COMMENTS

REGULATING DATA PRACTICES: HOW STATE LAWS CAN SHORE UP THE FTC'S AUTHORITY TO REGULATE DATA BREACHES, PRIVACY, AND MORE

GREGORY JAMES EVANS*

TABLE OF CONTENTS

Introduction 188
I. Data Practices and Privacy: How Data Practices are Viewed in a Privacy Framework 193
II. FTC Act: A Brief Look at the Commission's Scope and the *Wyndham* Challenge 201
III. State Level Movement on Security and Privacy: California as a Case Study 205
A. Conditions are Not the Same on the Federal Level 207
B. FTC, Commerce, and the White House All Want What California Already Has 209
IV. Federal-State Collaboration: How FTC can Regulate Data Practices by Indirectly Using State Laws 212
A. Triggering the FTC's Authority in this Proposed Regulatory Scheme 214
Conclusion 218

* J.D. Candidate, American University Washington College of Law, 2015; B.A. Philosophy, Politics & Economics, Pomona College, 2008. The author would like to thank Professor Jeffrey Lubbers and the *ALR* editors for their feedback and guidance throughout the writing process. What follows is an objective examination of privacy and data practices, followed by a recommendation. Any opinions expressed in this comment are the author's alone.

INTRODUCTION

Although the Federal Trade Commission (FTC or Commission) is authorized to regulate unfair or deceptive practices,[1] it was not until early 2014 that a court first held that the Commission's authority extends to regulating data security as an unfair practice.[2] By that time, FTC had already entered into over fifty consent agreements with companies regarding data security practices under its unfair or deceptive practices authority.[3] Those consent orders are essentially settlements prior to trial.[4] While the Commission has more than a decade of history of successfully regulating data security, it does not have a line of judicially decided cases supporting its authority.[5]

The Commission faced a significant legal challenge to its authority to regulate data security as an "unfair" practice in *Federal Trade Commission v. Wyndham*.[6] In *Wyndham*, FTC alleged that Wyndham Worldwide, a large hotel chain, failed to maintain reasonable and appropriate data security practices, allowing hackers to access consumers' information on three

1. Federal Trade Commission (FTC) Act, 15 U.S.C. § 45(a) (2012).

2. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 615 (D.N.J. 2014); *see* David J. Bender, *Tipping the Scales: Judicial Encouragement of a Legislative Answer to FTC Authority over Corporate Data-Security Practices*, 81 GEO. WASH. L. REV. 1665, 1665 (2013) (describing the challenge as the first opportunity for a court hearing).

3. *See* FTC, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf [hereinafter Commission Statement] (announcing the fiftieth data security settlement on January 31, 2014, just twelve years since the first settlement in 2002); *see also* Transcript of Nov. 7, 2013 Oral Argument on Motion to Dismiss at 21, FTC v. Wyndham Worldwide Corp., No. 13-1887 (ES), 10 F. Supp. 3d 602 (D.N.J. 2014), 2014 WL 1349019 (considering the effect of then-approximately forty data security settlements on the question of whether Congress intended FTC should have authority to regulate data security); FTC, LEGAL RESOURCES, http://business.ftc.gov/legal-resources/29/35 (last visited Nov. 17, 2014) (listing cases FTC has brought charging individuals or companies with deceptive or unfair practices as a result of privacy and data security concerns).

4. The agreements do not require the violating company to admit or deny any of the allegations in FTC's complaints. *See, e.g.*, TRENDnet, Inc., F.T.C. File No. 122 3090 (F.T.C. 2013), *available at* http://www.ftc.gov/sites/default/files/documents/ cases/2013/09/130903trendnetorder.pdf (Agreement Containing Consent Order) (describing the agreement as an admission to only the facts necessary to grant FTC authority, but neither an admission or denial of any of the allegations in the complaint).

5. *See* Bender, *supra* note 2, at 1665 ("The *Wyndham* case . . . represents the first opportunity for judicial review of the extent of the FTC's authority in this area, and the outcome will likely have far-reaching consequences in an area of law that is largely devoid of legislative direction.").

6. *Wyndham Worldwide Corp.*, 10 F. Supp. 3d at 615.

separate occasions in less than two years.[7] FTC alleged that this was an unfair practice under § 5 of the FTC Act.[8] Industry commentators predicted the case would have far-reaching consequences on FTC's ability to regulate data practices.[9] Despite the lack of clear statutory authority to regulate data practices prior to *Wyndham*, FTC exercised its unfair practices authority under § 5 to regulate data security.[10] Critics charged that such authority does not stretch to data security, and that without targeted legislation dealing with various data practices, the Commission exercised its § 5 authority in an area that Congress did not intend.[11]

While FTC prevailed in the district court on the issue of whether data security is within its authority,[12] it is still not clear how FTC will regulate data security and other data practices without new legislation.[13] Industry commentators were quick to point out that the district court's ruling on FTC's authority is far from the type of unambiguous authority necessary to keep up with the speed of the changing electronic landscape.[14]

FTC continues to face significant challenges in keeping pace with a rapidly changing and increasingly complex consumer market.[15] Today,

7. First Amended Complaint for Injunctive and Other Equitable Relief at 2, 5–6, FTC v. Wyndham Worldwide Corp., (No. CV 12-1365-PHX-PGR) (D. Ariz. Aug. 9, 2012), 2012 WL 3281910.

8. *Id.* ¶ 47–49. FTC complaint against Wyndham included allegations of unfair and deceptive practices. *Id.* To be clear, Wyndham contested all of FTC's allegations of wrongdoing, but the case is important because Wyndham challenged FTC's authority to bring a data security case as an unfair practice. *Wyndham Worldwide Corp.*, 10 F. Supp. 3d at 607.

9. *See* Bender, *supra* note 2, at 1665.

10. *See* Motion to Dismiss Defendant Wyndham Hotels & Resort LLC at 1, FTC v. Wyndham Worldwide Corp., (No. CV 12-1365-PHX-PGR), 2012 WL 3916987 (D. Ariz. Aug. 27, 2012) (challenging FTC's authority); Alan L. Friel, *Why We Don't Need the FTC on Big Data Lifeguard Duty: Recent Comments From Chairwoman Are Worrisome*, ADVERTISING AGE (Oct. 8, 2013), http://adage.com/print/244128 (describing how *Wyndham* "may serve to check the creeping expanse of [FTC's] authority").

11. *See* Friel, *supra* note 10; Wyndham Hotels and Resorts' Motion to Dismiss, *supra* note 10, at 9.

12. *Wyndham Worldwide Corp.*, 10 F. Supp. 3d at 615.

13. *See generally* Christopher A. Cole et al., *FTC Data Security Authority Remains Murky Despite* Wyndham, LAW 360 (Apr. 8, 2014, 2:44 PM), http://www.law360.com/articles/525058/ftc-data-security-authority-remains-murky-despite-wyndham.

14. *Id.*

15. *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 2 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter FTC 2012 REPORT] (noting that "privacy frameworks have struggled to keep pace with the rapid growth of technologies and business models that

collecting consumer information is nearly ubiquitous and data breaches can result in substantial harm to consumers and the economy as a whole.[16] The stakes remain high for FTC, and despite the district court's ruling in *Wyndham*, the issue of whether and how FTC can regulate data security and other data practices is far from settled.[17]

Regulating data practices raises questions about the use, control, and security of consumer data, not to mention consumer rights, transparency, and privacy.[18] FTC has repeatedly called on Congress to pass "baseline" privacy and data security legislation.[19] Members have proposed privacy

enable companies to collect and use consumers' information in ways that often are invisible to consumers"); 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/privacy-final.pdf [hereinafter WHITE HOUSE CONSUMER DATA PRIVACY].

16. The term "data breach" refers to "unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers." U.S. GOV'T ACCOUNTABILITY OFFICE (GAO), GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 2 & n.2 (2007), *available at* http://www.gao.gov/new.items/d07737.pdf [hereinafter GAO, PERSONAL INFORMATION]. Identity theft alone caused estimated economic losses of more than $15 billion in a single year. *See* FEDERAL TRADE COMMISSION–2006 IDENTITY THEFT SURVEY REPORT 9 (2007), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-2006-identity-theft-survey-report-prepared-commission-synovate/synovatereport.pdf. In late 2013, a breach of information held by the retail corporation, Target, affected an estimated seventy million consumers whose names, mailing addresses, phone numbers, or email addresses may have been disclosed as the result of a hack. Forty million consumers may have been affected in less than one month alone. *See Data Breach FAQ: Answers to Commonly Asked Questions for Guests Impacted by the Recent Data Breach*, TARGET.COM, https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888 (last visited Oct. 6, 2014); *see generally* TJX Companies, Inc., F.T.C. File No. 072-3055 (F.T.C. 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf (Complaint) (alleging a security breach at a retail store compromised tens of millions of unique payments cards and personal information of over 450,000 consumers, resulting in tens of millions of fraudulent charges).

17. *See* Woodrow Hartzog & Daniel J. Solove, *The FTC as Data Security Regulator:* FTC v. Wyndham *and Its Implications*, 13 PRIVACY & SECURITY L. REP. 621 (BNA Apr. 14, 2014).

18. *See generally* WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 47–48.

19. *See* FTC 2012 REPORT, *supra* note 15, at 12–13 (calling on Congress to act); *Safeguarding Consumers' Financial Data: Hearing Before the S. Subcomm. on Nat'l Sec. & Int'l Trade & Fin. of the Comm. on Banking, Hous., & Urban Affairs*, 113th Cong. 2 & n.4 (2014) (statement of Jessica Rich, Dir. of the FTC Bureau of Consumer Protection) [hereinafter Rich Hearing] (reiterating FTC's request and bipartisan support of data security legislation and citing reports dating back to 2008 to demonstrate the length of time FTC has wanted Congress to act); *see also* GAO, GAO-13-663, INFORMATION RESELLERS: CONSUMER PRIVACY

and data security bills, but Congress has not yet passed significant legislation.[20] In addition, the White House supports legislation consistent with the Consumer Privacy Bill of Rights and enforceable Codes of Conduct,[21] but the White House has so far been unsuccessful in convincing Congress to adopt its recommendations.[22]

Curiously, FTC continues to ask Congress for a legislative answer to a question which FTC simultaneously states that Congress has already provided an answer; in other words, the Commission supports new privacy legislation, giving it the authority to regulate data practices, while asserting that it already has the same authority.[23] And yet, FTC has stated that it lacks authority to address data practices, and the authority it does have is limited to making sure companies follow their own privacy policies.[24] According to the district court, these statements do not equate to a "resolute, unequivocal position" that FTC lacks authority to bring

FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE 32 (2013) [hereinafter GAO, INFORMATION RESELLERS] (noting that both FTC and the White House expressly called on Congress to act).

