United States of America

Federal Trade Commission

"Privacy Regulation in the Internet Ecosystem"
Remarks of Maureen K. Ohlhausen[1]
Commissioner, U.S. Federal Trade Commission

Free State Foundation
EIGHTH ANNUAL TELECOM POLICY CONFERENCE

March 23, 2016

Thank you to the Free State Foundation for inviting me today. Congratulations, Randy and team, for lining up another stellar Telecom Policy Conference. The theme of this year's conference is "The FCC and the Rule of Law." It probably won't surprise anyone here that I have thoughts on both. But, standard disclaimer, these thoughts are my own, and do not necessarily represent the views of the FTC or other Commissioners.

The rule of law is a fascinating, complicated topic. In one of the many, many notices I received from Free State Foundation about today's conference, Randy quoted Friedrich Hayek's definition of the rule of law from Hayek's book, *The Road to Serfdom*.[2]

Of course, Hayek dove deeply into the philosophy of law in his later three-volume work, *Law, Legislation, and Liberty*.[3] A key theme in that work, one relevant to today's event, is the

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.
[2] Randolph J. May, *The FCC and the Rule of Law*, THE FREE STATE FOUNDATION (Mar. 21, 2016, 11:28 PM), http://freestatefoundation.blogspot.com/2016/03/the-fcc-and-rule-of-law html.
[3] FRIEDRICH A. HAYEK, LAW LEGISLATION AND LIBERTY, VOL. I (1973).

difference between Law and Legislation. Hayek explained that Law - the enforceable rules of conduct - long preceded Legislation, which is the deliberate making of law.[4] Law includes legislation, but also includes rules evolving from spontaneous order. Language is a good example of rules emerging from spontaneous order. A grammarian might write down the rules of language, but she is *describing* those rules rather than *establishing* them.

Similarly, the common law is a body of customary rules that accumulates from applying reason to specific disputes over time. In the common law system, judges apply long-standing legal precedent to specific cases, and their decisions become precedent for future cases. In that way, over time, the common law has developed. Thus, it is law but not legislation.

The common law approach has much to recommend it. As Cato Senior Fellow Jim Harper noted in a recent article, "part of the genius of the common law is its mix of adaptability and consistency."[5] It is adaptable because it is inductive, drawing general principles out of specific facts and controversies. And it is consistent because it is incremental and, therefore, relatively slow to change.

The FTC's case-by-case enforcement shares many of the features of the common law approach – features that I believe are significant benefits. I've talked about those benefits at length before, including at FSF's sixth telecom policy conference.[6] Today, I'd like to describe how that case-by-case approach has shaped and benefited the FTC's *privacy* enforcement.[7]

---

[4] *Id.* at 72-74.
[5] Jim Harper, *Remember the Common Law*, CATO POLICY REPORT (Mar./Apr. 2016), [hereinafter "Harper"], http://www.cato.org/policy-report/marchapril-2016/remember-common-law..
[6] *See* Maureen K. Ohlhausen, Commissioner, Fed. Trade Cmm'n, The Procrustean Problem with Prescriptive Regulation (Mar. 18, 2014), https://www.ftc.gov/public-statements/2014/03/procrustean-problem-prescriptive-regulation; Maureen K. Ohlhausen, Commissioner, Fed. Trade Cmm'n, FTC-FCC: When is Two a Crowd? (Dec. 4, 2015), https://www ftc.gov/public-statements/2015/12/ftc-fcc-when-two-crowd.
[7] As Harper points out, the history of privacy law *starts* in the common law, specifically privacy torts that developed after Warren and Brandeis's influential article, "The Right to Privacy." Harper.

FTC Approach to Privacy. Despite rumors to the contrary, the FTC is the primary privacy and data protection agency in the U.S., and probably the most active enforcer of privacy laws in the world. We have brought more than 150 privacy and data security enforcement actions, including actions against ISPs and against some of the biggest companies in the Internet ecosystem.[8] (For our purposes here I consider data security to be a subset of privacy. So when I say "privacy" today I also mean data security.) The FTC has gained this expertise *because of* - not in spite of - our prudent privacy approach, which maximizes consumer self-determination.

The FTC protects consumer privacy primarily by relying on its Section 5 authority to stop deceptive and unfair acts or practices. First, our deception authority seeks to promote an effective marketplace for consumers' privacy choices. We know from experience as well as academic research that people have widely varying privacy preferences in many areas.[9] Some people wish to minimize the information they share with others. Other people post their most embarrassing moments on Twitter or are glad to share information in exchange for services. Our privacy approach respects the autonomy of all consumers. As such, it seeks to enable consumers to match their privacy preferences with a company's privacy practices. Under our deception authority, then, we bring cases when a company makes privacy promises to consumers that materially affect consumers' actions, but the company does not keep those promises. This deception-based approach encourages the marketplace to develop privacy solutions that match widely varying consumer privacy preferences.

