

Comments of Jim Harper to the Federal Trade Commission

Hearings on Competition and Consumer Protection in the 21st Century: Consumer Privacy, February 12-13, 2019

Docket ID: FTC-2018-0098

December 21, 2018

I have been studying privacy in various capacities for about twenty years, from congressional staffer to think-tanker and now as an unaffiliated private citizen. I have not kept track of all the FTC panels and inquiries in which I have participated over years,¹ but the earliest record I can find of involvement in Federal Trade Commission privacy matters was in October, 2001.² I was a founding member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee in 2005 and served for several years on that panel.³ I have written numerous studies and commentaries on privacy, identity, and related matters, and I have testified in Congress and state legislatures and on privacy and related matters many, many times.⁴

I represent no party and have not been paid to prepare this comment. I was encouraged by a professional friend who says you need to hear from me.

¹ See, e.g., Federal Trade Commission, "Agenda, Exploring Privacy: A Roundtable Series," (Dec. 7, 2009) https://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/privacyroutables_agenda1.pdf.

² "Privacilla Applauds FTC Privacy Agenda," Privacilla.org press release (Oct. 4, 2001), <http://www.privacilla.org/releases/press012.html>.

³ See "DHS Announces Appointments to Data Privacy and Integrity Advisory Committee," Government Technology (Mar. 1, 2005), <http://www.govtech.com/security/DHS-Announces-Appointments-to-Data-Privacy.html>.

⁴ See, e.g., "Consumer Online Privacy," Hearing Before the Committee on Commerce, Science, and Transportation, United States Senate, 11th Cong., 2nd Sess. (July 27, 2010) (testimony and prepared remarks) <https://www.govinfo.gov/content/pkg/CHRG-111shrg67686/pdf/CHRG-111shrg67686.pdf>; Testimony of Jim Harper, Director of Information Policy Studies, The Cato Institute, to the Senate Committee on the Judiciary, "Will REAL ID Actually Make Us Safer? An Examination of Privacy and Civil Liberties Concerns," (May 8, 2007) https://www.judiciary.senate.gov/imo/media/doc/harper_testimony_05_08_07.pdf; Testimony of Jim Harper, Director of Information Policy Studies, The Cato Institute, to the Senate Judiciary Committee Hearing Entitled "Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs," (Jan. 10, 2007) https://www.judiciary.senate.gov/imo/media/doc/harper_testimony_01_10_07.pdf; Testimony of Jim Harper, Director of Information Policy Studies, The Cato Institute, at the Hearing Entitled "The Promise of Registered Traveler," Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, Committee on Homeland Security, U.S. House of Representatives (June 9, 2005) www.privacilla.org/releases/RT_Testimony.pdf; Prepared Statement of Jim Harper, Editor of Privacilla.org at the Hearing on Red-Light Cameras U.S. House of Representatives Committee on Transportation and Infrastructure Subcommittee on Highways and Transit (July 31, 2001) http://www.privacilla.org/releases/red-light_camera_testimony.html.

Privacy is complicated, as you know, but you need not invest deeply in understanding privacy or changing technology and business models in the abstract. The right role for the Federal Trade Commission is to support consumers' privacy choices and trade-offs simply by seeing that contract terms dealing with personal information are honored.

Personal data is best conceived of as property that, in the online world, is often allocated by contract, with the contract terms appearing in or implied from privacy policies and terms of service statements. If companies are violating contracts, the FTC has authority to investigate such wrongdoing. If they are not, the FTC should leave well enough alone.

Privacy is a complex, value-laden issue. Indeed, people use the word "privacy" to refer to a number of different values, including control of personal information, fairness in the use of information, seclusion or repose, dignity/non-objectification, personal security, and more.

The strongest and most relevant sense of the term "privacy" for the purposes of these hearings is the "control" sense. And a good, if legalistic, definition of that "control" sense is that privacy is the subjective condition people enjoy when they have the power to control information about themselves and when they use that power consistent with their interests and values.⁵

Importantly, privacy is subjective. For every assumption you make about what information is sensitive, or what information people want to keep private, there are countless examples of people feeling and wanting the opposite. Privacy is individual and personal. One person cannot decide for another what his or her sense of privacy is or should be. Government regulation purporting to pursue privacy as such can only interpose the assumptions of a few about what is right and good, usurping the role of real consumers in deciding what they want. It's a fool's errand. Americans make their highly individual privacy judgments based on culture, upbringing, experience, and the individualized costs and benefits of interacting and sharing information. Consumers' judgments will never stop changing, and they should not.

