

Statement of Professor Paul Ohm
Associate Professor, University of Colorado Law School;
Faculty Director, Silicon Flatirons Center for Law, Technology, and
Entrepreneurship

Before the
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
U.S. House of Representatives
February 28, 2014

Chairman Terry, Ranking Member Schakowsky, and Members of the Subcommittee, I appreciate the opportunity to be here with you today to discuss the Federal Trade Commission (“FTC”) at 100, reflecting on the past, present, and future of this important government agency.

I am an Associate Professor of Law at the University of Colorado Law School and a Faculty Director of the Silicon Flatirons Center for Law, Technology, and Entrepreneurship. I have written and lectured extensively on information privacy, computer crime, and technology and the law. From 2012 to 2013, I served for ten months as Senior Policy Advisor in the Office of Policy Planning of the FTC. These comments are made in my personal, academic capacity and do not necessarily reflect the views of any organization with which I am now affiliated or have been affiliated with in the past. Although some of what I discuss below involve matters that were pending during my year at the FTC, I rely upon only facts in the public record. My comments do not necessarily reflect the views of the FTC, its staff, or individual Commissioners.

I will focus my remarks on the FTC’s work on data security and consumer privacy, and especially the privacy of information collected from consumers via the Internet. I will not focus on the FTC’s important work in other aspects of consumer protection and competition.

Although vital work on privacy protection takes place throughout federal, state, and local governments, were it not for the activities of the FTC, no agency would play the

critical roles of leader, central clearinghouse, and backstop. The FTC is the only agency with the authority and expertise to oversee the many industries that are not regulated specifically by statute. It has been recognized as a peer by the community of data protection authorities from other countries for its central role in American privacy policy. The FTC has become the centerpiece of privacy policy in this country, and I encourage Congress to continue to grant it the tools and authorities it needs to continue to do its job well.

At the outset, consider a simple, important fact: The United States boasts the most innovative, dynamic technology industry in the world. The burbling fount of activity and competition and vibrancy in this industry belies any argument that the FTC has sapped the innovative spirit. Indeed, the FTC has demonstrated that consumer protection and technological dynamism can prosperously coexist.

1 THE FTC'S EXERCISE OF ITS ENFORCEMENT DISCRETION

Many employees of the FTC see the agency first and foremost as a civil law enforcement agency. Of course the agency also promulgates regulations and guidance and engages in research and consumer education, but these roles are second in priority for many at the FTC. The beating heart of the FTC reverberates in its investigations, judicial filings, adjudications, settlements and consent decrees.

In its privacy enforcement activity, the FTC has exercised wise and measured discretion. I will elaborate this point to urge the Subcommittee to focus not on a hypothetical FTC or imaginary FTC, one which wields its power like a sword and presses the envelope of statutory text. It should focus on the actual FTC, one which chooses cases with care.

The simplest reason why the FTC exercises great discretion in selecting cases is

structural: The FTC is a very small agency. It employs only 1,100 civil servants, many of whom are engaged in something other than its consumer protection mission. With such a small workforce, the agency can investigate only a tiny fraction of the many complaints it receives each year.¹

Political accountability exerts another structural check on the agency's enforcement decisions. The statutorily mandated bipartisan composition of the Commission ensures that more than one political party will influence and cast votes on enforcement actions.² In addition, FTC Commissioners and staff meet regularly with members of Congress and Congressional staff and know that they will be held to account for overly aggressive action.

The FTC's wise use of its enforcement discretion is apparent in the cases it brings. Most of the cases the FTC brings each year are clear cut. It almost always brings cases in which the proof of deceptive or unfair conduct is undeniable, cases in which the defendant's conduct falls well below standards of reasonableness.³ This is not to say that these cases are easy; on the contrary, many are quite complex. But the FTC tends to focus on cases with a significant impact on consumer protection, avoiding marginal cases that push the envelope unnecessarily.

Another measure of the strength of these cases is the rate at which they are settled. In the history of the FTC's work on online privacy, the number of cases that have not led to swift settlement can be counted on one hand.⁴ And many of the cases that have settled have

¹ For example, the FTC received more than two million complaints to its Consumer Sentinel database in 2012 alone. FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK: FOR JANUARY – DECEMBER 2012 at 3.