---

[8] FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE (2015) (Jan. 2016), [hereinafter "*FTC Privacy & Data Security Update*"], https://www ftc.gov/reports/privacy-data-security-update-2015.

[9] A recent Pew survey and focus groups testing consumer privacy preferences with regard to six different scenarios found 17% of polled rejected all the scenarios, 4% accepted all the scenarios, and the substantial majority indicated that at least one of the scenarios was potentially acceptable. *See* LEE RAINIE AND MAEVE DUGGAN, PEW RESEARCH CENTER , PRIVACY AND INFORMATION SHARING (Dec. 2015), http://www.pewinternet.org/2016/01/14/2016/Privacy-and-Information-Sharing/.

Under our unfairness authority, however, we have found certain privacy practices to be unfair, even if a company has made no promises to a consumer. Specifically, our unfairness authority prohibits practices that cause substantial harm that is unavoidable by consumers and which is not outweighed by benefits to consumers or competition.[10] Practices that the FTC has found unfair consistently match practices that consumers generally reject. For example, we brought an unfairness case against a data broker that sold highly sensitive financial information to individuals whom the data broker knew or should have known were identity thieves.[11]

Thus, unfairness establishes a baseline prohibition on practices that the overwhelming majority of consumers would never knowingly approve. Above that baseline, consumers remain free to find providers that match their preferences, and our deception authority governs those arrangements.

Establishing the baseline at the proper level is important. Too low, and we would not stop harmful practices that most consumers oppose. Too high, and we would prohibit services many consumers would prefer. If we set the privacy baseline too high, the privacy preferences of the few are imposed on the many. Our unfairness test's emphasis on real consumer harm and cost-benefit analysis helps ensure that the baseline is in the right place. And the FTC's procedural protections, such as review by our Bureau of Economics and mandatory Commission votes on settlements, create consensus and force changes to be incremental. Thus, privacy practices found by the FTC to be unfair are those that reflect consumer consensus.

---

[10] *See* 15 U.S.C. § 45(a)(1) (providing that"[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful").
[11] Fed. Trade Comm'n, In the Matter of Sequoia One, LLC, https://www ftc.gov/enforcement/cases-proceedings/132-3253/sequoia-one-llc.

The FTC's case-by-case enforcement of our unfairness authority shapes our baseline privacy practices. Like the common law, this incremental approach has proven both relatively predictable and adaptable as new technologies and business models emerge.

Baseline privacy principles are established in one additional way: by Congress passing a law. Because legislation must overcome multiple practical and procedural hurdles to becoming law, Congress's privacy directives generally line up with broad consumer preferences. For example, we have HIPPA restrictions on how health data can be used. Fair Credit Reporting Act restrictions on use of creditworthiness information. And Children's Online Privacy Protection Act restrictions on collection and use of information about children.

Thus, whether established through case-by-case enforcement or through congressional action, baseline privacy protections generally prohibit behaviors that the overwhelming majority of consumers would reject.

Having explained the FTC's case-by-case approach to privacy, let me switch gears. I'd like now to talk about a sweeping consumer privacy effort by a federal agency. An effort that involves both the FCC and FTC. One that prompts questions about jurisdiction and statutory authority and proper procedure. An effort that I have been following since its inception.

A privacy effort that humor columnist Dave Barry referred to as "the most popular federal concept since the Elvis stamp."[12]

Did that last one catch you by surprise? Did you think I was referring to the FCC's Broadband ISP Privacy Notice of Proposed Rulemaking? Sorry, no. I am referring to a different initiative, undertaken by the ***FTC*** under Chairman Tim Muris, in 2002 and 2003, to establish the national Do Not Call registry. That effort, one of the most popular regulatory actions in recent

[12] Dave Barry, *Idea for telemarketers: Hang up and go away*, DESERET NEWS, Aug. 31, 2003, http://www.deseretnews.com/article/1006979/Idea-for-telemarketers-Hang-up-and-go-away.html?pg=all.

memory, contains important parallels to and lessons for the FCC's current effort to mandate specific privacy practices for broadband ISPs.