20. *See* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 143 (2008) ("[T]he Commission pushed for specific legislation to provide broad consumer privacy protection, but Congress thus far has declined to act."); *see* Data Security and Breach Notification Act of 2013, S. 1193, 113th Cong. (2013) (referred to Committee on June 20, 2013). The bill has a five percent chance of making it past committee and a two percent chance of being enacted. This bill was referred to Committee, but never enacted by the 113th Congress. *See S. 1193: Data Security and Breach Notification Act of 2013*, GOVTRACK, https://www.govtrack.us/congress/bills/113/s1193 (last visited Feb. 13, 2015). The 2013 bill found the same fate as similar bills that preceded it. *See, e.g.*, Data Security and Breach Notification Act of 2012, S. 3333, 112th Cong. (2012) (referred to committee, but died in committee); *S. 3333: Data Security and Breach Notification Act of 2012*, GOVTRACK, https://www.govtrack.us/congress/bills/112/s3333 (last visited Feb. 13, 2015); *see, e.g.*, Data Security Act of 2007, H.R. 1685, 110th Cong. (2007) (referred to committee, but died); *H.R. 1685: Data Security Act of 2007*, GOVTRACK, https://www.govtrack.us/congress/bills/110/s1260 (last visited Feb. 13, 2015); Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007) (referred to committee, but died); *S. 239: Notification of Risk to Personal Data Act of 2007*, GOVTRACK, https://www.govtrack.us/congress/bills/110/s239 (last visited Feb. 13, 2015).

21. Both the Consumer Privacy Bill of Rights and the Codes of Conduct would be based on internationally recognized privacy and security principles. *See* WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 6–7.

22. *Id.*

23. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 611–12 (D.N.J. 2014) (noting defendants claims that FTC has asked Congress to give it the very authority it "'purports to wield'"); Cole et al., *supra* note 13 (discussing how "FTC is proceeding as though it has authority on one hand while asking for express" authority on the other hand).

24. *See Wyndham Worldwide Corp.*, 10 F. Supp. 3d at 614 (considering and ultimately finding those statements unpersuasive).

unfairness claims when it comes to data practices.[25] So while FTC won round one, *Wyndham* did not clear up these issues and FTC's authority remains unsettled.[26]

But even without new privacy and data collections laws, FTC still has the power to publish guidelines and reports that state legislatures can use to create or model their own state laws.[27] State legislatures have in the past deferred to FTC interpretations and modeled state laws after federal laws,[28] bringing state law in sync with what FTC would like to see implemented on a national level.[29]

While FTC cannot directly enforce state laws,[30] FTC can act under its § 5 authority when violating state laws also deceives consumers under federal law.[31] In terms of data security, FTC's unfairness authority is still questionable or at the very least, nowhere near as well-established as its deceptive practices authority.[32] The district court granted an interlocutory appeal so the Third Circuit of Appeals could weigh in on what the court called "novel, complex statutory interpretation issues that give rise to a substantial ground for difference of opinion."[33]

As such, FTC should look to shore up its authority to regulate data practices under a deceptive practices analysis. This Comment argues that state level regulatory efforts provide FTC an opportunity to do just that. Increasingly strict, state-level regulations, like those of California, require

25. *Id.*

26. The court's ruling is not a "blank check to sustain a lawsuit against every business that has been hacked." *Id.* at 610. Obviously any suit based on unfairness would have to meet elements of an unfair practice, but beyond that it is unclear why *Wyndham* is not a "blank check" for the FTC. If *Wyndham* is not recognition of full authority then what is it?

27. Commission Statement, *supra* note 3 (describing educational materials provided by FTC to industry and the public to explain the steps a company should take to implement "reasonable data security practices"). These guidelines provide "practical, concrete advice" for developing data security programs, including how to dispose of sensitive digital information. *See* Rich Hearing, *supra* note 19, at 9.

28. *See generally* Justin J. Hakala, *Follow-On State Actions Based on the FTC's Enforcement of Section 5* 7 (2008), *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/section-5-workshop-537633-00002/537633-00002.pdf (describing state laws which incorporate interpretations of FTC, called "state Little FTC Acts").

29. *See infra* 171 and accompanying text; *see also infra* Part III.B.

30. The Commission's authority comes from its empowering act, not a state law. FTC Act, 15 U.S.C. § 45(a) (2012). *See generally Statutes Enforced or Administered by the Commission*, FTC, http://www.ftc.gov/enforcement/statutes (last visited Dec. 14, 2014) (listing FTC enforcement acts which provide authority in addition to the Commission's empowering act).

31. *See* discussion *infra* Part IV (describing state laws that invoke FTC's deceptive practices authority).

32. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 634 (D.N.J. 2014).

33. *Id.*

companies to make public commitments about the information they collect.[34] FTC can regulate data practices by going after companies when they fail to keep commitments made in response to smartly designed state laws that require companies make representations about their data practices.[35]

This Comment examines FTC's efforts to regulate data practices by first explaining how data practices, including collecting and securing consumer information, are viewed within a privacy framework. Part Two briefly explains the *Wyndham* challenge to FTC's ability to regulate data under its unfair practices authority. Part Three examines successful regulatory efforts in California, looking at the state as a case study for implementing national regulations. Part Three continues, however, by explaining why it is unlikely that regulations similar to those in California will be implemented on the federal level. Part Four recommends a regulatory scheme whereby FTC is empowered to regulate data practices by encouraging states to pass laws that trigger FTC's deceptive practices authority. The goal of this Comment is to provide a means for FTC to implement its 2012 privacy plan, albeit in piecemeal, even if the Commission cannot fully regulate data practices under its unfairness authority. Finally, this Comment concludes that FTC can use the commitments data collecting companies make in response to increasingly strict, state-level data regulations to implement its privacy plan. Such an approach may be the best hope for regulating consumer privacy, data collection, and data security in lieu of congressional action.

I. DATA PRACTICES AND PRIVACY: HOW DATA PRACTICES ARE VIEWED IN A PRIVACY FRAMEWORK

In a world of increasing data collection, data security cannot exist without privacy, and privacy cannot exist without sufficient security of personal information.[36] The proliferation of data collectors and sellers

34. *See infra* Part III (describing California's legislative action over online privacy and data collection).

35. *See infra* Part IV.

36. *See* Omer Tene, *2013: The Year of Privacy*, PRIVACY RISK ADVISORS (Dec. 22, 2013), http://www.privacyrisksadvisors.com/news/a2013-the-year-of-privacy-by-omer-tene/ (noting that according to the Department of Commerce's (Commerce's) National Institute of Standards and Technology (NIST) Preliminary Cybersecurity Framework, "any security tit must be met by a privacy tat," as demonstrated by the NIST's call to calibrate privacy control to meet security requirements); *see also* NAT'L INST. OF STANDARDS & TECH., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK 38–39 (2013), *available at* http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf (discussing privacy research

raises privacy concerns that the current statutory framework for consumer privacy is not well-suited to handle.[37] For instance, while "the United States is a world leader in exporting cloud computing, location-based services,"[38] and other data-related businesses, "[m]uch of the personal data used on the Internet . . . is not subject to comprehensive Federal statutory protection."[39] Current federal "data privacy statutes apply only to specific sectors [of the economy], such as healthcare, education, communications, and financial services or, in the case of online data collection, to children."[40] In addition, the original enactment of key federal privacy laws predates much of the technology at issue in today's data collection discussions.[41] Consumer privacy laws at the federal level have "gaps" in the existing framework, including when and to whom the laws apply.[42]

used to identify current privacy gaps and how there are insufficient standards to mitigate the security concerns). The framework includes considerations for the protection of individual's privacy and personally identifiable information under the category of "data security." *See id.* at 33–34 (describing various methodologies to protect privacy and civil liberties for a cybersecurity program); *see also* FTC 2012 REPORT, *supra* note 15, at 23 (including data security, reasonable collection limits, sound retention practices, and data accuracy under the umbrella of "substantive privacy protections"); *see generally* ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), THE EVOLVING PRIVACY LANDSCAPE: 30 YEARS AFTER THE OECD PRIVACY GUIDELINES 5 (2011), *available at* http://www.oecd.org/dataoecd/22/25/47683378.pdf ("The abundance and persistence of personal data, readily available globally, has provided benefits while at the same time increasing the privacy risks faced by individuals and organisations.").

37. *See* GAO, INFORMATION RESELLERS, *supra* note 19, at 1, 7–10 (recommending that Congress reconsider the current privacy framework because it does not fully address changes in technology and marketplace practices).

38. WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 6.

39. *Id.* at 6.

40. *Id.*; Rich Hearing, *supra* 19, at 3 (describing several statutes that the FTC uses to promote data security). Those statutes include the Fair Credit Reporting Act, Pub. L. No. 91-508 , 84 Stat. 1114 (codified as amended in scattered of 12 U.S.C. and 15 U.S.C) (2012) (concerning financial services); the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C) (2012) (concerning financial services); and the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (2012) (concerning children's activities on the internet). Outside of FTC, privacy requirements may fall under the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (concerning communications); the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 16 Stat. 1936 (concerning healthcare).

41. *See* GAO, INFORMATION RESELLERS, *supra* note 19, at 7–10 (illustrating a timeline of key legislation such as the Gramm-Leach-Bliley Act, COPPA, and HIPAA which Congress enacted prior to the advent of behavioral advertising, location-based services, social media, smart phones, mobile application, and mobile payments).

42. *See* WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 6–7 (explaining that most of the personal data used on the Internet is not subject to federal statutes because of the gaps left by existing statutes). Some have referred to the areas not covered by sector

Changing technology and marketplace practices "fundamentally have altered the nature and extent to which personal information is being shared with third parties."[43] Whereas large corporations and government agencies were traditionally the primary collectors of personal data, data collection is now more decentralized, pervasive, and subject to a wider array of purposes.[44] FTC has recognized the increased privacy and data security concerns posed by the growing connectivity of devices that can collect consumer information, transmit data back to companies, and compile large amounts of information about consumer habits for third parties.[45]

These devices allow "people and things to be connected Anytime, Anyplace, with Anything and Anyone."[46] Because of this omnipresent connectivity, threats to consumer privacy and data security exist even in traditionally private places.[47] What has changed in recent years in the

specific laws as "gaps" in the privacy framework. *See* DEP'T OF COMMERCE, INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 12 (2010), *available at* http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf [hereinafter COMMERCE 2010 REPORT] ("Much of the personal data traversing the Internet falls into [the] gaps. . . . [M]any of the key actors (e.g., online advertisers—and their various data sources—cloud computing services, location-based services, and social networks) in Internet commerce operate without specific statutory obligations to protect personal data"). *But see* GAO, INFORMATION RESELLERS, *supra* note 19, at 27 (describing how marketing and information resellers argue that the sector-specific regulation is sufficient to protect consumers and does not leave significant gaps).

43. GAO, INFORMATION RESELLERS, *supra* note 19, at 46; *see* Richard Martinez & Melissa Goodman, *Technology: 5 Things to Know Now About the FTC and Data Security*, INSIDE COUNSEL (Sept. 13, 2013), http://www.insidecounsel.com/2013/09/13/technology-5-things-to-know-now-about-the-ftc-and?page=2 (discussing the changing marketplace for consumer information and the wide range of devices that collect personal information about consumers. "Smart appliances from phones to bathroom scales, thermostats, refrigerators and wristfitness monitors transmit a steady stream of personal data to manufacturers, service providers, and others.").

44. WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 9.

45. FTC held a public workshop to explore consumer privacy and security issues in light of the growing connectivity of devices. *See generally* FTC, INTERNET OF THINGS - PRIVACY AND SECURITY IN A CONNECTED WORLD (Nov. 19, 2013), http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world ("The ability of everyday devices to communicate with each other and with people is becoming more prevalent and often is referred to as 'The Internet of Things.'").

46. Letter from Justin Brookman, Director, Consumer Privacy Project, CTR. FOR DEMOCRACY & TECH. (CDT), to FTC (Jan. 10, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/2014/01/00016-88256.pdf (citing Charith Perera et al., *Context Aware Computing for The Internet of Things: A Survey*, 16 IEEE COMMC'NS. SURVEYS & TUTORIALS 414, 416–17 (2014)).

47. *Id.* at 2–3 (noting that sensors may be able to tell when people leave their homes).

consumer information market is not the fundamental technology behind connected devices, but the scope of the collection, which has become more complex and oversaturated even in private locations like the home and office.[48] For example, a new generation of appliances, called "smart" appliances, gathers detailed information about consumers, their homes, and information outside the normal context in which consumers use the devices.[49] An intercepting third party could use this information to determine when a person is home or even which rooms are empty.[50] In some cases, a third party can actually see inside of homes.[51] Outside the home, consumers carry smart devices on their persons that collect geolocation and sensitive health information while consumers are on the move.[52] That information is also vulnerable to accidental disclosures and

48. *Id. at* 4.

49. *Id.* at 2–4 (explaining how an interactive and connected television called a

> smart television [that] uses voice or face recognition to personalize the user experience, [] can also easily measure signals in its surrounding environment—e.g., a living room—that have nothing to do with entertainment. For example, it may be able to determine how often a family plays board games, or record the conversation of a phone call that takes place in the living room without the knowledge of the user.).

(citations omitted)

50. *Id.* at 3 (describing how light sensors can tell how often a room is occupied and temperature sensors like those in smart thermometers may be able to "tell when one bathes, exercises, or leaves the home entirely").

51. Consumer groups have already shown that security flaws in smart technologies allow hackers to remotely activate the cameras and microphones embedded in these devices. *See* Sen. Chuck E. Schumer, Press Release, New "Smart" TV's Have Built in Cameras, Microphones, and Internet Access, Allowing Viewers to Access Online Media and Make Video Calls (Aug. 6, 2013), *available at* http://www.schumer.senate.gov/record.cfm?id=345512& (calling on manufacturers of smart devices to create a uniform standard of security and urging consumers to be vigilant of privacy and security threats). In addition, FTC took action against a home security company whose software vulnerabilities were exploited by hackers who posted live feed of the inside of consumers' homes on the Internet. *See* TRENDnet, Inc., *supra* note 4, at 5.

52. Christopher Wolf & Jules Polonetsky, *An Updated Privacy Paradigm for the "Internet of Things,"* FUTURE OF PRIVACY FORUM 9 (2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf (describing the benefits of wearable smart devices, like fitness bands, which collect user information, but may also "yield unanticipated health insights that could be provided individually to users or used in the aggregate to advance medical knowledge"). Sensitive information includes information that can be used to identify an individual. These fitness bands collect personally identifiable and anonymized information such as a user's gender, age, height, weight, and usage data, which the data collecting company then discloses to other companies. *See, e.g.*, *Privacy Policy*, FITBIT, http://www.fitbit.com/company/previousprivacypolicy (last updated Aug. 10, 2014) ("Fitbit may also share your personal information with companies who provide services such as information processing, order fulfillment, product delivery, customer data management, customer research and the like."). This type of information should be treated

hacking,[53] presenting not only privacy, but also health risks.[54] Increasingly, the nature of the information collected and the vulnerabilities in design and execution of new smart technologies presents significant challenges for regulators.[55]

In this environment of increasing information gathering in the private sector, current federal laws provide only limited protections.[56] Consumers have little say in much of the principal activities of data collection. For instance, consumers lack universal rights to access, correct, or control their personal information used for marketing.[57] No federal statute provides them the right to learn what information is held about them or even who holds their personal information.[58] Additionally, consumers do not have a

as sensitive information under HIPAA. *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,222 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160 & 164) (while responding to a public comment on the HIPPA Privacy Rule, the Department of Health and Human Services (HHS) states that "[t]he Department treats all individually identifiable health information as sensitive and equally deserving of protections under the Privacy Rule").

53. Hacking refers to accessing computer systems without authorization. *See* GAO, PERSONAL INFORMATION, *supra* note 16, at 2, 18–19; *see also* Brookman, *supra* note 46, at 12 (noting that new smart health devices are often provided by entities not covered by HIPAA or subject to HHS enforcement, leaving only FTC § 5 or state law to protect consumers' health and privacy). However, providers of smart health devices may be considered business associates under HIPAA, which would mean HIPAA would apply. *See* 45 C.F.R. § 160.103(ii)(3)–(4) (2013) (defining "business associate"); Modifications to the HIPAA Privacy, 78 Fed. Reg. 5571 (Jan. 25, 2013) (stating that entities with "more than 'random' access to protected health information . . . would fall within the definition of 'business associate'"); Christopher Budd, *Before You Put on That "Wearable,"* TRENDMICRO BLOG (Jan. 9. 2014), http://blog.trendmicro.com/put-wearable/ (warning consumers about the potential vulnerabilities of wearable technology, including privacy and potential health risks, if hackers gain control of mobile health devices).

54. *See* Budd, *supra* note 53 (referencing the decision to have doctors disable the wireless functionality of a heart pump implanted in former Vice President Dick Cheney because of fears that the device could be wirelessly hacked and manipulated); *see also* Daniel Halperin et al., *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*, *in* 2008 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 129–30 (May 2008) (demonstrating how implantable medical devices (IMD) such as implatanable pacemakers, insulin drug pumps, and cardioverter defibrillators which use computers and radios to monitor and treat patients outside of hospitals can be reverse engineered to reveal patient information, manipulated to administer improper treatment including electric shocks, and rendered ineffective by software or signals that deplete the battery).

55. WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 9.

56. *Id.* at 6.

57. *Id.* at 13.

58. *Id.* at 1. This is particularly important given the large amount of data collection involved in a single website visit. *See* Julia Angwin, *Online Tracking Ramps Up: Popularity of User-Tailored Advertising Fuels Data Gathering on Browsing Habits*, WALL ST. J. (June 17, 2012), http://www.onlinemediadiva.com/online-tracking-ramps-up/ (explaining a study found

right to choose the types of personal information collected, the sources used, or the methods used by information collectors.[59] Consumers also have limited ability to change privacy controls related to technologies, such as web tracking and mobile devices.[60] Recently, "new and more advanced technologies . . . have vastly increased the amount and nature of personal information collected [as well as] the number of parties [using or sharing] this information," while consumers continue to have only limited protections.[61]

In 2012, the White House asked Congress to pass comprehensive privacy legislation by "filling gaps in the existing framework."[62] The White House's privacy framework is supposed to provide clearer protections to consumers and allow greater certainty for companies while promoting innovation at minimal compliance costs.[63] If adopted, the privacy framework would apply to any "commercial uses of personal data," including aggregations of data which is linkable to a specific individual.[64]

fifty-six instances of data collection in the average website visit in 2011, increasing from just ten instances in an initial study one year prior in 2010); INFORMATION RESELLERS, *supra* note 19, at 18 (explaining that consumer data is collected from many sources—including warranty registration cards, consumer surveys, retailers, online discussion boards, social media sites, blogs, web browsing histories, and web searches—and federal law does not mandate disclosure to consumers that their information is being collected or used for marketing purposes).

59. *See* Brookman, *supra* note 46, at 4 (explaining that consumers should have control in the increasingly complex data collection by Internet capable devices). With the proliferation of Internet-enabled devices, it is unlikely a consumer could avoid some sort of data collection and impractical to rely on traditional notice and choice (consent-based) legal framework. *See* Wolf & Polonetsky, *supra* note 52, at 2, 3, 7–10. *But see* Jonas Lerman, *Big Data and Its Exclusions*, 66 STAN. L. REV. ONLINE 55, 55–56 (2013) (examining how "[b]illions of people worldwide remain on big data's periphery" and how even today the working poor manage to avoid making a large digital foot print).

60. INFORMATION RESELLERS, *supra* note 19, at 46.

61. *Id.*; Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (July 30, 2010) http://online.wsj.com/news/articles/SB10001424052748703940904575395073512989404 (reporting on an investigation of the online tracking practices of the fifty most popular websites in the United States, which account for forty percent of webpages viewed by Americans, finding that those sites installed 3,180 tracking files on a test computer used to visit them; twelve of those sites installed more than 100 tracking tools each).

62. WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 6–7.

63. *Id.*

64. *Id.* at 10. Personal data is linkable to a specific individual when "information can be used to distinguish or trace an individual's identity either alone or when combined" with other data. *Id.* at 10 & n.12. The definition of the "linkable" data is intended to provide the flexibility necessary to capture the many kinds of data companies collect. *Id.* at 10. The Consumer Privacy Bill of Rights does not provide specific standards for compliance with the security principle. Instead, the framework reflects a flexible approach to implementing privacy and security safeguards which may involve a multistakeholder process used to

The Obama Administration created and published the Consumer Privacy Bill of Rights, providing a framework that reflects a desire to bring commercial uses of personal data in line with the Fair Information Practices Principles (FIPPs).[65]

The FIPPs are a set of internationally recognized principles for protecting the privacy and security of personal information.[66] The principles were first proposed by a U.S. government advisory committee in 1973 in response to privacy concerns about the increasing use of computerized data systems.[67] The FIPPs influenced the Privacy Act, which governs how federal agencies collect, maintain, use, and disseminate personal information, in addition to the privacy recommendations of federal agencies such as FTC and the Department of Commerce (Commerce).[68] The Consumer Privacy Bill of Rights represents an interpretation of the FIPPs.[69] Although the FIPPs are not binding law, they provide a useful "framework for balancing the need for privacy with other interests."[70]

---

determine enforceable codes of conduct based on the Fair Information Practices Principles (FIPPs). *Id.* at 29.

65. *See* WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 1, 10. ("The Consumer Privacy Bill of Rights applies to commercial uses of personal data."). *But see* GAO, INFORMATION RESELLERS, *supra* note 19, at 32 (finding the Consumer Privacy Bill of Rights would not apply to a company whose "activities [are] subject to existing federal data privacy laws").