The FTC's efforts to grapple with privacy, including the current effort, have been lovely, well-intentioned, and increasingly sophisticated efforts to plan on behalf of the nation what privacy people should have and what technologies and business models will best serve people's privacy and competing interests. Alas, there is no amount of study or intellectualizing that can determine how it should all come out. People's privacy interests are too varied and changing, the technology they use is relentlessly advancing, and new businesses models could crop up at any time to serve newly discovered or modified consumer interests.

⁵ See Jim Harper, "Understanding Privacy—and the Real Threats to It," Cato Policy Analysis No. 520 (Aug. 4, 2004) <https://www.cato.org/publications/policy-analysis/understanding-privacy-real-threats-it>.

Rather than focusing on people's interest and values, the final part of the privacy definition above, the Commission should focus on what may be an actual strength: guarding people's exercises of power to control information. When people have legal control of data about themselves, they can protect their privacy with that power as they see fit. When their protections for information are wrongly defeated, that is an arguable unfair practice within the FTC's jurisdiction.

There is a surprisingly simple and orthodox way to recognize people's exercise of power over information: Treat privacy policies as contractual promises that allocate property rights in data.

Consumer-facing digital businesses issue very detailed promises in their privacy policies that divide up ownership of information about customer use of their services. Communications providers are also subject to regulations that similarly allocate rights to exclude, use, sell, and process information. When people use digital and communications services, they share and produce personal information that can be sensitive, intimate, and privileged. This is why most such policies allocate the bulk of rights to control and use personal data to customers. These property rights in data include the right of users to exclude others from personal data in all but closely defined circumstances.

Typical privacy policy language denies the service provider rights to sell or share data except as provided in the policy. The language doing this will typically say something like: "We do not sell, rent, or otherwise provide your personal information to unaffiliated third parties." The possessive pronoun "your" signifies that the bulk of the ownership of the data is the customer's. Such language is usually followed by a list of narrowly circumscribed cases in which the user's information can be shared. This, again, leaves the general right to exclude all others from the data with the customer, subject to exceptions.

Contract terms limiting disclosure and use of personal information have a long history.⁶ These rights are property rights.⁷ There is no sensible or juridical way to characterize the exchange of promises between service providers and customers other than as contracts allocating property rights.

Needless to say, recognition of personal data as property is widely lacking in the law and among lawyers and privacy professionals. Heretofore in the privacy debate, assertions of property rights in data have been used to argue that all personal data is somehow the property of the consumer. That is a bizarre notion that would be impossible to administer. Rather, personal data is allocated and subdivided in somewhat intricate ways, such as by allocating possession and some use rights to service providers, with most rights to exclude staying with the consumer.

⁶ See, e.g., *Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284, 290 (Idaho 1961), quoting 7 Am.Jur., Banks, § 196 ("[I]t is an implied term of the contract between a banker and his customer that the banker will not divulge to third persons, without the consent of the customer, express or implied, either the state of the customer's account or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account, unless the banker is compelled to do so by order of a court, [or] the circumstances give rise to a public duty of disclosure").

⁷ See *U.S. Trust Co. v. New Jersey*, 431 U.S. 1, 19 n.16 (1977) ("Contract rights are a form of property").

The FTC could do a great service in the privacy debate by helping to expand recognition of data as property that is allocated by contract, traded, used, and subdivided. It is often abandoned, too. Abandonment occurs when people take no control over data about them or produced by them—when they walk down the street for all to see, for example, or when they post information on public fora.

Along with recognition of property and contract generally, the FTC could help sort out the application of various contract terms to real-world disputes dealing with personal information and privacy. There is a well-developed body of state contract law that exists to interpret contract terms and determine what terms are implied. State common law also deals with things like ambiguous contract terms, occurrences that were unanticipated by the parties to contracts, and mistake. Without becoming a law-making body itself—because it is not one; there is no such thing as “common law” that rests on top of federal legislation—the FTC could help the legal community discover and apply the gap-filling rules that exist in the law of contract.

The program I recommend is somewhat different from the detailed study of consumer privacy interests you’ve proposed, your investigation of the trade-offs involved in opting for privacy over other goods, the economic considerations at stake, and so on. But it has the singular merit of being within the competence of the Federal Trade Commission.

I mean “competence” in two senses of the term, colloquial and legal: It is something you are able to do, unlike figuring out how things should come out. It is also something you can do consistent with your legal competence. At times, the FTC has seemed to work outside its legal competence, seeking to mold markets, technology, and business practices as though that were part of rooting out unfairness and deception.

Thank you for considering these comments, and best of luck!

Jim Harper