² 15 U.S.C. § 41.

³ Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. (forthcoming 2014) (manuscript at 19), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913 (“[T]he Commission also tends to target cases with a high likelihood of success and where companies have no viable defense.”).

⁴ *Id.* at 18 (finding only two out of more than 150 privacy-related cases that did not lead to settlement).

been brought against companies that have litigated privacy lawsuits brought by other plaintiffs tenaciously and relentlessly.⁵

Consider the data security case brought against Wyndham, which is one of the rare cases that did not settle but instead is actively being litigated in federal court.⁶ Wyndham has attracted the support of some academics and trade associations who have filed friend of the court briefs advancing aggressive and novel (and to my mind, far too creative) challenges to FTC jurisdiction.⁷ Almost none of Wyndham's champions have tried to defend the reasonableness of Wyndham's security practices, which appears to have been far below industry standards.⁸ I speak not only from my experience as a legal scholar, former FTC official, and former U.S. Department of Justice computer crimes prosecutor but also from my experience as an IT professional who helped defend several large computer networks. Once you move past the jurisdictional side show, the Wyndham case supports the point I am making: the FTC sued Wyndham because the case was clear cut and because the harm to consumers was so plain.

2 THE FTC AND EVOLVING STANDARDS

If the only measure of effective agency action were the promulgation of crystal clear,

⁵ *Compare* Press Release, Fed. Trade Comm'n, Google Will Pay \$22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (August 9, 2012), *available at* <http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented> *with* Venkat Balasubramami, *Google Wins Cookie Privacy Lawsuit*, TECH. & MARKETING LAW BLOG (Oct. 31, 2013) <http://blog.ericgoldman.org/archives/2013/10/google-wins-cookie-privacy-lawsuit.htm>.

⁶ *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887 (D.N.J. filed June 26, 2012).

⁷ Brief for International Franchise Association as Amicus Curiae Supporting Defendants, *Wyndham Worldwide Corp.*, No. 2:13-cv-01887 (D.N.J. filed May 3, 2013); Brief for Chamber of Commerce of the United States et al. as Amici Curiae Supporting Defendants, *Wyndham Worldwide Corp.*, No. 2:13-cv-01887 (D.N.J. filed May 3, 2013); Brief for TechFreedom et al. as Amici Curiae Supporting Defendants *Wyndham Worldwide Corp.*, No. 2:13-cv-01887 (D.N.J. filed May 3, 2013).

⁸ Amended Complaint, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887, at 10-12 (D. Ariz. Filed Aug 17, 2012) (alleging "Defendant's Inadequate Data Security Practices").

detailed, and highly prescriptive rules, we might worry about the FTC's emphasis on enforcement over rulemaking. This worry seems unfounded, however, because the FTC undertakes its enforcement activities in a way that leads gradually to evolving standards of appropriate conduct, standards most affected companies seem to have little trouble understanding. Two recent law review articles illuminate this point.

First, Daniel Solove and Woodrow Hartzog argue that the FTC's enforcement activities operate as a sort of common law of FTC Section 5 privacy law.⁹ With every settlement, the FTC approves and publishes a complaint, a consent order, and a press release, which lay out in some detail the theory of the FTC case. The consent order is the product of active negotiation between the FTC and the defendant, which helps ensure that at least one company's point of view is reflected.

What makes this common law analogy work, according to the authors, is the work of a large and growing cadre of privacy professionals in companies and law firms who give these FTC documents the level of scrutiny that litigators give to appellate decisions in other areas of the law.¹⁰ These professionals seem quite capable of determining the FTC's evolving standards without difficulty, and they give their clients the clear advice needed to avoid FTC scrutiny and enforcement.¹¹

Second, Deirdre Mulligan and Kenneth Bamberger have elaborated a theory of "Privacy on the Ground," meaning privacy policy as it emerges from the practices of these same privacy professionals.¹² According to them, we make a mistake if we look only to "privacy on the books," as codified in statute and regulation, because the practices of

⁹ Solove & Hartzog, *supra* note 3, 15-28.