66. *See* GAO, INFORMATION RESELLERS, *supra* note 19, at 5–6; *see also* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 99 (1992) (explaining that the OECD adopted the principles in 1978, setting the standard for Europe as well as creating the most influential expression of FIPPs). *Id.*

67. GAO, INFORMATION RESELLERS, *supra* note 19, at 5.

68. *Id.* at 6. The principles include collection limitation (limiting the means of collection and requiring consent), data quality (requiring personal information "be relevant to the purpose for which it is collected"), purpose specification (requiring disclosure of the purpose), use limitation (restricting use and disclosure absent consent), security safeguards (requiring reasonable security safeguards), openness (requiring "ready means" of informing individuals about privacy policies), individual participation (providing a right to access and correct personal information, and challenge the denial of rights), and accountability (making information collectors accountable for implementing the FIPPs). *Id.* at 6 & n.4.

69. *Id.* at 6. The Consumer Privacy Bill of Rights is composed of seven principles based on the FIPPs: individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability. The FIPPs are composed of eight principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. *See also* Wolf & Polonetsky, *supra* note 52, at 3–4 ("FIPPs have been presented in different ways with different emphases.") (arguing that policymakers should implement a flexible interpretation of FIPPs because the "Internet of Things" is not suited for a rigid interpretation).

70. GAO, INFORMATION RESELLERS, *supra* note 19, at 5–6.

The Consumer Privacy Bill of Rights acknowledges an important interconnectedness of consumer privacy and data security, namely that securing personal data is essential to protecting consumer privacy.[71] The Consumer Privacy Bill of Rights "carries FIPPs forward" by articulating the security principle of the FIPPs as a "right" owed to consumers and an obligation placed on companies.[72] The privacy framework also sets a baseline of rights designed to inform consumers of what they should expect from companies that handle their personal data:[73] consumers have a "right to secure and responsible handling of personal data," and companies are expected to "maintain reasonable safeguards" to control the risk of unauthorized access and improper disclosure.[74] Appropriate security measures may depend on a company's line of business, the kinds of personal data the company collects, the likelihood of harm to consumers in the event of a security breach, and other case specific factors.[75] The privacy framework recognizes that "reasonable safeguards" for one company may not be the same for another.[76] While the Consumer Privacy Bill of Rights advances the FIPPs by articulating the rights of consumers and obligations of data collectors,[77] it does not define what "reasonable safeguards" means—that important task is ultimately left to FTC.[78]

71. *See* WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 19 ("Technologies and procedures that keep personal data secure are essential to protecting consumer privacy."). The Consumer Privacy Bill of Rights is motivated by harms caused by security breaches; those harms "range from embarrassment to financial loss and physical harm" for consumers and reputational and financial harm for companies. *Id.* Again, it is not unusual to consider data security in the context of privacy. *See generally* COMMERCE 2010 REPORT, *supra* note 42, at 57 (recommending in Commerce's privacy report, a national "commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows States to build upon the framework in limited ways").

72. WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 49–52 (comparing the implementation of the FIPPs security requirement in the Consumer Privacy Bill of Rights, OECD Privacy Guidelines, Department of Homeland Security Privacy Policy, Asian-Pacific Economic Cooperation (APEC) Principles). Only the Consumer Privacy Bill of Rights expressly states that consumers have a "right" to the security of their personal information. *Id.* at 50.

73. *See id.* at 19; COMMERCE 2010 REPORT, *supra* note 42, at i ("New devices and applications allow the collection and use of personal information in ways that, at times, can be contrary to many consumers' privacy expectations.").

74. WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 19.

75. *Id.*

76. *Id.*

77. *Id.* at 50.

78. FTC is expected to provide advice in any stakeholder negotiations that lead to enforceable codes of conduct consistent with the Consumer Privacy Bill of Rights. Ultimately, FTC will investigate and enforce any violations of those codes. *See id.* at 29–30.

II. FTC ACT: A BRIEF LOOK AT THE COMMISSION'S SCOPE AND THE *WYNDHAM* CHALLENGE

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[79] FTC views its empowering statute as a "broad consumer protection mandate" that Congress intended to allow the Commission to respond to the "unanticipated, unenumerated threats" consumers face in the marketplace.[80] When bringing a § 5 action, FTC alleges facts based on unfairness, deception, or both, depending on the circumstances.[81]

The elements of unfairness differ from those of deception. To establish that an act or practice is unfair, FTC must plead that (1) an act or practice caused or is likely to cause substantial injury to consumers; (2) the injury was not reasonably avoidable by consumers; and (3) the injury was not outweighed by countervailing benefits to consumers or competition.[82] To establish that an act or practice is deceptive under § 5, FTC must demonstrate that "(1) there was a representation; (2) the representation was likely to mislead customers acting reasonably under the circumstances; and (3) the representation was material."[83] FTC pursues companies under both its unfairness and deceptive practices authority, although it usually relies on the latter when it comes to data security.[84]

79. 15 U.S.C. § 45(a)(1) (2012).

80. Plaintiff's Response in Opposition to the Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC at 2, FTC v. Wyndham Worldwide Corp., (No. 2:13-CV-01887-ES-SCM) (D.N.J. June 17, 2013); *see FTC Policy Statement on Unfairness*, Appended to Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984) (citing FTC v. R.F. Keppel & Bro., 291 U.S. 304, 310 (1934)) ("Neither the language nor the history of the [FTC Act] suggests that Congress intended to confine the forbidden methods [of business acts] to fixed and unyielding categories.").

81. *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief, *supra* note 7, at 18–19. FTC has expressly applied the unfair practices application to companies, including LabMD, Inc., a company that, like Wyndham, also challenged the FTC's authority. *See* LabMD, Inc., F.T.C. No. 9357, at 5 (2013) (provisionally redacted administrative complaint), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf (stating that the acts and practices alleged in the complaint constitute unfair acts or practices under § 5(a) of the FTC Act, 15 U.S.C § 45(a)).

82. 15 U.S.C. § 45(n) (2012); FTC v. NHS Sys., Inc., 936 F. Supp. 2d 520, 531 (E.D. Pa. 2013). The analysis of countervailing interest of consumer is "essentially a cost-benefit analysis[,]" requiring FTC to balance the benefits versus the substantial injury to consumers. *See* Transcript of Nov. 7, 2014 Oral Argument on Motion to Dismiss, *supra* note 3, at 73.

83. *See* FTC v. Magazine Solutions, LLC, No. 7–692, 2010 WL 1009442, at *11 (W.D. Pa. Mar. 15, 2010) (citing FTC v. Tashman, 318 F.3d 1273, 1277 (11th Cir. 2003)).

84. *See* Gerard M. Stegmaier & Wendell Bartnick, *Another Round in the Chamber: FTC Data Security Requirements and the Fair Notice Doctrine*, 17 J. INTERNET L., no. 5, Nov. 2013, at 1, 18 ("Usually, the FTC makes a deceptive practices claim when an entity experiences a data

FTC resolves most data security cases using consent orders in which companies agree to institute more robust data security procedures and make long-term commitments to third party security assessments.[85] FTC then uses the consent orders, which are private actions negotiated between the alleged violators and FTC, as fair notice that other companies must implement consistent practices.[86] Some have criticized FTC's heavy reliance on consent orders,[87] distinguishing those private agreements, which are merely FTC victories, from binding judicial precedent.[88]

In *Wyndham*, FTC faced a challenge to its authority to regulate data security under its unfairness authority.[89] FTC alleged that Wyndham Worldwide Corporation, a large chain of hotels and resorts, failed to provide reasonable and appropriate security for consumers' personal information, leading to more than $10.6 million in fraudulent charges on consumers' accounts.[90] Lawyers for the defendants in *Wyndham* agree that

breach after publishing statements that it secures data. Less frequently, the FTC alleges unfair practices in data-security cases.").

85. *See, e.g.*, TRENDnet, Inc., *supra* note 4, at 5–6 (agreeing to biennial, third-party assessments for a period of twenty years in addition to reporting requirements meant to substantiate certain safeguards); Consent Decree and Order for Civil Penalties, Injunction and Other Relief at 9–10, United States v. RockYou, Inc., No. 12-CV-1487 (N.D. Cal. Mar. 28, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyouorder.pdf (agreeing to biennial assessments for a period of twenty years conducted by independent, third-party professionals).

86. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 617 (D.N.J. 2014) (affirming the use of consent orders as fair notice).

87. *See* Stegmaier & Bartnick, *supra* note 84, at 18–19. Additionally,

> [i]n light of the agency's current approach toward data-security enforcement, challenges to FTC actions under the fair notice doctrine may become increasingly justified. Although the FTC has undertaken significant efforts to develop and improve notice of its interpretation of § 5, the nature, format, and content of the agency's data security-related pronouncements raise equitable considerations that create serious due process concerns.

Id.

88. Transcript of Nov. 7, 2013 Oral Argument on Motion to Dismiss, *supra* note 3, at 65–66. Consent decrees or orders are merely "FTC victories." *Id.* "[A] consent decree is not a decision on the merits and does not therefore adjudicate the legality of any action by the party thereto, nor is a consent decree a controlling precedent for later Commission action." *Id.*

89. Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 1, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR, 2012 WL 4766957 (D. Ariz. Oct. 1, 2012).

90. First Amended Complaint for Injunctive and Other Equitable Relief, *supra* note 7, at 2, 10. *Wyndham* was somewhat different from the only other significant data security challenge FTC has faced in that it involves a security breach caused by a third party as opposed to the defendants causing the breach. The LabMD breach was caused, not by hackers, but, by an employee who installed a peer-to-peer application on a work computer

data breaches are harmful, but they deny any wrongdoing, and also point out that FTC has not let the national political process develop data security standards.[91] They argue that "FTC has not waited for Congress or the President. Instead of allowing the political process to settle the debate over the costs and benefits of cybersecurity policy, the FTC filed [the] action" against Wyndham.[92]

Defendants in *Wyndham* are correct that efforts to update the consumer privacy framework have thus far stalled or failed at the federal level, but the same is not true on the state level. For example, California has led the way in addressing privacy and data security, passing innovative legislation whereas Congress is slow to take action.[93] This is not a new position for California, which was the first state to enact security breach notification legislation in 2002.[94] Following California's lead, forty-five states, the District of Columbia, and Puerto Rico have adopted similar breach notification laws.[95] If history is any indicator, the solution to regulating

and then designated a folder containing health records as the shareable folder. *See* LabMD, Inc., *supra* note 81, at 3–5; Peter S. Frechette, Note, FTC v. LabMD*: FTC Jurisdiction over Information Privacy is "Plausible," but How Far Can It Go?*, 62 AM. U. L. REV. 1401, 1414 (2013) ("[T]he FTC faces a different challenge to its use of the FTC Act's unfairness category in *FTC v. Wyndham Worldwide Corp*. Both Wyndham and amicus parties argue that the FTC's authority to regulate unfair practices does not extend to data breaches caused by third parties.").

91. Motion to Dismiss by Defendant Wyndham Hotels and Resorts LLC, *supra* note 10, at 1-2; Transcript of Nov. 7, 2013 Oral Argument on Motion to Dismiss, *supra* note 3, at 15 (arguing that data security threat is rapidly evolving and both the government and sophisticated hackers are taking interest).

