enacting legislation that would allow consumers "to learn of the existence and activities of data brokers and provide consumers with reasonable access to information about them held by these entities."[40] In particular, the report suggested that Congress require that data brokers provide a centralized portal giving consumers access to private data they hold, provide a variety of notices to consumers, describe the inferences drawn from consumer data, and allow consumers to suppress the use of their data, among other mandates. The report also urged that merchants be required to inform customers about which data broker's information they relied upon in limiting a consumer's ability to complete a transaction, enable consumers to require that data brokers correct information, and allow consumers to opt out of having their information included in "people search" products.

In short, the FTC's data broker report recommended that a large number of limitations be placed on lawful companies that employ consumer data without inquiring into whether such onerous new requirements would prove cost-beneficial to producers or to consumers (whose online purchases and searches might be rendered less efficient by such new restrictions). The report also failed to undertake a serious empirical analysis of consumer harm in this area.

This is highly problematic. In commenting on the report, FTC Commissioner Joshua Wright recently highlighted the serious problems with this approach:

> I would ... like to see evidence of the incidence and scope of consumer harms rather than just speculative hypotheticals about how consumers might be harmed before regulation aimed at reducing those harms is implemented. Accordingly, the FTC would need to quantify more definitively the incidence or value of data broker practices to consumers before taking or endorsing regulatory or legislative action....
>
> We have no idea what the costs for businesses would be to implement consumer control over any and all data shared by data brokers and to what extent these costs would ultimately be passed on to consumers. Once again, a critical safeguard to insure against the risk that our recommendations and actions do more harm than good for consumers is to require appropriate and thorough cost-benefit analysis before acting. This failure could be especially important where the costs to businesses from complying with any recommendations are high, but where

37. The Power of Data, Maureen K. Ohlhausen, Commissioner, Fed. Trade Comm'n, Remarks at the Georgetown University McCourt School of Public Policy and Georgetown Law Center (Apr. 22, 2014),*available at* http://www.ftc.gov/system/files/documents/public_statements/299801/140422georgetownbigdataprivacy.pdf.

38. *Id.*

39. Press Release, Fed. Trade Comm'n, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), *available at* http://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data.

40. Press Release, Fed. Trade Comm'n, FTC Recommends Congress Require the Data Broker Industry to Be More Transparent and Give Consumers Greater Control Over Their Personal Information (May 27, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more.

> the ultimate benefit generated for consumers is minimal.... If consumers have minimal concerns about the sharing of certain types of information—perhaps information that is already publicly available—I think we should know that before requiring data brokers to alter their practices and expend resources and incur costs that will be passed on to consumers.[41]

Consistent with Commissioner Wright's analysis, the FTC would be well advised to withdraw its legislative recommendations pertaining to data brokers and to refrain from further regulatory proposals in this area that are not backed by detailed cost-benefit analysis.

State Data Security Regulation Creates Excessive and Inappropriate Burdens

FTC initiatives are supplemented by an increasing number of state government actions bearing on data security. Forty-seven states now have legislation "requiring private or government entities to notify individuals of security breaches of personally identifiable information."[42] Such state "information protection acts" add additional burdens on businesses to those already imposed by the FTC.

Florida's Information Protection Act, passed in May 2014, is typical. It requires businesses to notify the Florida Attorney General if they experience any breach that would affect more than 500 residents.[43] This law also expands the definition of "personally identifiable information" to include consumers' usernames and passwords, which will result in a greater number of incidents qualifying as data breaches that could subject companies to further sanctions.[44]

Under this statute, the Florida Attorney General's request for documents can easily expand to a public records request, which would make proprietary information public and thus damage the company's security system that the law originally was meant to protect. One commentator predicts that breached entities will respond either by "not requesting [incident] reports at all" or by requesting a "sanitized" version for the Attorney General while keeping their own more substantive records secret—another result the law attempted to avoid. In short, this law and other state laws like it may be counterproductive to the extent that they incentivize greater business data secrecy, which would hurt consumers in the long run.

Given the inherently interstate nature of electronic commerce and associated data breaches, state regulation in this area appears to be inappropriate. In addition to the extra burdens and counterproductive effects of the above-identified state laws, differences among state statutes render the data protection efforts of merchants who may have to safeguard data from across the country enormously complex and exceedingly onerous.