¹⁰ *Id.* at 24-27.

¹¹ *Id.*

¹² Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).

professionals help build a richer body of privacy protection.¹³ They have documented through careful qualitative empirical research how Chief Privacy Officers and other privacy professionals look in particular to pronouncements from the FTC to help them develop and understand privacy on the ground.¹⁴

We should prefer the FTC's development of evolving standards of privacy law to prescriptive rulemaking. Privacy is complex and contextual. What people expect and worry about can tend to shift with every technological advance. It is very unlikely that this contextual complexity can ever be fixed in a rigid set of promulgated rules. Instead, what is needed is a flexible standard, administered by an expert and independent agency (perhaps one constrained by limited resources and political accountability) which is dedicated to making public the reasoning underlying its enforcement actions. In other words, what is needed is precisely what Congress and the FTC have developed.

3 THE ROLE OF "SOFT LAW" AT THE FTC

The FTC influences debates over privacy policy through activities that are far less formal than enforcement actions or regulation. Solove and Hartzog refer to these as the "soft law" of the FTC, which take "the form of guidelines, press releases, workshops, and white papers."¹⁵ These activities leverage the expertise, competence, and convening power of the FTC to produce high quality reflections on the state of privacy today.

The high watermark of this activity is perhaps the 2012 report on *Protecting Consumer Privacy in an Era of Rapid Change*.¹⁶ The FTC staff worked on this report for more than a

¹³ *Id.* at 251.

¹⁴ *Id.* at 273-75.

¹⁵ Solove & Hartzog, *supra* note 3, 27.

¹⁶ FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), *available at* <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade->

year, holding several well-received workshops featuring many different interested stakeholders, issuing a draft report and receiving public comment, and incorporating that feedback and working with Commissioners to issue the official report.¹⁷

The report explains that it is “intended to articulate best practices” but not necessarily announce how the agency interprets its authorities or intends to use its discretion.¹⁸ And indeed, the Report does give examples of privacy best practices that go beyond what might be considered deceptive or unfair under Section 5.¹⁹ But some critics seem to forget or distrust this statement of purpose and instead assume that the framework announced in the report reveals the new enforcement agenda of the agency.²⁰ These critics argue that some of the privacy best practices discussed are in fact outside the agency’s authority or at least represent rules the agency would be unwise to enforce.²¹ Once again, these critics seem to be focusing on a hypothetical FTC rather than the real FTC.

We should celebrate not castigate the FTC for taking on this difficult project. The privacy report engages seriously with competing arguments and reflects soberly and wisely on these conflicts. Modern debates about privacy and technology count among some of the thorniest, most complex debates in which we as a society are engaged, and there is always

commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

¹⁷ *Id.* at 2-3.

¹⁸ *Id.* At iii (“These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this Report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.”).

¹⁹ For example, the report concludes that “affirmative express consent is appropriate when a company uses sensitive data for any marketing,” which seems to state advice about best practices rather than a blanket requirement for triggering Section 5 liability. *Id.* at 47.

²⁰ *E.g.* Thomas M. Lenard and Paul H. Rubin, *The FTC and Privacy: We Don’t Need No Stinking Data*, THE ANTITRUST SOURCE (OCT. 2012).

²¹ *Id.* at 3 (“It is inappropriate for the FTC to call for a massive new regulatory scheme when the only available systematic surveys of the industry are both out of date and suggest significant improvement over time.”).

room for rigorous thought leadership of the kind the FTC has provided. The final product has already had great influence on privacy debates, here and abroad, and it promises to enjoy a long, useful shelf life. We should encourage the FTC to conduct more work along these lines.

4 EMPOWERING AN FTC FOR THE NEXT 100 YEARS

Overall, this statement paints an optimistic picture of privacy enforcement at the FTC. I urge Congress not to upset the status quo in any significant ways. Still, I offer four smaller proposals for reforms and clarifications Congress could enact that would help the FTC with its privacy mission: clarifying the FTC's Section 5 authority to police data security; amending the definition of "unfair" in Section 5 to keep pace with changing privacy harms; bolstering the FTC's authority to lodge civil penalties; and granting the FTC additional resources, particularly with respect to hiring in-house technologists.

