REVIEW: ANTITRUST POLICY IN THE DATA ECONOMY, SELLING PRIVACY OR JUST PRIVATE DATA?

Cobun Keegan*

CITE AS: 3 GEO. L. TECH. REV. 216 (2018)

For those entrenched in the data privacy profession, it is refreshing to read work that tackles familiar questions, such as those surrounding the value of personal data, through a less familiar lens. The practice of privacy is flourishing because of the many novel challenges sparked by the proliferation of personal data. Questions abound about how best to manage access to personal information, how to control its spread, and how to signal its quality and sensitivity. With such goals in mind, privacy is concerned with minimizing harm to consumers, to institutions, and even to society. Though there can be no perfect solution to these complex issues, it never hurts to consider them through a variety of legal and regulatory regimes. In his book, *Antitrust Law in the New Economy*, Mark R. Patterson provides a taste of the implications of the battle for control of personal information through an antitrust lens by focusing on the commodification of data.[1]

Data privacy law, stemming from theories of consumer protection rather than antitrust, usually conceives of the risks of informational harms in a manner that focuses on individual consumers rather than optimal markets. For example, a privacy professional may consider the extent to which a given dataset includes sensitive data elements or whether it could be used to identify individuals. Instead of this focus on the personal nature of information, Patterson's book is rooted in the notion of "market information." From this perspective, information—defined broadly—is

* Formerly a Westin Research Fellow at the International Association of Privacy Professionals, currently works as the Deputy Director, Privacy Initiatives at the Council of Better Business Bureaus.

[1] MARK R. PATTERSON, ANTITRUST LAW IN THE NEW ECONOMY: GOOGLE, YELP, LIBOR, AND THE CONTROL OF INFORMATION (2017).

itself a product that can lead to market failures and other anticompetitive outcomes. The consumer harms that flow from these market failures may go hand-in-hand with privacy harms but may also be entirely unrelated. That is, an entity may acquire market power based on the information it controls, even if this data is not relevant to individual consumers. This serves as a useful reminder that much of the economic value of information may be rooted in factors other than its personal nature.

Patterson's outline and re-interpretation of antitrust for the modern data-driven economy is an engaging thought experiment. He outlines the ways in which data could play into various antitrust analyses: from excluding competition through the delivery of higher-value services, to differential pricing, to the accumulation of market power. Throughout the book, I had to keep memories of my rather conservative antitrust professor from intruding on some of the creative ways that Patterson shapes his vision of a new antitrust for the digital age. It is true, in theory, that assigning monetary value to data could go a long way toward establishing harm to competition in antitrust cases. Without a full understanding of the costs and benefits in a data-to-dollars exchange, much may be missing from economic analysis. Yet drawing analogies strong enough to convince legal scholars about risks of informational market failures is likely not enough to convince judges that harm to the competitive process has occurred—let alone the higher bar of injury-in-fact in private antitrust actions. Accomplishing this will require careful analysis of demonstrable market effects on a case-by-case basis. Of course, it is only through further scholarship in a wide range of disciplines that we can hope to fully capture data externalities in the courtroom.

The implications of Patterson's arguments may be equally profound for data privacy law. Patterson dedicates a chapter of his book to the concept of "privacy as an information product."[2] Like other scholars before him, he grapples with the problem of deciphering the role that privacy qua privacy plays in modern markets.[3] Is a product's level of privacy protection simply one measure of the quality of that product, or is data protection a commodity unto itself? Is our personal data the currency with which we purchase services, or is it simply an input to the production of other valuable goods? It may be, in fact, that the answers to these

[2] *See id.*, at ch. 7.

[3] For a review of scholarship on the economics of privacy, see Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015), http://science.sciencemag.org/content/347/6221/509.

questions are different for personal data than for impersonal data. It is axiomatic in the privacy profession that the value of personal data depends on context: the context of its creation, collection, and use, as well as the interaction between these contexts.[4] Such an amorphous value system may be intrinsically resistant to commodification.[5]

An example of the tension between privacy-as-commodity and privacy-as-preference is found in Patterson's critique of the Federal Trade Commission's portrayal of privacy harms as "non-price attributes of competition" in its review of the Google-DoubleClick merger.[6] Patterson contrasts this assumption in the FTC's analysis with the fact that economic analysis does not usually require consumers' tastes to be justified. In fact, "for final goods, [economics] normally takes tastes as given and asks how well a market or an economic system satisfies those tastes."[7] In this model, a person's privacy sensitivity is a taste to which maximally efficient markets would cater. Regulators have begun to take seriously the potential anticompetitive effects brought about by mergers of large data systems containing sensitive personal information, but they have so far largely failed to incorporate potential reductions in privacy choices.[8]

Patterson's data-as-resource theory also lends support to the ideas of some privacy scholars. One such scholar, Paul M. Schwartz, went so far as to enumerate the elements that a formalized market for private data would require: "limitations on an individual's right to alienate personal information; default rules that force disclosure of the terms of trade; a right of exit for participants in the market; the establishment of damages to deter market abuses; and institutions to police the personal information

---

[4] *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009); Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J.L. & TECH. 59 (2014).

[5] *See* Beate Roessler, *Should Personal Data Be a Tradable Good? On the Moral Limits of Markets in Privacy*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 141, 155–58 (Beate Roessler & Dorota Mokrosinska eds., 2015).

[6] *See* Statement of Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170, at 2–3 (Dec. 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf.

[7] PATTERSON, *supra* note 1, at 167 (quoting Joseph Farrell, *Can Privacy Be Just Another Good?*, 10 J. ON TELECOMM. & HIGH TECH. L. 251, 253 (2012)).

[8] *See* Lisa Kimmel & Janis Kestenbaum, *What's up with WhatsApp: A Transatlantic View on Privacy and Merger Enforcement in Digital Markets*, 29 ANTITRUST 48 (2015) (exploring this distinction and concluding that regulators should rely on privacy law, rather than antitrust, to mitigate harms to privacy from mergers).

market and punish privacy violation."[9] A step toward adopting Patterson's information marketplace ideas would also go far toward establishing, or at least justifying, such a regulated market. Thus, strengthening the conception of the intrinsic value of information could have broad implications beyond antitrust. As another example, such progress could go far in the effort to quantify informational injury, with which regulators have been recently grappling.[10]

There is some danger in over-reliance on quantification. Economists, even Coasian ones, are inherently limited by their focus on markets from capturing non-economic risks and harms. Though Patterson never presents antitrust as a panacea for privacy harms, but merely an underused and potentially helpful regulatory tool, there may be something lost in any reliance on the idea of data as a product. As Julie Cohen has described, attaining and preserving privacy does something for individuals that goes beyond an economic preservation of value. "Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops."[11] The accumulation and concentration of data may threaten these less-quantifiable benefits even more than it harms information markets. The lingering question is whether commodifying privacy, even toward a goal of protecting it, risks the continued de-valuation of the human need for privacy or at least the smoothing over of its contextual contours.

Patterson's book is an insightful overview of the possible impacts of ubiquitous data on competition policy in the twenty-first century. Antitrust lawyers may find its oblique and cross-disciplinary angle frustrating, but this privacy lawyer (and sofa-bound social scientist) found it intriguing. There is a long way to go in fully grappling with questions of the value of personal data, but this book adds a necessary piece to the emerging puzzle.

---

[9] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2056 (2004).

[10] *See, e.g.*, Recording of Informational Injury Workshop, FED. TRADE COMM'N (Dec. 12, 2017), https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop.

[11] Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1906 (2013).