First, a Do-Not-Call history lesson. In 1994, Congress adopted the Telemarketing and Consumer Fraud and Abuse Prevention Act, which directed the FTC to issue a trade regulation rule defining and prohibiting deceptive or abusive telemarketing acts or practices.[13] The FTC subsequently adopted the Telemarketing Sales Rule, part of which prohibited a company from calling consumers who had specifically asked that company not to call, and outlawed all calling before 8AM or after 9PM.[14] When the FTC reviewed the rule in the late 1999 and through 2000, evidence indicated that the company-specific do not call provision had significant flaws. In addition, many states had begun to create state do-not-call registries with sometimes conflicting requirements.

Subsequently, in 2002, the FTC proposed and then adopted new rules to address these concerns.[15] The centerpiece of the proposal was a national do-not-call registry. If consumers opted in to the registry by submitting their number, telemarketers were prohibited from calling that number. Mirroring the FTC's efforts, the FCC adopted very similar rules under the Telephone Consumer Protection Act, which had been passed in 1991.[16] The FCC's rules relied on the FTC's registry, and enforcement is coordinated between the FTC and the FCC.

Some advertising trade groups challenged the FTC's new rule in court. One challenger argued that the FTC lacked specific authorization to create a national registry. When an

---

[13] 15 U.S.C. §§ 6101-08.
[14] 16 C.F.R. § 310.3-310.4.
[15] 67 Fed. Reg. 4492 (Jan. 30, 2002). On January 29, 2003, the FTC issued final amendments to the Telemarketing Sales Rule ("TSR") that, inter alia, established the National Do Not Call Registry, codified at 16 C.F.R. § 310.
[16] The TCPA specifically allowed the FCC to adopt a single national registry, but until the FTC's rulemaking in 2002, the FCC had adopted a company-specific approach. *See* 47 U.S.C. § 227(c)(3); ANGIE A. WELBORN, CONG. RESEARCH SERV., RS21122, REGULATION OF THE TELEMARKETING INDUSTRY: STATE AND NATIONAL DO NOT CALL REGISTRIES 2 (2002).

Oklahoma court decision threatened to shut down the registry,[17] the FTC asked Congress to clarify its authority. Congress stepped in and passed, within 24 hours, a bill specifically authorizing the FTC to establish the registry.[18] I am told that this was the fastest bill to pass Congress since the authorization of war after Pearl Harbor. Seriously.

Since taking effect, the FTC and Congress have occasionally adjusted the Do Not Call regime. And today it remains popular and overwhelmingly successful at effectuating consumer preferences regarding telemarketing calls.

Lessons for Today. What has made the Do Not Call rule successful, and what are the lessons for the FCC's attempts to protect consumer privacy? Let's consider some similarities and differences between the Do Not Call rule and the Privacy NPRM, based on the recently released talking points.[19]

First, the similarities. Both the Do Not Call Rule and the Privacy NPRM mandate specific behaviors by the companies subject to them. Thus, they establish a baseline practice intended to protect privacy. Both also mandate a framework for consumer choices. In the Do Not Call rule, consumers can opt out of all covered telemarketing calls by registering their telephone number in a Do Not Call registry. In the FCC proposal, for first party marketing the ISP must permit consumers to opt out. For all other non-service related uses of consumer data the ISP must get consumers to opt in.

A quick aside on this point. The FCC's proposal differs significantly from the choice architecture the FTC has established under its deception authority. Our deception authority

---

[17] U.S. Security, et al. v. Fed. Trade Comm'n, Order, No. CIV-03-122-W (Sept. 23, 2003).
[18] Do-Not-Call Implementation Act, 15 USCS § 6101 (2003).
[19] Press Release, Fed. Comm. Comm'n, Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice, Transparency & Security With Respect to Their Data (Mar. 10, 2016), https://www.fcc.gov/document/broadband-consumer-privacy-proposal-fact-sheet.

enforces the promises companies make to consumers. But companies are not required under our deception authority to make such privacy promises. This is as it should be. As I've already described, unfairness authority sets a baseline by prohibiting practices the vast majority of consumers would not embrace. *Mandating* practices above this baseline reduces consumer welfare because it denies some consumers options that best match their preferences. Consumer demand and competitive forces spur companies to make privacy promises. In fact, nearly all legitimate companies currently make detailed promises about their privacy practices. This demonstrates a market demand for, and supply of, transparency about company uses of data. Indeed, recent research by Doug Brake of ITIF shows that broadband ISPs in particular already make strong privacy promises to consumers.[20]

