Lessons from Antitrust:
The Path to a More Coherent Privacy Policy

James C. Cooper
Associate Professor of Law and Director, Program on Economics & Privacy
Antonin Scalia Law School
George Mason University

U.S. CHAMBER OF COMMERCE FOUNDATION

We all know that today's economy lives on data—the information economy accounts for an estimated 6 percent of GDP.[1] This means that privacy regulation, which is essentially about restricting these data flows, leaves a large footprint. One need only look to the hullabaloo generated by the recent Federal Communications Commission (FCC) broadband privacy rule and calls to block the proposed AT&T-Time Warner deal on privacy grounds.[2] As such, it's crucial that privacy regulators—chiefly the Federal Trade Commission (FTC)—get it right.

Unfortunately for consumers, the twin pillars of FTC privacy policymaking—consent orders and workshop reports—lack economic analysis or empirical evidence. The complaints and analyses to aid public comment that accompany consent orders do little more than recite the elements of an alleged FTC Act violation. Its workshop reports, which are treated as *de facto* enforcement guidelines by the private sector, are truly "economics-free" zones; they develop concepts such as "privacy by design" and "data minimization" without any serious benefit-cost analysis. Instead **the policies developed in these reports are based almost solely on anecdotes and worst-case hypotheticals.[3] The result is a regulatory framework that is woefully ill-equipped for the task at hand.**

Lessons from Antitrust

Forty years ago, antitrust was in a similar state. Business practices were condemned merely because they led to larger firms or impacted smaller companies. Consumers suffered, as antitrust was more concerned with protecting inefficient competitors than promoting competition. That all changed after a series of Supreme Court cases embraced a consumer welfare standard guided by economic analysis.[4] It is widely recognized that antitrust has enjoyed success as a regulatory endeavor in large part due to this metamorphosis.[5] Today, no one could imagine the FTC attempting to block a merger based on a workshop report or a survey. Yet, this is exactly the state of play in privacy policy.

Consider Facebook's 2014 acquisition of WhatsApp. On the antitrust side, the FTC's Bureau of Competition (BC) applied the cost-benefit framework laid out in the Horizontal Merger Guidelines (HMG) to determine that the combination of social media platforms didn't pose a threat to competition.[6] Fortunately for consumers, the FTC refused to heed calls from some to incorporate privacy concerns into antitrust and block the merger because it would give Facebook "too much" personal data. This would have been a mistake on a number of grounds: it ignores the benefits built into new uses of data in the form of richer and more personalized content, heterogeneous consumer preferences, and the First Amendment implications of undue restrictions on data flows.[7] Modern antitrust wisely eschews non-competition concerns.

Juxtapose the BC's antitrust framework with the FTC's Bureau of Consumer Protection's (BCP) response to the deal. Accompanying the FTC's closing of its

antitrust investigation into the acquisition was a letter from the BCP, cautioning that if WhatsApp failed to "obtain consumers' affirmative consent" before using their data "in a manner that is materially inconsistent" with the promises it made at the time of collection it may be in violation of the FTC Act.[8] Although requiring notice for a change in data sharing is not novel (assuming the changes in data use were material) and potentially could violate the FTC Act, the opt-in requirement sprung to life without *any* analysis.[9] Yet, it's probably not an exaggeration to say that this requirement—which later was made clear to apply to all merging firms—was only slightly less punitive than blocking the merger itself. What is more, this new opt-in requirement will create ripples far beyond Facebook and WhatsApp. It surely will deter some companies from engaging in beneficial changes to their current data collection practices and cause others to think twice before pursuing acquisitions.[10]

The Benefit of a Benefit-Cost Framework

That the FTC developed a requirement with huge potential impact on the way data are used in such an ad-hoc manner—without any analysis of likely impact on consumers or competition—is troubling. **As privacy regulation's influence on the economy has grown, so must the sophistication of the analysis on which it relies.** On this front, regulators should take a cue from antitrust's evolution and adopt a benefit-cost framework—one that uses economic analysis to identify practices that are likely to harm consumers.

