



United States of America
Federal Trade Commission

**“Privacy Regulation in the Internet Ecosystem”
Remarks of Maureen K. Ohlhausen¹
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).

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 U

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

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.

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 unforeseeable 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,

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.