Thus, consistent with federalism, relying solely on *appropriate* FTC data protection initiatives appears significantly preferable to relying on burgeoning state regulation. Federal preemptive legislation, however, would be required to achieve this end.

FTC and State Data Protection Initiatives in Perspective

The FTC can play a useful role in ferreting out and prosecuting deceitful and fraudulent activity related to data security—activity that harms consumers and has no redeeming features other than obtaining business for the fraudsters. It needs to do a much better job, however, of confining its data security enforcement to cases of deceit or cases in which the costs of the businesses' practices clearly outweigh any benefits they may engender.

This is a stringent test, but it is crucial that cost-benefit considerations remain paramount in an industry sector characterized by rapid innovation. The rate of introduction of new and highly desired online services sought by consumers could slow significantly if the FTC imposes overly stringent enforcement policies that fail to weigh costs and benefits.

41. Wright, *supra* note 16, at 18–19.
42. Judith H. Germano and Zachary K. Goldman, *After the Breach: Cybersecurity Liability Risk*, The Center on Law and Security, NYU School of Law, http://www.lawandsecurity.org/Portals/0/Documents/CLS%20After%20the%20Breach%20Final.pdf (last visited Aug. 25, 2014).
43. Companies must notify the state attorney general even of breaches about which they would not ordinarily inform consumers because of potential future state liability. Al Saikali, *Why Every Business Should Care About Florida's Information Protection Act*, Data Security Law Journal, May 26, 2014, http://www.datasecuritylawjournal.com/.
44. *Id.*

Relatedly, given the costly uncertainty associated with reliance on consent decrees in the absence of judicial guidance, the FTC should carefully consider issuing guidelines, rooted in cost-benefit analysis, that clarify its enforcement intention regarding data protections. Similarly, the commission should proceed cautiously in light of cost-benefit analysis before promoting new sorts of data protection–related regulation that involves data brokerage, the use of "big data," or related novel business practices. FTC efforts to recommend new business restrictions that ignore this advice could stymie business innovations and reduce consumer welfare.

Finally, Congress should seriously consider preempting state authority over data security, given the serious risk that new state enforcement actions and regulations in this area (an area that inherently implicates interstate commerce) will impose overlapping and prohibitively costly regulatory burdens on business without proven benefits to consumers.

What Specific Reforms Are Needed?

Appropriate reforms could reduce the excessive costs associated with current FTC policies while at the same time maintaining the FTC's essential role in combatting deficient business practices that lead to excessive data security breaches.

First, the FTC should issue data security guidelines that clarify its enforcement policy regarding data security breaches pursuant to Section 5 of the Federal Trade Commission Act. Such guidelines should be framed solely as limiting principles that tie the FTC's hands to avoid enforcement excesses. They should studiously avoid dictating to industry the data security principles that firms should adopt. These guidelines might, for example, specify that:

- The FTC will employ a cost-benefit approach in assessing all potential "unfairness" cases based on the alleged failure of a business to safeguard data adequately.

- Consistent with cost-benefit considerations, the FTC will prioritize cases of hard-core fraud (for example, explicit and false claims that a company offers data security protection).

- The FTC will eschew any sort of "strict liability" standard in all of its data security cases.

- The FTC will encourage private-sector organizations to consider discussing and developing non-binding data security best practices protocols, which could be shared broadly and made publicly available.

- The FTC will take into account these and other informal self-regulatory mechanisms and the practices they embody in developing and (if and when appropriate) revising the guidelines.

- In each matter it investigates for "unfairness," the FTC will determine, based on the specific facts on hand, whether a data breach involves business conduct that (1) has imposed or is likely to cause substantial injury to consumers that (2) could not reasonably have been avoided and (3) is not outweighed by countervailing benefits to consumers or to competition.

- In weighing potential benefits, the FTC will ask whether any potential remedy it might seek to impose (for example, new costly changes in business procedures or technologies) will impose higher costs on consumers and business that are greater than the likely costs of future breaches that will be averted. The FTC will consider imposing only a remedy that meets this cost-benefit test. If the costs of *each* potential remedy outweigh the harm of averted future breaches, the FTC will not bring an enforcement action.

- Even if all three unfairness factors are met, the FTC will not bring an enforcement action unless it determines that the business under investigation acted unreasonably, taking into account best industry practices extant. (Business unreasonableness may be reflected in inappropriate action or inaction that fails to meet best current standards.)