A good start would be for the FTC to begin to grapple with the available empirical evidence on consumers' willingness to reveal data.[11] Consumer harm is the legal trigger for FTC action. The FTC Act bans "unfair and deceptive acts and practices."[12] For an act or practice to be unfair it must fail a cost-benefit test, causing "substantial injury to consumers" that is unavoidable and isn't outweighed by "countervailing benefits to consumers or competition."[13] For a practice to be deceptive under the FTC Act, there must be a "material" misrepresentation.[14] In this manner, materiality is a proxy for harm, because the misrepresentation distorted consumers' decisions.[15] The FTC, however, needs to confront the lack of empirical evidence that the practices that are the focus of the FTC's privacy regime are giving rise to the type of injury that Congress empowered it to address.

The FTC justifies its privacy program on the need to foster "trust" in the online environment, relying on various surveys to support the notion that consumers place a large value on privacy or feel that they have lost control of their data.[16] But surveys, or what economists call "stated preference," tell us only that privacy, like most other things, has value. It cannot answer the real question for policymakers: **How willing are consumers to swap personal data for other things they value? These tradeoffs are what matter.**

What Consumers Are Saying

Once the focus shifts to what economists call "revealed preference," or how consumers actually make tradeoffs, the story becomes quite different. Far from suggesting that consumers are reticent to engage the online ecosystem, the real world behavior illustrates consumers who are largely comfortable with the tradeoffs they make in their digital lives. There are 1.3 billion daily Facebook users,[17] 150 million people using Snapchat daily,[18] a growing number of health tracking apps and wearables,[19] and nearly half of U.S. households choosing to purchase an Amazon Prime account.[20]

Of course revealed preference is useful only if consumers are informed about the tradeoffs they are making. Some argue that consumers simply don't understand the costs associated with data sharing, and if they did their revealed preferences would look quite different. But the empirical literature suggests otherwise; economic studies that have attempted to measure the value of personal data nearly universally find that even when consumers are fully aware of the trades they are making, they are willing to provide personal information for small amounts of compensation, or alternatively are only willing to pay very little to avoid personal data collection.[21] For example, one study finds that consumers are only willing to make a one-time $4 payment to avoid real-time geolocation tracking.[22] Moreover, a recent study presented various versions of Google's Gmail privacy policies to a random sample of representative Gmail users. [23] Although the subjects generally believed that Gmail's automated content analysis was intrusive, two-thirds were unwilling to pay anything to avoid the practice—they perceived some privacy cost, but it was not as large as the value of free email. For the rest of the subjects, the median annual payment they were willing to make to avoid email scanning was only $15.

It's also crucial to consider who's doing the watching. There is evidence to suggest the common-sense notion that there **is a world of difference in the privacy implications between an email or browsing history being read by an algorithm so to serve relevant ads, and a real person engaging in surreptitious viewing of intimate activities in the home**.[24] Yet, the former scenario is often conflated with the latter in privacy policy discussions.

Data in the Balance

The takeaway from all of this is not that privacy is valueless, or that certain types of data collection and use do not give rise to privacy concerns, but rather that most consumers are comfortable with the typical bargain of sharing information with faceless servers in return for free content and services, such as email and social networking platforms. These considerations raise serious questions for mainstays in the FTC's privacy program such as data minimization and privacy by design. These slogans obscure the fact that tradeoffs exist between privacy and other characteristics that consumers value. Why not "speed" or "functionality" by design,

or "cost minimization" or "performance maximization"? Until it confronts the empirical evidence, the FTC has not made the case that it, rather than the market, is better at mediating how consumers trade among competing values. Indeed, the FTC's posture appears to be based on the preferred mix of privacy and functionality for the most privacy sensitive consumers. This posture could be welfare-enhancing only if consumers are incapable of making informed choices because they systematically underestimate privacy harms. If this is the case, the FTC should state their position clearly and engage in research to demonstrate what seems to be a necessary predicate for its regulatory agenda.