In contrast to the choice framework of the FTC, the FCC's proposal, according to the recent fact sheet, seeks to mandate that broadband ISPs adopt a specific opt in / opt-out regime. The fact sheet repeatedly insists that this is about consumer choice. But, in fact, opt in mandates unavoidably *reduce* consumer choice. First, one subtle way in which a privacy baseline might be set too high is if the default opt in condition does not match the average consumer preference. If the FCC mandates opt in for a specific data collection, but a majority of consumers already prefer to share that information, the mandate unnecessarily raises costs to companies and consumers. Second, opt in mandates prevent unanticipated beneficial uses of data. An effective and transparent opt-in regime requires that companies know at the time of collection how they will use the collected information. Yet data, including non-sensitive data, often yields significant consumer benefits from uses that could not be known at the time of collection. Ignoring this, the

[20] DOUG BRAKE, DANIEL CASTRO, AND ALAN MCQUINN, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION, BROADBAND PRIVACY: THE FOLLY OF SECTOR-SPECIFIC REGULATION (Mar. 1, 2016), https://itif.org/publications/2016/03/01/broadband-privacy-folly-sector-specific-rules.

fact sheet proposes to ban all but a very few uses unless consumers opt in. This proposed opt in regime would prohibit unforseeable future uses of collected data, regardless of what consumers would prefer. This approach is stricter and more limiting than the requirements that other internet companies face. Now, I agree such mandates may be appropriate for certain types of sensitive data such as credit card numbers or SSNs, but they likely will reduce consumer options if applied to non-sensitive data.

If the FCC wished to be consistent with the FTC's approach of using prohibitions only for widely held consumer preferences, it would take a different approach and simply require opt in for specific, sensitive uses.

Back to the similarities between Do Not Call and the FCC's proposal. The third similarity: The FTC faced some questions about statutory authority when adopting the Do Not Call rule. The FTC actually lost in court on the statutory authority issue, but its effort was so popular that, as I mentioned, Congress broke speed records clarifying the FTC's authority. Here, the FCC proposes, for the first time ever, to apply a statute created for telephone lines to broadband ISPs. That raises some significant statutory authority issues that the FCC may ultimately need to look to Congress to clarify.

Now, the differences. First, the Do Not Call rule, consistent with the FTC's general approach to privacy under unfairness and under Congressional directives, reflected an overwhelming consensus among consumers, universal support among the FTC Commissioners, and strong support in Congress. Heck, the rule was so popular that the FCC adopted it, too!

In contrast, the current FCC proposal appears to reflect the preferences of privacy lobbyists who are frustrated with the lax privacy preferences of average American consumers.

Furthermore, the proposal doesn't appear to have the support of the minority FCC Commissioners or Congress.

Another difference is that the Do Not Call rule treats all commercial telemarketers the same, regardless of industry segment. In contrast, the FCC proposal applies to just one segment of the internet ecosystem, broadband ISPs, even though there is good evidence that ISPs are not uniquely privy to your data.[21]

While I have you all here, and before I end, I'd also quickly like to push back a little bit on two narratives I've heard in some of the discussions about the FCC's NPRM. First, I've heard an odd suggestion that the FCC is better suited to govern consumer privacy because it considers the effects of privacy on competition. However, fully half of the FTC's mission is to evaluate and promote competition, and our Bureau of Economics reviews every single privacy enforcement action we take. Second, I read an assertion the other day that the FTC is not a "Data Protection Agency." I respectfully suggest that our 150+ privacy and data security-related enforcement actions, our key international role including Safe Harbor and Privacy Shield enforcement, and our Congressional mandate to implement and enforce a number of privacy laws, including COPPA, FCRA, GLB and others, actually make the FTC one of the most active and effective data protection agencies in the world.[22]

Conclusion

At its core, protecting consumer privacy ought to be about effectuating consumers' preferences. If privacy rules impose the preferences of the few on the many, consumers will not be better off. Therefore, prescriptive baseline privacy mandates like the FCC's proposal should

---

[21] *See* PETER SWIRE, ONLINE PRIVACY AND ISPS: ISP ACCESS TO CONSUMER DATA IS LIMITED AND OFTEN LESS THAN ACCESS BY OTHERS (Feb. 29, 2016), http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps.
[22] *See* generally, FTC Privacy & Data Security Update.

be reserved for practices that consumers overwhelmingly disfavor. Otherwise, consumers should remain free to exercise their privacy preferences in the marketplace, and companies should be held to the promises they make. This approach, which is a time-tested, emergent result of the FTC's case-by-case application of its statutory authority, offers a good template for the FCC.