92. Motion to Dismiss by Defendant Wyndham Hotels and Resorts LLC, *supra* note 10, at 1–2.

93. *See* The Hogan Lovells Privacy Team, *California Continues to Shape Privacy and Data Security Standards*, PRIVACY ASS'N (Oct. 1, 2013), https://www.privacyassociation.org/privacy_tracker/post/california_continues_to_shape_privacy_and_data_security_standards (noting that California was one of the first states to provide an express right to privacy in its constitution. The California Constitution creates a presumption that individuals are harmed when their privacy is violated or information is otherwise obtained without consent); *see* CAL. CONST. art. 1, § 1 (1879) ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and *privacy*.") (emphasis added); *see also* Kamala D. Harris, Attorney Gen. of Cal., Statement on Privacy Enforcement and Protection (Oct. 9, 2014), *available at* http://oag.ca.gov/privacy (protecting the right to privacy is one of the California Attorney General's "top priorities" and "[t]oday more than ever, a strong privacy program is essential to the safety and welfare of the people of California and to our economy").

94. *See* The Hogan Lovells Privacy Team, *supra* note 93.

95. *Id.*

data practices may come from the states, not the federal government.[96]

With the exception of sector-specific requirements, there is no federally mandated breach notification requirement.[97] FTC and Commerce have recommended Congress adopt national breach notification legislation, recognizing the success of notification initiatives at the state level.[98] More than ten years after California adopted its breach notification law, members of Congress continue to introduce breach notification bills hoping to federalize data security measures.[99] California's privacy and data security standards are some of the strictest in the nation and, as a result, many companies decide to comply with California's laws to avoid a state-by-state approach to setting their privacy and data security practices.[100] This type of bottom-up privacy and data security policymaking, combined with some of the strictest privacy and data security laws in the United States, means that California laws have set national standards for privacy and data security while FTC enforces case-by-case adjudication without a clear national mandate.[101]

96. *See* Emily S. Tabatabai et al., *United States: California Enacts Several Pieces of New Privacy Legislation,* ORRICK (Oct. 9, 2013), http://www.orrick.com/Events-and-Publications/Pages/California-Enacts-Several-Pieces-of-New-Privacy-Legislation.aspx.

97. *See supra* note 40 and accompanying text; *see also* GAO, PERSONAL INFORMATION, *supra* note 16, at 2.

98. *See* FTC 2012 REPORT, *supra* note 15, at 26 ("[The FTC] reiterates its call for Congress to enact data security and breach notification"); *see also* COMMERCE 2010 REPORT, *supra* note 42, at 7 (noting that "Finally, we recommend the consideration of a Federal commercial data security breach notification (SBN) law that sets national standards, addresses how to reconcile inconsistent State laws, and authorizes enforcement by State authorities. State-level SBN laws have been successful in directing private-sector resources to protecting personal data and reducing identity theft, but the differences among them present undue costs to American businesses. The FTC and individual States should have authority to enforce this law.").

99. *See, e.g.*, Data Security and Breach Notification Act of 2013, S. 1193, 113th Cong. (2013) (referred to Committee on June 20, 2013); Data Security and Breach Notification Act of 2012, S. 3333, 112th Cong. (2012) (referred to committee, but died in committee); Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011); Data Breach Notification Act of 2011, S.1408, 112th Cong. (2011); Data Security Act of 2011, S. 1434, 112th Cong. (2011).

100. *See* The Hogan Lovells Privacy Team, *supra* note 93; Tabatabai, *supra* note 96 (noting that "if history is any indication, other states will follow California's lead" by adopting aspects of California's privacy and data security framework, including changes which broaden the scope of the framework).

101. *See* The Hogan Lovells Privacy Team, *supra* note 93; Tabatabai, *supra* note 96.

III. STATE LEVEL MOVEMENT ON SECURITY AND PRIVACY: CALIFORNIA AS A CASE STUDY

California is an important market not only for online services but also for enacting laws that will impact the nation's privacy and data security framework. The state has an active legislature that passes online privacy and data collection laws that affect a large number of companies and businesses.[102] Moreover, the laws are written so that they apply to every website that collects information about Californians or that Californians visit.[103] The number of websites and online services subject to these types of laws is further amplified by the fact that more than eighty percent of Californians use the Internet.[104] Indeed, efforts to regulate data practices in California have involved companies with large Internet footprints including Amazon, Apple, Google, Hewlett-Packard, Microsoft, and Research In Motion.[105]

102. *See* The Hogan Lovells Privacy Team, *supra* note 93 (noting that California is poised to become the eighth largest economy in the world and that one in eight Americans lives in the state). Both factors suggest regulations in California influence national privacy and data security framework. In some cases those regulations apply to a large number of online companies because they operate in California or collect information about Californians. *See, e.g.*, Assembly Bill (AB) 370, CAL. BUS. & PROF. CODE § 22575 (2013) (imposing consumer Internet privacy regulations to all commercial Internet websites that collect personal identifiable information about consumers residing in California); Senate Bill (SB) 568, CAL. BUS. & PROF. CODE §§ 22580–82 (2014) (prohibiting an operator of an Internet website, online service, online application, or mobile application, as specified, from marketing or advertising specified types of products or services to a minor).

103. *See, e.g.*, AB 370, CAL. BUS. & PROF. CODE § 22575 (2013) (applying to "[a]n operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online"). *See* Tabatabai, *supra* note 96 ("The new laws affect all operators of commercial Web sites or online services that collect personally identifiable information from California residents (i.e., most Web sites). As a result, these laws apply generally to companies inside and outside of California that do business in the state."). In addition, the U.S. Census estimates thirty-eight million people reside in California in the year 2013, which is about 12% of the nation's total population. *See State & County QuickFacts: California*, U.S. CENSUS BUREAU, http://quickfacts.census.gov/qfd/states/06000.html (last visited Jan. 31, 2014).

104. *See* Mark Baldassare et al., *California's Digital Divide*, PUB. POL'Y INST. OF CAL. (2013), http://www.ppic.org/content/pubs/jtf/JTF_DigitalDivideJTF.pdf (noting that 86% of Californians use the Internet in 2013, marking a 16% increase over five years); U.S. DEP'T OF COMMERCE, NAT'L TELECOMM. & INFO. ADMIN., CURRENT POPULATION SURVEY (CPS) INTERNET USE 2010 (Jan. 28, 2011), *available at* http://www.ntia.doc.gov/files/ntia/data/CPS2010Tables/t11_2.txt (finding that 84.19% of Californian households use the Internet either in the home or elsewhere).

105. *See* Kamala D. Harris, Attorney Gen. of Cal., Joint Statement of Principles (Feb. 22, 2012), *available at* http://oag.ca.gov/system/files/attachments/press_releases/n2630_signed_agreement.pdf? (announcing an agreement with those companies to strengthen data

In 2013 alone, the state legislature enacted six significant privacy and data security bills.[106] Two of those laws directly address data breaches: one amends the state's breach notification law by adding usernames and passwords to the kinds of personal identifiable information that, once breached, trigger a notification;[107] and the other imposes notification requirements on local, state government agencies.[108] Another law prohibits companies from sharing data about consumers' utilities usage without consent and requires companies "implement and maintain reasonable security procedures and practices . . . to protect the data from unauthorized . . . disclosure."[109] California law restricts data practices in the name of privacy, but also addresses data security by imposing standards for handling personal information.[110] The remaining laws deal more with pure privacy concerns rather than the mix of privacy and data security, which motivated other legislation enacted in 2013.[111] For instance, Senate Bill (SB) 568 restricts advertising of products and services on websites and online services directed to, or knowingly used by, minors.[112] The bill also requires websites and online services to provide a way for minors to remove content they have posted online.[113] In a single year, the California legislature enacted

security and privacy in the mobile application market).

106. CAL. DEP'T OF JUSTICE, OFFICE OF THE ATTORNEY GEN., *Privacy Legislation Enacted in 2013*, http://oag.ca.gov/privacy/privacy-legislation/leg2013 (last visited Feb. 28, 2015) (describing laws enacted in 2013).

107. SB 46, CAL. CIV. CODE §§ 1798.29, 1798.82 (2014).

108. AB 1149, CAL. CIV. CODE § 1798.29 (2014).

109. *See* AB 1274, CAL. CIV. CODE §§ 1798.98–.99 (2014).

110. *Privacy Legislation Enacted in 2013*, *supra* note 106 (summarizing AB 658 as a law requiring any business that offers medical software or hardware, including mobile applications, to "keep[] medical information confidential when creating, maintaining or disposing of [medical information]"); *see* AB 658 Senate Floor Analysis, 2013–2014 Leg. (Cal. 2013), at 2 (describing the handling of personal health records in terms of "standards for maintaining the *security* of [patients'] medical information") (emphasis added).

111. *Compare* AB 370, CAL. BUS. & PROF. CODE § 22575 (2013) (requiring companies' privacy policies disclose how websites respond to "Do Not Track" signals), *with* SB 46, CAL. CIV. CODE §§ 1798.29, 1798.82 (2014) (requiring breach notification), *and* AB 1274, CAL. CIV. CODE § 1798.98 (2014) (requiring "reasonable security procedures and practices"). The term "Do Not Track" refers to online mechanisms consumers use to "exercise some control over how third parties use personal data or whether they receive it at all." WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 12.

112. *See* SB 568, CAL. BUS. & PROF. CODE §§ 22580–82 (2014).

113. *See id.* at § 22581 (requiring websites "[p]ermit a minor . . . to remove or, . . . to request and obtain removal of, content or information posted on the operator's Internet Web site, online service, online application, or mobile application by the [minor]" and also "[p]rovide notice to a minor . . . that the minor may remove . . . [the] content or information" as specified); *see also* Tabatabai, *supra* note 96 (referring to SB 568 as the "Internet Eraser Law").

six bills which address privacy, data security, and a combination of the two concerns in a wide variety of scenarios, ranging from those affecting the rights of minors in the content they post online to the security of information about consumers' use of home utilities.[114]

A. Conditions Are Not the Same on the Federal Level

Despite hopes for a renewed national privacy and data security framework, it is unlikely that the type of progress seen in California over the past decade will be replicated on a national level.[115] In many ways the national dialogue about privacy and data security remains in a holding pattern while interested parties discuss whether or not an overhaul of the current framework is even necessary.[116] Part of the problem is that industry and privacy advocates have starkly different views of the current federal framework.[117] Even the White House has sent mixed messages, recognizing the need to fill the gaps in the current framework, while also claiming that the current framework is sufficiently flexible to address the nation's changing needs.[118]

Indeed, efforts to create national standards have been a challenge from

114. *See generally Privacy Legislation Enacted in 2013*, *supra* note 106 (summarizing SB 568 and AB 1274, two bills enacted in 2013).

115. Somini Sengupta, *No U.S. Action, So States Move on Privacy Law*, N.Y. TIMES (Oct. 30, 2013), http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html (quoting Jonathan Stickland, a Republican state representative in Texas, as saying "Congress is obviously not interested in updating [privacy laws] or protecting privacy").

