

Comment
Internet of Things
Project No. P135405

January 10, 2014

James C. Cooper*
Law & Economics Center
George Mason University School of Law

The Internet of Things (IOT) broadly is a network of devices that collect and transmit –to users, the cloud, and other machines – data about the world around them, such as the temperature of a house, the details of driving habits, or vital signs. The benefits from the data flows enabled by the IOT promise to be transformative: driverless cars and road sensors promise to greatly reduce traffic injuries and congestion; smart appliances will save energy and make life easier by sending notices of new items needed from the grocery store; vital sign monitors can improve health in a variety of ways. In addition to these direct consumer benefits, moreover, the data generated by these devices will allow public and private researchers to uncover patterns and trends that can lead to beneficial policies and practices.

In light of the tangible benefits that the IOT stands ready to deliver to consumers the FTC should approach the IOT with a large measure of regulator humility. More specifically, it should avoid using either enforcement or non-enforcement tools in a manner that potentially would hinder IOT innovation absent a strong empirical basis that doing so is necessary to protect consumers. This inquiry presents a chance for the FTC to use its formidable economic research capability to help guide one of its key consumer protection programs. By hewing to such a course, the FTC can avoid the missed opportunity of its 2012 Privacy Report,¹ which failed to provide any empirical basis or economic analysis to support its policy recommendations;² recommendations that have in large part become *d facto* regulations.³

* This comment reflects the views of the author only. It does not necessarily represent the views of any donors or board members of the Law & Economics Center.

¹ Federal Trade Commission, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (March 2012).

² See Thomas M. Lenard & Paul H. Rubin, *The FTC and Privacy: We Don't Need No Stinking Data!* ANTITRUST SOURCE, October 2012, available at http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/oct12_lenard_10_22f_authcheckdam.pdf; see also Concurring Statement of Commissioner William E. Kovacic, D1-D-2,

A. Benefit-Cost Analysis

The starting point of any regulatory initiative should be a benefit-cost analysis of intervention. Just as the FTC must empirically demonstrate likely consumer harm to block a merger,⁴ it should refrain from recommending any policies that would retard IOT innovation unless there is empirical evidence that these policies are needed to address any actual or likely consumer harm.⁵ By applying the same economic rigor to its consumer protection mission as it does to its competition mission, the FTC can improve the chances that its policies provide consumers with net benefits.⁶

B. Privacy Harms

Although the benefits from the IOT identified at the workshop appear very real, the costs identified by most workshop participants were largely hypothetical and subjective.⁷ This is not to say that subjective harm can never form the basis for regulatory action. Indeed, unwanted monitoring of intimate activities or unauthorized revelation of health conditions are likely harmful to most consumers.⁸ Subjective harms involved in selling anonymized data streams to third parties for marketing or research purposes, on the other hand, are likely to be suffered very differently across consumers.⁹ When sensitivity to harm varies widely, a uniform

Federal Trade Commission Staff Report, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (Dec. 1, 2010).

³ See Chairwoman Ramirez, IOT tr. at 9 (to “embrace their role as stewards of the consumer data they collect and use” firms must “adhere[] to the three core best practices espoused by the FTC: privacy by design, simplified consumer choice, and transparency.”).

⁴ See U.S. Department of Justice and Federal Trade Commission, HORIZONTAL MERGER GUIDELINES (Aug. 19, 2010).

⁵ The FTC can form an empirical basis for its policies both by reviewing and synthesizing the relevant extant empirical literature and by using its own economic research capabilities to conduct new empirical research.

⁶ See James C. Cooper, *Comment on FTC Strategic Plan 2014-2018* (August 16, 2013), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2333794.

⁷ See, e.g., Prof. Calo, IOT tr. at 364. (data from a health monitoring device may be used to target junk food ads to consumers when they have finished exercising).

⁸ See, e.g., *In the Matter of Designerware, LLC* (Apr. 15, 2013), available at <http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2013/04/designerware-llc-matter>
In the Matter of Eli Lilly & Co., (May 10, 2002), available at <http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2002/05/eli-lilly-and-company>.

⁹ See, e.g., Kai-Lung Hui & I.P.L. Png, *The Economics of Privacy*, in HANDBOOKS IN INFORMATION SYSTEMS VOL. 1, ECONOMICS AND INFORMATIONAL SYSTEMS 489-92 (Andrew B. Whinston & Terrence Hendershott, eds., 2006) (reviewing the empirical literature and noting that “the key policy issue is not whether individuals value privacy. It is obvious that people value privacy. What is not known is *how* much people value privacy and the extent to which it varies.”); see also Leslie K. John et al., *Strangers on a*

solution – especially one geared toward people with above average sensitivities to non-monetary harm – will impose costs on large swaths of the population. Many would be willing to trade lower levels of privacy for lower prices or greater functionality.

