

Before the FEDERAL TRADE COMMISSION

Washington, D.C. 20024

Hearings on Competition and Consumer Protection in the 21st Century

Topic 5

The Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters

Pre-Hearing Comment

Hearing on Feb 12-13, 2019

**Larry Downes, Project Director
Georgetown Center for Business and Public Policy¹**

December 17, 2018

In a 2013 policy analysis for The Cato Institute, I proposed a simple solution to what was already being characterized as a growing crisis in the collection and use of consumer data—increasingly but unhelpfully referred to as “privacy.”²

Some legal academics had recommended solving the problem by transforming an undefined class of data with personal connection to some user or users into a form of intellectual property. Initial ownership of the property would be assigned to the subject of the data, with rights to dispose of it by contract. “Private” information would be treated just as patents and copyrights had been since the founding of the Republic.

¹ Larry Downes is Project Director of the Evolution of Regulation and Innovation project at the Georgetown Center for Business and Public Policy. He is the author of several books on disruptive innovation and its impact on industry structure, business strategy and regulation, including “Big Bang Disruption: Strategy in the Age of Devastating Innovation” (Portfolio 2014) (with Paul Nunes), “The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in the Digital Age” (Basic Books 2009), and “Unleashing the Killer App: Digital Strategies for Market Dominance” (Harvard Business School Press 1998).

² Larry Downes, “A Rational Response to the Privacy ‘Crisis,’” Policy Analysis 716, THE CATO INSTITUTE, Jan. 7, 2013, available at <https://object.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf>. In addition to a long history of emotional baggage attached to the term “privacy,” and its undefined meaning, much of the discussion on data collection and use does and ought to concern a much wider range of information than what is included in even the broadest definitions of “private” or “personally-identifiable” information.

The problem with that model, I noted, was that the copyright and patent systems were never intended to create property rights in the first place (the term “intellectual property” appears nowhere in the Constitution). During the last several decades, in fact, the accelerating descent of copyright, patents, and trademarks into a property model through both legislation and litigation was the cause of growing dissatisfaction with the system and, indeed, for copyright and patents in particular, the open revolt of consumers.

Instead, I proposed that information collection and use be governed more closely by the more flexible law of licensing. Consumers and businesses that jointly created value in the entry, structure, storage, consolidation and repurposing of any information—personal or otherwise—would agree how that information could be used, and divide among themselves the value generated.

I noted that a nascent information licensing system was already implicit and working in examples including grocery store loyalty cards, frequent flyer programs, and on most websites on the Internet, where consumers licensed the data they entered or otherwise generated in exchange for free or subsidized content and services.

To fully resolve the so-called “privacy crisis,” the article concludes, market participants and other stakeholders, including regulators, would need to embrace five simple principles:

1. Embracing meaningful disclosure, where service providers make as clear as possible what information is being collected and what they will do with it.
2. Reducing the transaction costs of licensing negotiations between collectors of information and consumers, enhancing the existing “opt-out” model rather than discarding it in favor of “opt-in,” which would introduce considerably more such costs.
3. Securing collected information and treating it as the valuable source of future uses that it is, including the adoption of proven data handling practices, such as the ISO 27000 series.
4. Improving self-regulatory practices, including third-party certification and automated auditing of data collection and use processes.
5. Avoiding crisis-management regulation, resisting “the siren call of the privacy crisis du jour, littering the law books with specialized statutes aimed at solving short-term technical problems that will have evolved or mutated before the ink is dry.”³

³ *Id.* These recommendations echoed earlier work John Perry Barlow and I had done on data collection and use, going back to the dawn of the commercial Internet. See “John Perry Barlow on Facebook’s Latest Woes,” FORBES,

Since 2013, the Internet ecosystem has witnessed both positive and negative progress on each of these principles. On the one hand, the largely frictionless model of information exchange in the opt-in Internet—what is sometimes referred to as the Internet’s “Grand Bargain”—continues to drive profound economic growth, including traditional news websites, new web-based platform services, social networks, and a rapidly-expanding Internet of Things.

Most businesses have implemented improved security and data management practices, often at the urging of consumers and with the nudging of the Federal Trade Commission and regulators in other countries. Overall, disclosure of data collection and use practices has improved. And despite a continued series of embarrassing examples of data misuse and security breaches by some collectors, including some notable repeat offenders, policymakers in the U.S. have largely resisted increasingly emotional calls to pass new, sweeping and vague “privacy” laws.