116. Some interested parties argue that the national framework is not fraught with gaps and that sector-specific protections are sufficient to meet changing needs so as long as there are "robust industry enforcement mechanisms," which they argue are already present. *See* GAO, INFORMATION RESELLERS, *supra* note 19, at 27–29 (explaining that marketing and information reseller industries have argued that the sector-specific approach has not left significant gaps. They claim consumers are sufficiently protected, citing four main reasons: 1) federal and state laws are "extensive"; 2) the current framework provides "adequate privacy protections" including the flexibility to address new technologies; 3) any gaps in the current framework are the result of gaps in *enforcement*, rather than in the legal framework, itself; and 4) consumers' expectations of privacy have changed in the technological age, mitigating the need for strict controls).

117. "Proponents of legislation argue the [data collection] industry is a Wild West where consumer data are gathered and sold without restrictions." *See* Julia Angwin, *Watchdog Planned for Online Privacy*, WALL ST. J. (Nov. 11, 2010), http://online.wsj.com/news/articles/SB10001424052748703848204575608970171176 01; GAO, INFORMATION RESELLERS, *supra* note 19, at 28 (explaining that privacy advocates and consumer organizations stress that privacy laws have not been updated to address challenges arising from technological developments, which have "rendered parts of the U.S. privacy policy framework out of date" and no longer irrelevant to key actors in the Internet age).

118. GAO, INFORMATION RESELLERS, *supra* note 19, at 46.

the beginning, plagued by some of the most basic issues. For instance, the stakeholders invited to address potential national standards—including privacy advocates and companies that sell consumer information—cannot settle on whether to support a legislative solution to fill the gaps in the current framework or allow the data industry to self-regulate.[119] Even if a legislative solution is chosen, many stakeholders question whether the gaps in the current framework represent an identifiable harm that new legislation might attempt to cure.[120] Emblematic of the national effort, after years of deliberations, the industry working group tasked with standardizing a "Do Not Track" option for Internet browsers appears to being going nowhere.[121] The group is unable to agree on the most basic of issues, including what Internet tracking even *means*.[122] If lawmakers make it past these issues, they must also consider the lingering questions about the extent to which aspects of a federal privacy and data security framework should preempt already successful privacy and data security frameworks at

119. *See id.* at 27 ("Stakeholder views have diverged on whether significant gaps in the current legal framework for privacy exist, whether more legislation is needed, or whether self-regulation can suffice."). FTC called on Congress to pass legislation to fill the gaps, but the Commission also supports promoting self-regulation efforts. *See* FTC 2012 REPORT, *supra* note 15, at i ("The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.").

120. *See* GAO, INFORMATION RESELLERS, *supra* note 19, at 29.

121. Tene, *supra* note 36; *see A Status Update on the Development of Voluntary Do-Not-Track Standards: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 113th Cong. 9–10 (2013) (statement of Justin Brookman, Consumer Privacy Director, Center for Democracy & Technology), *available at* https://www.cdt.org/files/pdfs/Brookman-DNT-Testimony.pdf (calling the Internet industry's refusal to honor Do Not Track signals built into Internet browsers, like Safari, frustrating and perplexing and stating that "the tortured Do Not Track saga is a stark demonstration of why consumers fundamentally need comprehensive privacy law").

122. Tene, *supra* note 36. Do Not Track refers to mechanisms that allow consumers to choose what information is collected about them while using the Internet. *See The Do Not Track Option: Giving Consumers a Choice*, FTC, http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-not-track (last visited Mar. 22, 2015). A casual observer may find hope in the trend of major Internet browsers, like Internet Explorer and Firefox, voluntarily incorporating default Do Not Track mechanisms and websites voluntarily committing to honor Do Not Track signals. That hope should be tempered by the fact that the Internet is a global vehicle for information exchange and "[u]nless Web sites and services specifically change their practices, turning on Do Not Track in a Web browser will do *absolutely nothing* to protect users' privacy." Geoff Duncan, *Why Do Not Track May Not Protect Anybody's Privacy*, DIGITAL TRENDS (June 9, 2012), http://www.digitaltrends.com/mobile/why-do-not-track-may-not-protect-anybodys-privacy/#!2dfKx.

the state level.[123] Thus far, efforts to make changes to the federal framework have been slow and primarily unsuccessful,[124] suggesting it will continue to be up to the states to move privacy and data security forward.[125]

B. The FTC, Commerce, and the White House All Want What California Already Has

California's privacy and data security framework is similar to what the FTC, Commerce, and the White House want to see implemented nationwide. In order to address what these proponents of national reform want, it is first necessary to note that the privacy frameworks offered by the FTC and Commerce are not all that different from each other or the White House's Consumer Privacy Bill of Rights.[126] FTC and Commerce view their privacy recommendations as complimentary initiatives, representing a

123. *See* Grant Gross, *Lawmakers Push for Federal Data Breach Notification Law*, PC WORLD (July 18, 2013), http://www.pcworld.com/article/2044673/lawmakers-push-for-federal-data-beach-notification-law.html ("The debate over whether a national law should preempt state laws—along with debates over what types of information should be subject to breach notification rules and how long companies have before reporting the breaches—has held up a national breach notification bill in Congress for years . . . ."). These decisions would be made in an environment where commentators have expressed concern that FTC's willingness to step in to fill a void left by Congress is another example of an ever-expanding § 5 authority. *See* Alan L. Friel, *Why We Don't Need the FTC on Big Data Lifeguard Duty: Recent Comments From Chairwoman are Worrisome*, ADVERTISING AGE (Oct. 8, 2013), http://adage.com/print/244128 (describing how *Wyndham* "may serve to check the creeping expanse of [FTC's] authority"). Lawmakers may look to the Do Not Call laws for guidance on maintaining consistent state legislation. *See Attorney General To FTC: Do Not Preempt State "No Call" Programs Protecting Consumer Privacy*, CAL. DEP'T OF JUSTICE, OFFICE OF THE ATT'Y GEN. (Apr. 12, 2002), https://oag.ca.gov/news/press-releases/attorney-general-ftc-do-not-preempt-state-no-call-programs-protecting-consumer (urging FTC to avoid preempting states' Do Not Call programs when creating a national program); FTC, COMPLYING WITH THE TELEMARKETING SALES RULE (2011), http://www.business.ftc.gov/documents/bus27-complying-telemarketing-sales-rule (stating that "FTC and FCC continue to work to harmonize state and federal Do Not Call laws" with the goal of creating a single national registry).

124. *See supra* note 122 (discussing Do Not Track).

125. Sengupta, *supra* note 115; *see also* Margaret H. Lemos, *State Enforcement of Federal Law*, 86 N.Y.U. L. REV. 698, 719 (2011) (arguing that "state enforcement tends to ramp up precisely when—and because—federal enforcers have determined to cut back on enforcement," which suggests that the states will have a counterbalancing relationship).

126. The White House privacy plan directs Commerce to conduct multistakeholder negotiations to develop enforceable codes of conduct consistent with the Consumer Privacy Bill of Rights. *See* U.S. DEP'T OF COMMERCE, NAT'L TELECOMM. & INFO. ADMIN., PRIVACY MULTISTAKEHOLDER PROCESS: MOBILE APPLICATION TRANSPARENCY (2013), http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

consistent approach to privacy protection.[127] Furthermore, both agencies have a long history of working together and having consistent approaches to privacy protection.[128] For example, similar to the White House, both agencies recommend that the United States recognize the FIPPs as the foundation of a commercial data privacy framework.[129] Similar to California's framework, FTC's framework embodies the need for "increased transparency and consumer control, the need for privacy protections to be built into basic business practices, and the importance of accountability and enforcement."[130] These principles are consistent with the Consumer Privacy Bill of Rights, those embraced by Commerce, and principles recognized by other organizations that have considered privacy issues.[131]

The California framework is consistent with what the agencies and the White House want to implement, even down to many of the specific details.[132] California implemented a breach notification law in 2002, and

127. *See* FTC 2012 REPORT, *supra* note 15, at 3 (explaining how FTC and Commerce worked together to ensure that their privacy initiatives were complementary and the agencies "communicated regularly on how best to develop a meaningful, effective, and consistent approach to privacy protection").

128. *See id.* (explaining how the agencies imagine that with any national framework they will "continue to work collaboratively to guide implementation of [their] complementary privacy initiatives"); *id.* at 14 (discussing how FTC will participate in Commerce's efforts to develop sector-specific codes of conduct and "[t]o the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work"); COMMERCE 2010 REPORT, *supra* note 42, at vi (noting that Commerce, the White House, and FTC have taken a similar approach on issues of commercial data privacy since the early days of the Internet).

129. *See* COMMERCE 2010 REPORT, *supra* note 42, at 4 (describing how the "FIPPs should promote increased transparency through simple notices, clearly articulated purposes for data collection, commitments to limit data uses to fulfill these purposes, and expanded use of robust audit systems to bolster accountability"); *see* FTC 2012 REPORT, *supra* note 15, at i (urging companies to adopt practices consistent with the FIPPs).

130. *See* FTC 2012 REPORT, *supra* note 15, at 10.

131. *See* WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at app. B (comparing the Consumer Privacy Bill of Rights to other privacy statements based on the FIPPs); INTERACTIVE ADVERTISING BUREAU ET AL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 2–4 (July 2009), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf (noting that the Digital Advertising Alliance calls for consumer control of collection and use of online behavioral data, consistent with the principles of education, transparency, consumer control, data security, material change (concerning consent), sensitive data (accounting for sensitivity of information), and accountability). *But see* Cole, *supra* note 13 (writing that the efforts of Department of Defense and other government agencies questions FTC's authority in the field of data security).

132. *See* Letter from Joanne B. McNabb & Jeffrey Rabkin, Cal. Dep't of Justice, to Lawrence E. Strickling, Nat'l Telecomm. & Info. Admin. 1 (Aug. 14, 2013), *available at* http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/letter_NTIA_mobile_app.pdf (noting

in 2013, the state expanded the types of personal identifiable information that warrant a notification if released.[133] Starting in 2014, California required websites to disclose how they respond to consumers' Internet browser-based Do Not Track requests.[134] Although the state law is a disclosure requirement and not a Do Not Track requirement, supporters believe that transparency is the first step in the direction of an eventual Do Not Track requirement.[135] In the state's analysis of the law, members of the state legislature considered the efforts at the federal level to implement a Do Not Track standard protocol.[136]

While the Do Not Track movement and other efforts are not making progress at the federal level, California keeps pushing for more transparency and privacy protections.[137] For example, the state legislature passed laws to secure medical information on mobile applications and consumer information collected by utility companies using household devices, while the federal government continues to stall in these areas.[138] California also passed innovative laws to protect minors, requiring that websites have an easily available method for erasing information minors post online.[139] Indeed, FTC and the White House call for "greater protections" for personal data obtained from minors.[140] The White House calls for "appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation," which would account for the

that the code of conduct developed by multistakeholder negotiations is consistent and "very similar" with several of the recommendations in California's mobile application plan, *Privacy on the Go*).