In addition to incorporating what we know about how consumers make tradeoffs involving personal data, policymakers also need to account for the direct costs of privacy regulation. For example, one study finds that increased consent requirements for sharing health care data reduces incentives to adopt health information technology, leading to worse health outcomes, especially for minority babies.[25] Another pair of economists finds that opt-in requirements for selling consumers' financial information reduces the marketability of these data and hence firms' incentives to assure its accuracy.[26] Not surprisingly, this led to laxer underwriting and concomitantly higher foreclosure rates. Another study also suggests that the European Union's (EU) Privacy Directive—which makes collection of consumer data more expensive and difficult—decreased advertising effectiveness in the EU by 65 percent on average compared to the rest of the world.[27] Policies that limit the collection and use of data are also likely to exacerbate problems associated with a lack of marketplace information, such as adverse selection and moral hazard. Again, there is a vast empirical literature examining the problems that arise when markets lack information that needs to enter into privacy policy calibration.[28] There are also competitive implications that needed to be considered. When the FTC enters into consent agreements that limit the ability of firms to collect and use data for twenty years, it necessarily will diminish their ability to innovate and compete.[29] Without taking serious stock of these negative impacts, the FTC almost surely underestimates the costs of its actions surrounding privacy.

Conclusion

As data flows have become increasingly vital in today's economy, privacy regulation has grown in importance. It's probably not an exaggeration to say that privacy is at least as important as antitrust. It's time that privacy policy making grow in rigor to match its status.

---

1 *See* Stephen Siwek, *Measuring the U.S. Internet Sector*, Internet Association (Dec. 10, 2015), *available at* http://internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf.

2 See, e.g., *Lloyd Grove, The Perils of an AT&T-Time Warner Merger*, The Daily Beast (Oct. 26, 2016), at http://www.thedailybeast.com/articles/2016/10/26/the-perils-of-an-at-t-time-warner-merger.html.

3 FTC, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION: UNDERSTANDING THE ISSUES (Jan. 2016) ("Big Data Rep."), *at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf; FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (Jan. 2015)("IOT Rep."), *at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014)("Data Brokers Rep."), *at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (March 2012)("2012 Privacy Rep."), *at* https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

4 See Douglas H. Ginsburg, *Originalism and Economic Analysis: Two Case Studies of Consistency and Coherence in Supreme Court Decision Making*, 33 HARV. J.L. PUB. POL'Y 217 (2015).

5 *Id*.

6 *See* Chelsey Dulaney, *Facebook Completes Acquisition of WhatsApp*, WALL ST. J. (Oct. 4, 2014), *at* http://www.wsj.com/articles/facebook-completes-acquisition-of-whatsapp-1412603898.

7 *See* James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, The First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129 (2013).

8 Letter from Jessica L Rich to Erin Egan & Anne Hoge (Apr. 10, 2014), at https://www.ftc.gov/public-statements/2014/04/letter-jessica-l-rich-director-federal-trade-commission-bureau-consumer. The letter called for "affirmative express consent" for changes, and a blog posting from a BCP staffer later clarified that merging parties needed to obtain "express opt-in consent" for material changes to data practices. *See Mergers and Privacy Policies* (Mar. 25, 2015), *at* https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises.

9 The only "legal" authorities relied on for this proclamation were complaints from settled case that had *nothing* to do with opt-in versus opt-out consent for privacy policy changes, but rather with alleged failures adequately to *notify* consumers about privacy policy changes. *In re Facebook, Inc.* Decision and Order, No. C-4365 (2012), *available at* http://www.ftc.gov/enforcementlcases-proceedings/092-3184/facebook-inc.; *In re Gateway Learning Corp.,* Decision and Order, No. C-4120 (2004), *available at* http://www.ftc.e:ov/enforcementlcases-proceedings/042- 3047/gateway-learning-corp-matter.

10 *See*, *e.g*., Jin-Hyuk Kim & Liad Wagman, *Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis*, 46 RAND J. ECON. (2015) (finding evidence that screening was less accurate when opt-in requirement for sharing was in place, because it limited revenue from selling to third parties); Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGM'T SCI. 57 (2011)(finding that EU privacy regulations governing web tracking, some of which require opt-in consent, reduce advertising effectiveness); *id*. at 60 (executives from large European companies report that it costs 15 Euros for each opt-in consent); HOWARD BEALES, THE VALUE OF BEHAVIORAL TARGETING (2010), *available at* http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

11 The FTC has made recent commendable steps in this direction with PrivacyCon and the recent disclosure workshop that present relevant empirical work.

12 15 U.S.C. § 45.

13 15 U.S.C. § 45(n).