4.1 CLARIFYING DATA SECURITY AUTHORITY.

I have already given my thoughts about the FTC's ongoing lawsuit against Wyndham. Wyndham presents an easy case for liability for patently unreasonable data security practices. The jurisdictional arguments, while creative, should not carry the day in federal court. Yet the force with which the case has been defended, and the cacophony of supporters who have filed briefs on behalf of Wyndham have cast a small cloud over the FTC's ability to police data security. Congress might consider making explicit what is already clearly within the broad strictures of Section 5: the FTC has the authority to find violations for unreasonable security practices, meaning practices that unreasonably fail to live up to industry standards. This recommendation would take on greater urgency were any federal court to rule in favor of Wyndham's creative arguments.

I know every member of Congress is well aware that this would be an awful time to weaken the few tools we have to encourage good data security. Every American citizen, it seems, has personally or at least knows someone who has been affected by the attacks that hit American retailers around the holidays. Threats on the Internet to sensitive data seem to be increasing in frequency and sophistication.

Although most American companies seem genuinely interested in trying to secure the personal and sensitive information of their customers, too many fall short. Perhaps they are overwhelmed by the significant technical challenges, or maybe they have calculated that their focus and resources are better spent elsewhere. They make these disastrous calculations despite the fact that the FTC has been a cop on the beat. How much worse might things become if the only government agency with a comprehensive, multi-industry responsibility for policing data security is forced to scale back its efforts?

4.2 AMENDING THE DEFINITION OF “UNFAIR” ACTS OF PRACTICES

In 1980, the FTC issued a policy statement detailing how it interpreted the word “unfair” in Section 5.²² At the heart of the policy statement was a harms versus benefits balancing test, which Congress largely incorporated into the statute by amendment in 1994.²³

In my opinion, this definition is unduly narrow and constrained, and Congress should consider amending it to keep up better with the seismic changes that have been wrought by the modern Internet, and even more so the changes yet to come. For example, in the 1980 statement, the FTC explained that

²² Fed. Trade Comm’n, FTC Policy Statement on Unfairness (Dec. 17, 1980), *available at* <http://www.ftc.gov/ftc-policy-statement-on-unfairness>.

²³ 15 U.S.C. § 45(n) (defining unfair acts or practices as those that “cause[] or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition”).

The Commission is not concerned with trivial or merely speculative harms. In most cases a substantial injury involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction. Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair. Thus, for example, the Commission will not seek to ban an advertisement merely because it offends the tastes or social beliefs of some viewers, as has been suggested in some of the comments.²⁴

While the Commission should be praised for having the foresight to draft a policy statement that still serves a purpose more than two decades on, several aspects of this passage seem no longer to describe new forms of privacy harm that the Internet has wrought. Although it still may be true that privacy injuries “involve[] monetary harm” in “most” cases,²⁵ it is also true that nonmonetary harm abounds online, and the FTC should be empowered to bring cases to redress those harms. As only one example, every person who has spent hours dealing with a stolen credit card number understands the concretely harmful impact of data breach, even if this injury might be difficult to measure in dollars.

Another part of the passage that has not aged well is the way it associates “emotional impact” only with mere offense to “tastes or social beliefs.”²⁶ Many privacy law scholars have documented how privacy harms often affect emotions first and foremost. The FTC itself seems to understand this, because it charged an unfairness count in *Designerware*, a case involving the use by furniture rental stores of hidden software installed on rental laptops that surreptitiously videotaped consumers in their homes.²⁷ The FTC found consumer harm from the fact that some of the companies used the software to record “images of visitors, children, family interactions, partially undressed individuals,

²⁴ FTC Policy Statement on Unfairness, *supra* note 22.

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Designerware, LLC*, 2013 WL 1684153 (F.T.C. 2013) (complaint, decision and order).

and couples engaged in intimate activities.”²⁸ This was unfair, in part, because “[s]haring these images with third parties can cause consumers financial and physical injury and impair their peaceful enjoyment of their homes.”²⁹ This may have been largely nonmonetary harm, and it seems to have involved primarily harm to emotions, yet the FTC was nevertheless correct to plead this as an unfairness case.