133. SB 46, CAL. CIV. CODE §§ 1798.29 & 1798.82 (2013).

134. AB 370, CAL. BUS. & PROF. CODE § 22575 (2013).

135. *See* CAL. S. RULES COMM., OFFICE OF S. FLOOR ANALYSES, AB 370 BILL ANALYSIS 5 (2013), *available at* http://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml# (arguing in support of the bill, Consumer Watchdog, states "there must ultimately be a legal Do Not Track requirement. However, in the absence of such legislation, transparency about a service's practices is a step in the right direction. Requiring transparency could well prompt companies to compete based on their privacy practices. AB 370 will likely prompt more companies to honor Do Not Track requests.").

136. *See id.* at 4.

137. Omar Tene, *DNT 2.0: What Next for Policymakers?*, PRIVACY PERSPECTIVES (Sept. 18, 2013), https://www.privacyassociation.org/privacy_perspectives/post/dnt_2.0_what_next_for_policymakers. The working group designing a federal Do Not Track standard has fallen apart and the group has little to show for its effort. *See* Tene, *supra* note 36.

138. AB 658, CAL. CIV. CODE § 56.06 (2013) (requiring confidentiality of medical information in mobile applications); AB 1274, CIV. CODE § 1798.98 (2013) (requiring privacy and security of customer electrical and natural gas usage data).

139. *See* SB 568, CAL. BUS. & PROF. CODE §§ 22580–82 (2013) (taking effect January 1, 2015).

140. WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 15.

"different degree of protection" needed for minors.[141] In sum, California's privacy and data security framework is similar to what the agencies and the White House want to see implemented nationwide, except California is actually getting it done.

IV. FEDERAL-STATE COLLABORATION: HOW FTC CAN REGULATE DATA PRACTICES BY INDIRECTLY USING STATE LAWS

Until Congress passes new privacy and data security laws, FTC should use innovative ways to implement the privacy recommendations from its 2012 Report.[142] FTC apparently views its § 5 authority broadly enough to already include the authority to regulate data security, even before *Wyndham*, but not sufficiently broad to implement its 2012 privacy plan. Of course the 2012 privacy plan is not law, but neither are the other guidance documents FTC uses to establish industry standards in the other industries it regulates.[143] The Commission should work with state legislatures seeking to adopt laws similar to the 2012 recommendations. State legislatures have been more productive than Congress in responding to growing concerns about data practices,[144] and the situation at the federal-level is unlikely to change.[145]

141. *See id. at* 17, 19. There are also differences in how the access and control is articulated. *See id.* at 48, 51 (noting that under the Consumer Privacy Bill of Rights consumers have the "right to access and correct personal data." Under the OECD Privacy Guidelines, access and control includes the right to "have the data erased, rectified, completed or amended.").

142. *See generally* FTC 2012 REPORT, *supra* note 15.

143. For example, FTC uses guidance to regulate environmental marketing claims, publishing scientific standards and substantiation requirements in its Green Guides. *See, e.g.*, Green Guides for the Use of Environmental Marketing Claims, 16 C.F.R. § 260.1 (2012). The guides are "interpretations of the law . . . [that] do not have the force and effect of law and are not independently enforceable," however, FTC uses the Green Guides to hold marketers accountable, taking action under § 5 when marketers do not follow the Green Guides. *See* FTC, THE GREEN GUIDES: STATEMENT OF BASIS AND PURPOSE 1, *available at* http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-issues-revised-green-guides/greenguidesstatement.pdf. FTC views the Green Guides as a publication that does not create obligations under § 5, but, instead, serve to clarify obligations already covered by § 5. *See id.* at 52 & n.188 (citing Pac. Gas & Elec. Co. v. Fed. Power Comm'n, 506 F.2d 33, 38 (D.C. Cir. 1974) (general statement of policy is not binding and is "not finally determinative" of issues or rights)); Nat'l Mining Ass'n v. Sec'y of Labor, Mine Safety & Health Admin., 589 F.3d 1368, 1371 (11th Cir. 2009)).

144. *See* Sengupta, *supra* note 115; *supra* Part III.A–B.

145. *See* Sengupta, *supra* note 115 (explaining that a proposed update to the twenty-seven year old Electronic Communications Privacy Act stalled in Congress even after the White House made consumer privacy a priority); *supra* Part III.A.

While FTC cannot directly enforce state laws,[146] if the act of violating a state data practices law deceives consumers, then FTC can enforce its § 5 prohibition against deceptive practices.[147] Similarly, if a state law is materially similar to the FTC's 2012 recommendations, then compliance with the state law will end up implementing data practices that FTC ultimately wants.

Newly proposed state laws provide a way for FTC to indirectly regulate data practices by extending the Commission's efforts of going after companies that fail to keep commitments to include commitments made in response to state regulatory schemes.[148] For example, California has laws that require companies to make public commitments about the information they collect.[149] Along with holding companies to the commitments or representations they make, FTC could continue to publish privacy and data security guidelines, which state legislatures could then adopt in full or part, depending on their state needs.[150] This proposed regulatory scheme would essentially be an informal federal-state collaboration whereby state legislatures adopt laws designed so that violating state law inherently deceives consumers under federal law.[151]

146. 15 U.S.C. § 45(a) (2012).

147. *See* FTC, POLICY STATEMENT ON DECEPTION, *available at* http://www.ftc.gov/ftc-policy-statement-on-deception ("The Commission will find an act or practice deceptive if there is a misrepresentation, omission, or other practice, that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment. . . . The Commission intends to enforce the FTC Act vigorously. [The Commission] will investigate, and prosecute where appropriate, acts or practices that are deceptive.").

148. *See* FTC, *Enforcing Privacy Promises*, http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Mar. 22, 2015) ("When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up [to those] promises.").

149. *See, e.g.*, AB 370, CAL. BUS. & PROF. CODE § 22575 (2013) (requiring websites "disclose how it responds to 'do not track' signals or other mechanisms that provide consumers a choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across different Web sites or online services"); AB 1274, Cal. CIV. CODE §§ 1798.98–.99 (2013) (requiring companies obtain express consent to share utility information and also requiring companies "conspicuously disclos[e] to whom the disclosure [of customer information] will be made and how the data will be used").

150. States already consider federal initiatives when adopting state legislation. *See, e.g.*, CAL. S. RULES COMM., OFFICE OF S. FLOOR ANALYSES, AB 370 BILL ANALYSIS 4–5 (2013), *available at* http://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml# (referencing FTC's 2012 privacy report and consideration of Do Not Track in state legislature's analysis of AB 370).

151. FTC already collaborates with states on national initiatives. *See, e.g.*, *Complying with the Telemarketing Sales Rule*, *supra* note 123 (working to "harmonize Do Not Call requirements

A. Triggering FTC's Authority in this Proposed Regulatory Scheme

The effectiveness of this proposal depends on state legislatures passing laws that trigger the deceptive practices authority of FTC.[152] A state might require a company publish detailed information in its privacy statements about data security measures used, types of information collected, or available consumer choices. The required disclosure would need to be specific enough to make a representation under § 5, but not so specific as to make the disclosure itself a security flaw. FTC has already brought enforcement actions against website operators for simple statements published in their privacy policies; for instance, FTC brought an action against a website operator for making claims it complied with European data security standards when the website did not actually comply with those standards.[153] The point is that even simple statements about a company's data practices are enough to make a representation that might deceive consumers.[154]

If complying with state laws requires that companies make public commitments about their data and privacy practices, then FTC can regulate the extent to which companies honor those public commitments.[155] State laws might simply require companies publish a statement that they comply with a particular state law governing data

at state and federal levels for a unified national system"). In some cases these laws may be what the state is already considering adopting—the state would only need to include a deceptive practices trigger.

152. *See generally* 15 U.S.C. § 45(a) (2012).

153. *See e.g.*, PDB Sports, Ltd., F.T.C. File No. 142 3025 (F.T.C. 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140625denverbroncoscmpt.pdf (Complaint) (alleging that the Web site operator "represented, expressly or by implication, that it was a 'current' participant in the U.S.-EU Safe Harbor Framework," but was not a current member because the operator failed to renew a required self-certification); BitTorrent, Inc., F.T.C. File No. 142 3020 (F.T.C. 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140625bittorrentcmpt.pdf (Complaint) (alleging similar facts). The U.S.-EU Safe Harbor Framework is an agreement between the United States and the European Union that establishes a method for U.S. companies to transfer personal data outside of Europe that is consistent with the requirements of the European Union Directive on Data Protection. *See U.S.-EU Safe Harbor Framework*, FTC, http://www.business.ftc.gov/us-eu-safe-harbor-framework (last visited Mar. 22, 2015).

154. In *Wyndham*, FTC alleged that the Defendants "directly or indirectly, expressly or by implication, [represented that] that they had implemented reasonable and appropriate measures." Defendant's privacy policy stated that they used "industry standard practices" and made "commercially reasonable efforts" to collect and protect customer information. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 620, 626 (D.N.J. 2014).

155. 15 U.S.C. § 45(a) (2012); *see* FTC v. Magazine Solutions, LLC, No. 7-692, 2010 U.S. Dist. LEXIS 145377, at *30 (W.D. Pa. Mar. 15, 2010).

practices.[156] For example, a California law could require websites publish the following statement in their privacy policies: "This website complies with breach notification requirements under SB 46." SB 46 requires companies disclose data breaches "in the most expedient time possible" to persons reasonably believed to be affected by the breach.[157] That statement is a representation that the company will notify consumers in the event it reasonably believes its systems have been breached. Consumers who have not received a breach notification would reasonably believe that their information has not been improperly accessed.[158] Failing to promptly notify consumers would constitute a violation of state law, and also, deceive consumers—that their information was safe—under federal law.[159]

There are of course drawbacks to not having a comprehensive, federal data security and privacy framework. For one, reliance on deceptive practices will not provide FTC with the full-fledged authority the agency asserts it already has because this proposal depends on state legislatures' willingness to adopt FTC guidelines. Additionally, it will not provide FTC with all the regulatory tools that the White House has asked Congress to provide to implement the Consumer Bill of Rights.[160] It will, however, avoid some of the due process concerns of informal rulemaking and notice requirements of agency interpretations by allowing states to define the specific regulatory parameters and provide notice to affected data collectors at the state level; data collectors are already on notice about the requirements of deceptive practices when it comes to privacy statements and other public commitments made to consumers.[161] The recommended regulatory scheme also relies on FTC's tried and true deceptive practices authority, avoiding substantial criticisms about the scope of § 5.[162]

156. SB 46, CAL. CIV. CODE § 1798.29(a) (2013).

157. *Id.*

158. The test for deceptiveness is whether the consumer's interpretation or reaction is reasonable under the circumstances. *See FTC Policy Statement on Deception*, *supra* note 147.