14 FTC Policy Statement on Deception, appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984), *available at* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

15 Id.

16 *See*, *e.g.*, IOT Rep. at 44 ("if a company decides that a particular data use is beneficial and consumers disagree with that decision, this may erode consumer trust."); 2012 Privacy Rep. at 8-9 ("although it recognizes that imposing new privacy protections will not be costless, the Commission believes doing so not only will help consumers but also will built trust in the marketplace").

17 Company Info, Facebook, http://newsroom.fb.com/company-info/ (last visited Oct, 10, 2016).

18 Sarah Frier, *Snapchat Passes Twitter in Daily Usage*, Bloomberg News, June 2, 2016, *available at* https://www.bloomberg.com/news/articles/2016-06-02/snapchat-passes-twitter-in-daily-usage.

19 By 2015, an estimated 500 million people worldwide will use a mobile health app. Stephen McInerney, *Can You Diagnose Me Now? A Proposal to Modify the FDA's Regulation of Smartphone Mobile Health Applications with A Pre-Market Notification and Application Database Program*, 48 U. MICH. J.L. REFORM 1073 (2015) (*citing* Kevin Pho, *Health App Users Beware*, USA Today (Apr. 2, 2014), http://www.usatoday.com/story/opinion/2014/04/02/medical-app-fitness-health-fda-technology-column/7224837/). Andrew Meola, *Wearables and Mobile Health App Usage has Surged by 50% Since 2014*, BUSINESS INSIDER (Mar. 7, 2016) (health tracker use increased from 16% in 2014 to 33% in 2015), *at* http://www.businessinsider.com/fitbit-mobile-health-app-adoption-doubles-in-two-years-2016-3. See also Susannah Fox, *The Self-Tracking Data Explosion*, PEW RESEARCH CENTER (June 4, 2013), http://www.pewinternet.org/2013/06/04/the-self-tracking-data-explosion/.

20 *See* Krystina Gustafson, *Half of America Could Have an Amazon Prime Account by the End of the Year,* CNBC, at http://www.cnbc.com/2016/09/26/amazon-prime-signing-up-members-at-a-faster-clip.html.

21 For a full review of this literature *see* Alessandro Acquisti *et al*., *The Economics of Privacy* , J. ECON. LIT. at 41 (*forthcoming*, 2017), *at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580411.

22 Scott Savage & Donald M. Waldman, *The Value of Online Privacy* (2013), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2341311.

23 Lior Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers ?*, J. LEG. STUD. (*forthcoming* 2017), *at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2838449.

24 *See*, *e.g.,* DesignerWare, LLC (Apr. 15, 2012), at https://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter. Indeed, the anonymity provided by the Web is likely to be a privacy *benefit* rather than a cost. See Benjamin Wittes & Jodie Liu, *The Privacy Paradox: The Privacy Benefits of Privacy Threats*, CENTER FOR TECHNOLOGY INNOVATION AT BROOKINGS (May 2015), http://www.brookings.edu/~/media/research/files/papers/2015/05/21-privacy-paradox-wittes-liu/wittes-and-liu_privacy-paradox_v10.pdf. *See also*, Stephanie Mathson & Jeffry Hancks, *Privacy Please? A Comparison Between Self-Checkout and Book Checkout Desk for LGBT and Other Books*, 4 J. ACCESS SERVS. 27, 28 (2007).

25 Amalia R. Miller & Catherine E. Tucker, *Can Health Care Information Technology Save Babies?,* 119 J. POL. ECON. 289 (2011); Amalia R. Miller & Catherine E. Tucker, *Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records*, 55 MGM'T SCI. 1077 (2009).

26 Jin-Hyuk Kim & Liad Wagman, *Screening incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis*, 46 RAND J. Econ. 1 (2015).

27 Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGM'T SCI. 57 (2011).

28 For a review of this literature *see* James C. Cooper, *Separation Anxiety*, __ VA. J.L. TECH. __ (*forthcoming* 2017).

29 *See* James C. Cooper, *The WhatsApp Privacy Policy Change: No Cause for Alarm*, FORBES, (Sept. 7, 2016), *at* http://www.forbes.com/sites/jamesccooper1/2016/09/07/the-whatsapp-privacy-policy-change-no-cause-for-alarm/#5b85cc5204db.