- The FTC will develop protocols to limit investigative costs imposed on business (for example, by avoiding excessive demands for interviews and superfluous documents) and to tailor investigative demands to the resources and scale of the entity under investigation. It should also place tighter time limits on administrative inquiries. The goal should be to avoid situations such as the LabMD investigation whose costs may have driven that small company out of business.

- The FTC will take into account the merits of informal self-regulatory efforts, including non-binding protocols, in gauging the reasonableness of particular business conduct.

- The FTC will also gauge the scale of and the resources available to the business under investigation in determining whether it acted reasonably.

- In each matter it investigates for "deception," the FTC will determine whether the business acted in a manner, with regard to data security, that (1) is likely to mislead a consumer who (2) is acting reasonably under the circumstances (3) to the consumer's detriment.

- The FTC will take into account current market conditions in evaluating the reasonableness of consumer actions. It will also require that detriment suffered by consumers be non-trivial before proceeding with a possible enforcement action.

- Before issuing the guidelines, the FTC will convene a series of workshops in which all points of view will be heard. It will then produce a draft set of guidelines and request public comments on the draft before finalizing them.

- The FTC will strictly adhere to the guidelines in all of its enforcement actions. If it believes that the guidelines require modification (for example, in light of changes in consumer expectations or reasonable business practices), it will make a public announcement to that effect, explaining its reasoning, and allow for at least 90 days of public comment on proposed modified guidelines before finalizing them.

- The FTC should review the Safeguards Rule to determine whether it merits being revised in light of the new guidelines (and future possible modifications to the guidelines).

Second, the FTC should consider establishing an online "data security information clearinghouse" portal on its website. The portal should not be designed to advance particular government-recommended policies, but rather to provide businesses with information they may deem valuable in devising their data protection policies. In particular, the portal should include, among other constantly updated information:

- The guidelines, the Safeguard Rule, and other regulatory and advisory materials involving data security generated by the FTC and other government entities;

- The status of enforcement actions by the FTC and other agencies regarding data security;

- Publicly available information regarding data security breaches that are reported to be occurring, here and abroad;

- Private self-regulatory efforts and other "best practices" initiatives aimed at stemming data security breaches (including any results);

- The status of government enforcement actions regarding data security breaches; and

- International enforcement, policy, and news developments regarding data security.

Third, the FTC should employ a strict cost-benefit analysis before pursuing any new regulatory initiatives, legislative recommendations, or investigations related to other areas of data protection, such as data brokerage or the uses of big data. More specifically, the FTC should announce that until further notice, it is withdrawing the legislative recommendations that it made in releasing its data brokerage report.

Fourth, Congress should consider enacting a carefully tailored, narrow statute that preempts state data security regulations. This would reduce excessive and duplicative state burdens on business and related costs passed on to consumers. *Such legislation should not, however, authorize the FTC to obtain civil penalties as an initial remedy*: The FTC's existing administrative and injunctive authorities should remain the tools available to sanction inappropriate data privacy policies. (The FTC would retain the right, which it now has, to seek civil penalties in federal court for violations of FTC orders, including agreements adopted through consent decrees.)

Although there is some risk that Congress might be tempted to go beyond narrow preemption and create new and unnecessary federal powers in this area, such a risk is worth running, given the poten-

tial magnitude of excessive state regulatory burdens and the ability to articulate a persuasive public policy case for narrow preemptive legislation.

Fifth, in its regular meetings with counterpart consumer protection agencies around the world, the FTC should urge them to adopt a cost-beneficial approach to data security prevention that is in line with the preceding suggestions. Such an approach could be touted as being in the interests of private-sector economic growth as well as ultimate consumer welfare.

These recommendations are no panacea, and the efforts of law enforcers both here and abroad will need to be mobilized to ferret out and punish the true villains: data thieves. The focus, though, should be on punishing the thieves, not on imposing excessive regulatory burdens on legitimate businesses—burdens that could both weaken the private sector and impose unwarranted costs on consumers.

*—**Alden F. Abbott** is Deputy Director of the Edwin Meese III Center for Legal and Judicial Studies and John, Barbara, and Victoria Rumpel Senior Legal Fellow at The Heritage Foundation. The author gratefully acknowledges Kayla Murrish for her research in connection with this paper.*