159. *Id.* ("Practices that have been found misleading or deceptive in specific cases include false oral or written representations [and] failure to perform promised services").

160. *But see* WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 6–7 (arguing that FTC already has authority to regulate privacy).

161. *See, e.g.*, 16 C.F.R. § 312.4(b) (2012) (requiring privacy policy for websites that children access); AB 370, CAL. BUS. & PROF. CODE §§ 22575–22579 (2013) (requiring California Web sites maintain privacy policies); *see also Complying with COPPA*, FTC (July 16, 2014), http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions#Privacy%20Policies%20 (recommending that all websites and online services post privacy policies).

162. *See* Friel, *supra* note 10 (describing how the "[u]se of the [FTC's] unfairness authority has long been a controversial issue" and that the unfairness standard does not provide a clear standard for businesses; however, deception authority provides a "clear cut" standard and makes it harder for companies to argue issues of notice and due process).

Even so, this proposal does not avoid the criticism that the country would be left with a patchwork of laws in lieu of a national standard.[163] Industry advocates complain of the compliance costs inherent in a patchwork approach.[164] Some of these concerns may be tempered by the fact that California is thought to have some of the strictest privacy and data security laws in the country, and the state is on the forefront of pushing those laws in the direction of more privacy and security.[165] As a result, companies may find it more useful and less burdensome to comply with California's laws, backed by FTC, instead of taking a state-by-state approach.[166]

The effectiveness of this proposal will not depend on whether FTC is the appropriate agency to handle the task of regulating data practices. FTC is more than familiar with the gaps in the federal framework and the challenges that lie ahead in an increasingly connected world.[167] FTC also has the White House's recommendations, which can be used as a guide for implementing privacy and data security initiatives. If FTC can find a way

163. *See* WHITE HOUSE CONSUMER DATA PRIVACY, *supra* note 15, at 39 (explaining that a patchwork of laws instead of a national standard imposed burdens on businesses "without much countervailing benefit to consumers," therefore, the White House supports a national standard).

164. *Id.*; *see* COMMERCE 2010 REPORT, *supra* note 42, at 57 & n.156 (noting comments from the National Business Coalition raising concerns about an "ever-shifting 'patchwork' of different State laws that can actually change, as between the various States, several times in any given year"). Note that consumer currently face a similar patchwork when it comes to a sector-specific statutory framework. *See id.* at 60 (providing one commenter's thoughts, "American consumers and companies currently face a confusing patchwork of privacy standards that differ depending on the type of data and the data collector; the vast majority of consumer data is not covered by any privacy law."); GAO, INFORMATION RESELLERS, *supra* note 19, at 33 (suggesting that "comprehensive privacy legislation could help reduce compliance costs because the current sectoral approach, with multiple laws, makes compliance a complex and costly task for many organizations").

165. Some companies choose to keep their practices compliant with California law, the strictest state. *See* The Hogan Lovells Privacy Team, *supra* note 93 (explaining that California is a leader in regulation and has strict laws).

166. *Id.* Here the phrase "backed by FTC" means that FTC would look favorably on companies that implement substantial security and privacy practices. S*ee* FTC, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY iii (Feb. 2013) [hereinafter FTC MOBILE PRIVACY] ("To the extent that strong privacy codes are developed, the FTC will view adherence to such codes favorably in connection with its law enforcement work.").

167. *See generally* FTC 2012 REPORT, *supra* note 15, at i (detailing proposals the Commission produced in 2010 and 2012 reports for protecting consumer privacy); *Legal Resources: Reports and Workshops*, FTC, http://business.ftc.gov/legal-resources/29/34 (last visited Dec. 14, 2014) (listing FTC workshops dating back to 1995 where FTC has convened business, government, and academic experts to discuss current and emerging topics and also to report on the agency's enforcement work and industry practices).

to reliably use its deceptive practices authority to regulate even a small sector of the data collection industry, the industry might be incentivized to make broader changes consistent with prevailing privacy and security standards.[168]

This federal-state collaboration is not all that different from the deference to FTC that many states already incorporate into their consumer protection laws.[169] In many instances, state legislatures already defer to FTC interpretations and model state laws on federal laws;[170] this practice can bring state laws and regulatory efforts in line with what FTC would like to see implemented on a national level.[171] The success of this proposed federal-state collaboration depends on the shared interests of federal and state governments.[172]

168. GAO, PERSONAL INFORMATION, *supra* note 16, at 32 (noting regulation of data practices in one limited area may incentivize companies to improve data security and privacy practices on a larger scale). State-level and sector-specific regulations significantly affect companies nationwide; according to GAO, breach notification requirements have had the effect of incentivizing companies to improve data security, in part to "avoid the possible financial and reputational risks that can be associated with a publicly reported data breach." *Id.* In addition, major Internet companies are beginning to embrace the increased demand for privacy. Google, for example, agreed to honor Do Not Track signals in Internet browsers for some purposes; however, Google will continue to track and use consumer data for market research and product development. *See* Julia Angwin, *Web Firms to Adopt 'No Track' Button*, WALL ST. J. (Feb. 23, 2012), http://www.wsj.com/articles/SB10001424052970203960804577239774264364692

169. *See generally* Hakala, *supra* note 28, at 6, app. A (describing state laws which incorporate interpretations of FTC, called "state Little FTC acts").

170. *See id.* at 3. This recommendation asks that FTC embrace and utilize the relationship between the Commission's guidelines and state legislatures that defer to FTC.

171. *See* FTC MOBILE PRIVACY, *supra* note 166, at 12 (discussing the California Attorney General's recommendations to "encourage transparency about data practices, limits on the collection and retention of data, meaningful choices for consumers, improved data security, and accountability for industry actors"—goals which FTC recommends for national implementation) (citing KAMALA D. HARRIS, CAL. DEPT. OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM 2 (Jan. 2013), *available at* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf).

172. *See* Lemos, *supra* note 125, at 719 & n.90 (stating that cooperation between the states and the federal government "break down in the face of sustained disagreement," but a lack of action on the federal level is the "most common stimulus to expansive state activity") (quoting Stephen Calkins, *Perspectives on State and Federal Antitrust Enforcement*, 53 DUKE L.J. 673, 734 (2003)). FTC already cooperates with State Attorneys General to, for example, maintain and enforce the national Do Not Call registry. The Do Not Call movement started as a state initiative, but is now primarily a national program handled by the FTC with assistance from states. *See* FTC, DO-NOT-CALL IMPROVEMENT ACT OF 2007: REPORT TO CONGRESS REGARDING THE ACCURACY OF THE DO NOT CALL REGISTRY 4 (Oct. 2008), *available at* http://www.ftc.gov/sites/default/files/documents/reports/do-not-call-improvement-act-2007-report-congress-regarding-accuracy-do-not-callregistry/p034305dncreport.pdf (describing how FTC uses customer information required by state regulators to ensure

This proposal is indeed a half-step when compared to the full implementation of a national data security and privacy plan. But, in lieu of congressional action, expanded use of deceptive practices is a necessary and viable half-step in the event FTC's authority is insufficient to implement a national plan.[173] If the *Wyndham* decision is overturned or limited on appeal, FTC may find itself only able to pursue practices that fall within the scope of its deceptive practices authority; but, the aim of this proposal is to bring data practices within that scope by working with state legislatures to require that companies make representations about what they do with consumer information.[174] This proposed regulatory scheme will depend on the extent a data collector, subject to state law, is required to publicly disclose information about its practices.[175] The state law must require the data collectors make representations about their data practices so that if data collectors stray from those representations they will not mislead consumers.[176]

CONCLUSION

FTC has the authority to regulate "unfair or deceptive acts or practices in or affecting commerce," but it is unclear if the Commission has the authority to respond to the needs of the country's privacy and data security framework.[177] While FTC defended its authority to regulate privacy and

that the national registry remains accurate and up to date).

173. Of course any action in lieu of congressional action is a half-step, unless FTC already has the authority to take that action.

174. This proposal does not suggest that the state would have less authority or ability to design and implement state laws. The proposal would make more use of the deceptive practices authority which may be the current limit of FTC's authority at least where data security is at issue. *See* Transcript of Nov. 7, 2013 Oral Argument on Motion to Dismiss, *supra* note 3, at 2 (arguing that FTC has limited use of the unfair practices when regulating data security and that FTC has previously said its authority is limited to making sure "if a company says something on their website, they have to abide by it").

175. *See* FTC v. Magazine Solutions, LLC, No. 7–692, 2010 WL 1009442, at *11 (W.D. Pa. Mar. 15, 2010) (citing FTC v. Tashman, 318 F.3d 1273, 1277 (11th Cir. 2003) (detailing the elements of a deceptive practice)).

176. *Id.* Whether or not the representation materially misleads consumers will depend on the specificity of the required disclosure. The Commission already favors specificity when it comes to companies disclosing how they use consumer information. *See* FTC 2012 REPORT, *supra* note 15, at 27 ("General statements in privacy policies, however, are not an appropriate tool to ensure [a suitable limit on data collection] because companies have an incentive to make vague promises that would permit them to do virtually anything with consumer data.").

177. 15 U.S.C. § 45(a)(2) (2012); *see* FTC v. Wyndham Worldwide Corp., CV 12-1365-PHX-PGR, 2013 WL 1222491 (D. Ariz. Mar. 25, 2013); *see also* LabMD, Inc., *supra* note 81, at 3.

data security, California had already enacted innovative laws which require companies disclose information about their data practices and implement reasonable security safeguards.[178] Many of these state laws mirror the recommendations of the White House, Commerce, and FTC.[179] Increasingly strict, state-level regulations will require companies make public commitments about the information they collect.[180] The scenario of a company failing to honor those commitments fits squarely in the scope of FTC's deceptive practice authority.[181]

Wyndham will not be the final challenge of FTC's authority where data practices are concerned, but even if FTC cannot regulate the industry under unfair practices, FTC can still rely on a deceptive practices analysis to make a significant impact on the national privacy framework. The Commission can lean on the representations data collecting companies make in response to state-level data regulation. Until Congress passes new privacy and data security laws, FTC should use innovative ways to implement its 2012 privacy recommendations by working with state legislatures to adopt state laws which, when violated, would also violate the § 5 prohibition against deceptive practices. Such an approach may be the best hope in regulating consumer privacy and data security until Congress adopts national standards that comprehensively address these issues.

178. Assembly Bill (AB) 370, CAL. BUS. & PROF. CODE § 22575 (2013); SB 46, CAL. CIV. CODE §§ 1798.29, 1798.82 (2013).

179. Assembly Bill (AB) 370, CAL. BUS. & PROF. CODE § 22575 (2013); SB 46, CAL. CIV. CODE §§ 1798.29, 1798.82 (2013); *see generally* FTC 2012 REPORT, *supra* note 15, at i–ix.

180. Assembly Bill (AB) 370, CAL. BUS. & PROF. CODE § 22575 (2013).

181. 15 U.S.C. § 45 (2012); *see, e.g.*, PDB Sports, Ltd., *supra* note 153.