None of this is to argue that Congress or the FTC should redefine unfairness to extend to vague, “trivial or merely speculative harms.”³⁰ On the contrary, as I have suggested in some of my writing, modern privacy harms are often concrete and deeply felt, even if nonmonetary and difficult to quantify. This is especially so if unfairness encompasses, as the Policy Statement says it does, not merely completed harm but also the “significant risk of concrete harm.”³¹

The victims of data misuse suffer fear and apprehension. Data gleaned from large databases have been used by stalkers.³² Modern databases, filled by the ever proliferating array of sensors that dot our landscape, track our every movement³³ and communication, including the kind of evanescent water-cooler chatter that was once saved nowhere. Newer sensors are detecting our paces, heartbeats and even brain waves.³⁴ Miniature cameras contain enough storage to snap a photo every moment.³⁵ And Big Data techniques give companies the power to make inferences from this rich database about our predilections,

²⁸ *Id.*

²⁹ *Id.*

³⁰ FTC Policy Statement on Unfairness, *supra* note 22.

³¹ *Id.* n. 12.

³² *E.g.* *Remsburg v. Docusearch*, 149 N.H. 148 (2003).

³³ Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES, March 26, 2011 at A1.

³⁴ Quentin Hardy, *Big Data in Your Blood*, N.Y. TIMES BITS BLOG, Sept. 7, 2012, <http://bits.blogs.nytimes.com/2012/09/07/big-data-in-your-blood/>.

³⁵ Duncan Geere, *Logging Life with a Lapel Camera*, MIT TECH. REV., May 10, 2013, <http://www.technologyreview.com/news/514361/logging-life-with-a-lapel-camera/>.

habits, and desires.³⁶ Four years ago, I described this confluence of technologies and business models as creating a “database of ruin,” one which holds a secret about every person in America that he or she would not want his or her worst enemy to know.³⁷ This description seems truer today than then. The database of ruin, when misused, can lead to significant harm, the kind of harm that should support a finding of unfair conduct.

I could direct this appeal at the FTC, which retains the power to revisit the 1980 unfairness statement. But it is also properly directed at Congress, which could amend Section 5 to make it more responsive to redressing privacy harm in the Internet age.³⁸ I urge Congress to amend the definition of “unfair” to allow it to apply to any harm, monetary or not, including harm with emotional impact, provided the harm is significant and concrete.

4.3 ENHANCING THE FTC’S POWER TO SEEK CIVIL PENALTIES

For the most part, the FTC has made the most of the remedial powers granted to it. Under its power to seek preliminary and permanent injunctions, it has crafted broad and aggressive consent decrees. Under the same authority, it has sought equitable monetary relief, to try to recover funds to make victims whole or disgorge ill-gotten gains.

But all too often, and particularly in data security cases, we see companies adopt lax, substandard practices that fall well below reasonable industry standards. It may be that these outliers do not feel deterred by the threat of FTC action. To try to alter that behavior of companies like these, Congress should increase the deterrent effect, by giving the FTC an

³⁶ VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, *BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK* (2013).

³⁷ Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 *UCLA L. REV.* 1701, 1748 (2010).

³⁸ If Congress is reluctant to amend Section 5, it could exhort the FTC to consider redrafting the 1980 policy statement, which after all was written in response to a letter from the Consumer Subcommittee of the House Committee on Commerce, Science, and Transportation. FTC Policy Statement on Unfairness, *supra* note 22.

enhanced authority to seek meaningful civil penalties from courts.

4.4 GRANT ADDITIONAL RESOURCES TO THE FTC

It is impressive that the FTC has accomplished as much as it has, despite the relatively small size of its staff and its relatively low operating budget. The agency has done much with little, so imagine what it might do with a little more.

I would emphasize in particular the need to give the FTC more resources devoted to keeping up with rapidly changing technology. The FTC already employs several very talented technologists in its staff, and some of its lawyers are recovering technologists too. But given the decidedly technological turn that the FTC docket has taken in recent years, it needs many more. And these technologists need access to cutting edge technologies for training, investigation, and forensic analysis, technologies that at the agency are currently in short supply.