Further, it is also unclear how providing certain institutions with more data to make decisions will be harmful to consumers.¹⁰ Business currently categorize consumers, and more data typically will allow for more, not less, accurate estimates of parameters like credit risk, health status, or interests. And although more accurate categorization may mean that some consumers receive worse terms, it also means that many consumers will receive better terms.¹¹ Further, firms have incentives to place consumers into correct categories; companies that systematically offer high interest credit cards to people with good credit or expensive auto insurance to good drivers will see their sales suffer. There may be societal reasons for setting price ceilings on credit or insurance, but preventing firms from observing differences and tailoring offers accordingly is an inefficient way to achieve this goal.

C. Privacy by Design and the IOT

Although “privacy by design” has become a cornerstone of FTC privacy policy, the FTC should consider carefully the extent to which requiring IOT firms to consider privacy “at every stage” will benefit consumers and impact innovation. Myriad considerations go into making a product attractive to a consumer. It is probably true that privacy is one of them, but enhanced privacy protections are costly and often can come at the expense of reduced data flows that negatively impact product quality.¹² Consumers ultimately bear these direct and indirect costs in the form of higher prices and reduced functionality. Further, IOT firms, rather than the FTC, are likely in a superior position to assess which combinations of price, quality, and privacy protections are most attractive to consumers. Companies that strike the wrong balance will suffer as consumers vote with their feet.

Plane: Context-Dependent Willingness to Divulge Sensitive Information, 37 J. CONSUMER RES. 858 (2011); Alessandro Acquisti et al., *What is Privacy Worth?*, (Carnegie Mellon University Working Paper), available at <http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-worth.pdf>.

¹⁰ See, e.g., Chairwoman Ramirez, IOT tr. at 12.

¹¹ This sort of precise categorization also may make competitive spatial price discrimination more likely. This sort of competition involves differentiated firms targeting discounts to consumers based on their relative distance (in product space) from a firm. In equilibrium, this can cause all consumers to pay lower prices. See James C. Cooper et al., *Does Price Discrimination Intensify Competition? Implications for Antitrust*, 72 ANTITRUST L. J. 327 (2005).

¹² See, e.g., Amalia R. Miller & Catherine Tucker, *Can Healthcare Information Save Babies?*, 119 J. POL. ECON. 289 (2011); Amalia R. Miller & Catherine Tucker, *Privacy Protection and Technology Diffusion: The Case of Medical Records*, 55 MGM'T SCI. 1077 (2009).

Absent empirical evidence of a market failure – for example, that firms do not fully internalize the costs associated with failing to provide desired levels of privacy or data security – the FTC should hesitate to suggest that an IOT firm risks a Section 5 complaint if privacy is not a paramount consideration at every stage of product development.¹³

D. Conclusion

The IOT holds great promise, and unwarranted restrictions on the ability of devices to collect and transmit data will harm consumers. Accordingly, the FTC should develop a firm empirical basis for doing so. As noted above, absent evidence of consumer harm and the degree to which a regulatory program will ameliorate this harm, it is impossible to determine whether such a program is actually benefiting consumers. Accordingly, before offering any recommendations with respect to the IOT, the FTC should engage in empirical research on the following topics:

- The likelihood that consumer data collected and transmitted via the IOT will be used in a manner that would cause consumer harm;
- The value that consumers place on subjective privacy harms;
- The extent to which consumers understand the privacy risks associated with IOT products and services;
- The extent to which consumers willingly undertake the risks of privacy harms in exchange for lower prices or better functionality;
- The extent to which consumers can take steps to ameliorate expected privacy harms and the costs of those steps;
- The extent to which firms internalize failures to provide levels of privacy and data security that consumers demand;
- The degree to which IOT firms compete by offering different levels of privacy and security.

* * *

In an empirical vacuum it is impossible to know whether FTC action surrounding the IOT is likely to benefit rather than harm consumers. The FTC should use its formidable economic research capabilities to fill this vacuum before making any policy recommendations with respect to the IOT.

¹³ See Chairwoman Ramirez, IOT tr. at 9; *In the Matter of HTC America, Inc.* (July 2, 2013), available at <http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2013/07/htc-america-inc-matter>.