On the other hand, data security practices in many private and public organizations still fail to meet minimum obtainable standards. ISO 27000 has not been widely adopted. Forty percent of data breaches are the result not of external hacks but company insiders.⁴ Consumers remain hesitant about adopting products as part of the Internet of Things, at least in part because of security concerns.⁵

The FTC has brought several IoT-related enforcement actions, revealing in many cases a shocking lack of concern by some IoT product developers for even the most basic data hygiene.⁶ The recent BITAG report underscored that problem, offering recommendations that should never have required amplification.⁷

On the legislative front, the EU’s General Data Protection Regulation, California’s badly garbled and misconceived Consumer Privacy Act of 2018, and the short-lived opt-in data collection and use rules enacted by the FCC solely for broadband ISPs, are each problematic, and potentially

April 9, 2018, available at <https://www.forbes.com/sites/larrydownes/2018/04/09/john-perry-barlow-on-facebooks-latest-privacy-woes/#619668d55053>.

⁴ *Id.*

⁵ Larry Downes, “Why You May Have Good Reason to Worry About all Those Smart Devices,” THE WASHINGTON POST, Dec. 6, 2016, available at https://www.washingtonpost.com/news/innovations/wp/2016/12/06/why-you-may-have-good-reason-to-worry-about-all-those-smart-devices/?utm_term=.ba32a28c71bf; *idem.*, “What’s Blocking Smart Beds from Helping you get a Great Night’s Rest,” THE WASHINGTON POST, Feb. 26, 2016, available at https://www.washingtonpost.com/news/innovations/wp/2016/02/26/whats-blocking-smart-beds-from-helping-you-get-a-great-nights-rest/?utm_term=.35ab84d6b2f8.

⁶ Larry Downes, Firing the Customer and other Cringe-Worthy Behavior Hurting Trust in Smart Devices, THE WASHINGTON POST, April 6, 2017, available at https://www.washingtonpost.com/news/innovations/wp/2017/04/06/firing-the-customer-and-other-criinge-worthy-behavior-hurting-trust-in-smart-devices/?utm_term=.f239e39b4f7a.

⁷ Broadband Internet Technical Advisory Group, “Internet of Things (IoT) Security and Privacy Recommendations,” Nov, 2016, available at [https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_\(IoT\)_Security_and_Privacy_Recommendations.pdf](https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf).

signal the unintended end of the Internet’s Grand Bargain.⁸ In its otherwise admirable 2015 staff report on the Internet of Things, the FTC repeated an unfortunate call for “enactment of data security and broad-based privacy legislation.”⁹

My recent publications, cited above, reflect my continuing view of the costs and benefits of data collection use laws and regulation, and of specific state, federal and international efforts to legislate the behavior of data collectors.

In short, I urge the FTC to continue its leadership in protecting U.S. consumers from poor practices and bad actors, using the tools described in the 2015 IoT Report: “enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders...to promote appropriate security and privacy protections.”¹⁰

In addition to those tools, the Commission should also encourage, through challenge grants, contests, and other modest financial incentives, entrepreneurial solutions to specific data collection and use problems. For example, the Commission’s 2012 Robocall Challenge inspired the creation of Nomorobo, which continues to provide relief for millions of consumers at no or minimal cost, even as the FCC continues to work with the communications industry on a systemic technical solution.¹¹

As Comm. Wright noted in his statement dissenting from release of the 2015 IoT Report, not all of the “best practices” recommended by FTC staff are supported, in the report or elsewhere, by anything approaching a rigorous cost-benefit analysis.¹² In its engagement with stakeholders,

⁸ Larry Downes, “GDPR and the End of the Internet’s ‘Grand Bargain,’” HARVARD BUSINESS REVIEW, April 9, 2018, available at <https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain>; *idem.*, “The Downside of the FCC’s New Internet Privacy Rules,” HARVARD BUSINESS REVIEW, May 27, 2016, available at <https://hbr.org/2016/05/the-downside-of-the-fccs-new-internet-privacy-rules>; “Industry Groups Beg Congress, FCC, to Restore Scrambled Internet Privacy Framework,” FORBES, Jan. 30, 2017, available at <https://www.forbes.com/sites/larrydownes/2017/01/30/industry-groups-beg-congress-fcc-to-restore-scrambled-internet-privacy-framework/#57bc69828871>; “Why Congress’s Rejection of Proposed FCC Data Rules Will Not Affect your Privacy in the Slightest,” FORBES, March 30, 2017, available at <https://www.forbes.com/sites/larrydownes/2017/03/30/why-congresss-rejection-of-proposed-fcc-data-rules-will-not-affect-your-privacy-in-the-slightest/#660c7fe48b14>.

