MARKETS FOR PRIVACY AND DATA SECURITY: AN ECONOMIC AND LEGAL ANALYSIS FOR THE INTERNET OF THINGS

Geoffrey A. Manne & R. Ben Sperry

Abstract

In this paper, we consider several questions relevant to the FTC's privacy and security missions and their relationship to the Internet of Things (IoT):

- What privacy and security problems may develop as IoT evolves?
- How do market forces, including the reputation market, regulate IoT companies, and how well do they function to prevent harm to consumers?
- How well do existing common law legal remedies address potential harms to consumers in an IoT world?
- How does the FTC's existing legal authority apply to these problems? What limiting principles will guide the FTC in applying Section 5 to the Internet of things? In particular, what does "materiality" mean in a system of machine-readable disclosures made between devices? In general, how will the FTC define the three required elements of unfairness?
- How will FTC enforcement actions interact with self-regulation and reputation markets?

The FTC should be applauded for hosting this workshop to consider the consumer protection issues related to privacy and security issues in the commercial sector, especially as the Internet of Things becomes an increasingly important medium through which consumers interact with products and services. But before engaging in ex ante regulation, the FTC should do the hard work necessary to understand the market at issue and the consumer protections already available.

Markets for privacy and data security have several aspects worth considering. Companies have responded to consumer preferences by giving them new options to control their privacy through settings. There are also many tools available in the marketplace, such as browser add-ons and identity protection services. Customers have also punished those companies that failed to meet consumer expectations on privacy and data security. On top of that, industry has committed to self-regulation efforts, resulting in a higher level of privacy protection for consumers. And finally, it is always essential to consider the extent and ability of consumers to refuse to purchase products and how this helps police marketplace behavior.

Before seeking new tools or novel applications of its authority, the FTC should analyze the legal tools, private constraints and doctrines already in existence. One of these tools is the continued use of the FTC's Section 5 authority, especially over deceptive practices. But there are other tools available directly to the public that require no FTC action: the common law and several statutes at the state and federal level, as well as a range of self-help mechanisms. The FTC's 2012 Privacy Report failed fully to investigate the existing legal landscape. Among other things, that Report doesn't even mention tort law, which is supported by the flexibility of the common law process, as a viable means of achieving data security and improving privacy.

The White House and the FTC have stated that their goal is to promote self-regulation in this area. Much like the FTC's enforcement efforts on deception, the common law promotes self-regulation by holding companies liable for consumer harms they cause. Before asking for more legislation or regulatory authority over privacy or security, the FTC should analyze the ways self-regulation is already promoted under current law.

The FTC should also be aware of the consequences of how it chooses to use its Section 5 authority. As IoT develops, issues like regulation of location data, the nature of opt-in versus opt-out, and the importance of materiality in promises about privacy will become increasingly important. Sensors will increasingly be deployed in infrastructure and appliances, making everything around us "smart." This has incredible potential benefits, but will also allow for the increased collection of location data, which raises questions about how consumers can choose privacy levels that match their preferences. And as machine to machine communication becomes the norm, the application of legal doctrines must evolve in a way that makes sense and does not place an undue burden upon innovation.

This paper will engage in an economic and legal analysis of the markets for privacy and security as they relates to the IoT. Part I will introduce the law and economics of reputation markets and describe how the law can both reinforce and impede the effective functioning of these markets. Part II will assess how reputation markets have functioned in the IoT space and the extent to which they have encouraged companies to improve their information practices. Part III will examine the existing legal regime and the remedies available to consumers and companies for harms related to privacy and data security and how the current regulatory regime encourages companies to protect privacy and secure information. Part IV will conclude with recommendations for the FTC to consider as it enforces its consumer protection mission in the IoT space, including how to analyze the effects of agency action on self-regulation and reputation markets.

This research will be the first we are aware of to apply a law and economics framework to questions of privacy and data security in the IoT. This paper has not been commissioned by any company or published in any journal.