⁹ FTC Staff, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD at 55, Jan, 2015, available at <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> (hereinafter “2015 IoT Report”)

¹⁰ *Id.*

¹¹ Larry Downes, “Policymakers Alone Cannot Stop those Pesky Robocalls,” THE WASHINGTON POST, Feb. 8, 2017, available at https://www.washingtonpost.com/news/innovations/wp/2017/02/08/policymakers-alone-cannot-stop-those-pesky-robocalls/?utm_term=.f1bfc5284f1f.

¹² Dissenting Statement of Commissioner Joshua D. Wright, ISSUANCE OF THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, Staff Report, January 27, 201, available at https://www.ftc.gov/system/files/documents/public_statements/620701/150127iotjdwstmt.pdf.

however, the Commission should continue to highlight two proven techniques for avoiding data collection and use problems, both described in the 2015 IoT Report:

Minimization — The best way to protect customer information from unwanted and unintended disclosure is not to collect it in the first place. Digital devices should only record data that they need and, where possible, do so on an anonymized basis where data stored in the cloud is not tied to specific customer identifiers. For most uses, specific identification isn't needed, but engineers either don't think through the implications of collecting unneeded data or of how identifiers can be avoided and still achieve product design objectives.

Retention — If personally identifiable data is collected, the best way to ensure it doesn't leak out by accident or criminal intervention is to get rid of it as soon as it's no longer needed. But again, product designers have little incentive to spend time thinking through the deletion of data at all, let alone adopt aggressive retention policies. The same goes for third-party cloud providers that host applications and data on behalf of clients. Storage costs continue to decline, discouraging good data hygiene.¹³

At the same time, the Commission should resist expanding its enforcement actions beyond cases where a collector fails to follow its own security practices, as promised to consumers and other stakeholders, leading to an avoidable security breach or other demonstrable consumer harm.

Two recent enforcement actions failed to follow that essential limiting principle, unnecessarily unbalancing developer incentives to the detriment of consumers.

The Commission's theory in the *Wyndham Hotels* case, for example, argued that a failure to practice unspecified data security practices, even absent specific promises to do so, could itself constitute "unfair" behavior, enforceable under Section 5 of the FTC Act.¹⁴

A 2017 complaint against D-Link, similarly, alleged a violation of Section 5 for poor security practices in the design of the company's connected cameras and routers, even though no actual data breach had occurred.¹⁵

These are worrisome precedents. As the Commission noted in the 2015 IoT Report, many emerging data collection and use applications, including the IoT, are in "relatively early stages."¹⁶

¹³ FTC Staff, 2015 IoT Report, *supra* note 9; Larry Downes, "Firing the Customer and Other Cringe-Worthy Behavior is Hurting Trust in Smart Devices," *supra* note 6.

¹⁴ Federal Trade Commission, "Wyndham Settles FTC Charges it Unfairly Placed Consumers' Payment Card Information at Risk," Dec. 9, 2015, available at <https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment>.

¹⁵ Complaint, FTC v. D-LINK, U.S. District Court for the Northern District of California, Jan. 5, 2017, available at https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf.

¹⁶ 2015 IoT Report, *supra* note 9 at 48.

Expanding enforcement of existing law along the lines of the *Wyndham* and *D-Link* actions will stifle innovation and defer valuable social benefits from the widespread deployment of new data-driven technologies.

Worse, expanded Section 5 enforcement will hit hardest at entrepreneurs and start-ups lacking the resources or experience to engage outside counsel. Even if they can, responding to an expanded threat of FTC enforcement, would result, at best, in higher prices for new devices and services.

Likewise, the adoption by Congress of broad, vague, general “privacy” legislation, along the lines of the California statute, the GDPR, or otherwise, would have disastrous impact throughout the Internet ecosystem. More “broad” privacy laws threaten new and emerging technologies including the IoT, autonomous vehicles, robotics, applied artificial intelligence, connected medical devices and smart infrastructure.

They also seriously jeopardize the continued vitality of nearly every existing Internet-based product, service, and device currently enjoyed by consumers worldwide—the Internet’s “Grand Bargain.”

The FTC should stop recommending passage of such legislation.