This column delves into privacy risks of the IoT using risk concepts that are more native to the security domain in order to conceptually bridge our collective understanding, articulation, and management of privacy concerns in the IoT which otherwise might not be sufficiently considered or foreseen by existing legal and technical controls.

Economics and Incentives Driving IoT Privacy and Security, Pt. 1

by Erin Kenneally
Department of Homeland Security (USA)
International Computer Science Institute

Data in the IoT is not self-executing: sensors and actuators provide the frontend collection and backend mobilization of data, respectively. Analogously, privacy and security in the IoT depend on sensors (awareness and control of data collection, use and disclosure) and actuators (law and market enforcement functions) to precipitate underlying rights and interests. Apropos to the theme of this edition, just as sensors and actuators effectuate data in the IoT, risk economics effectuate privacy and security risk controls in the IoT. My December 2018 column looked at IoT privacy and security risk through the lens of laws, standards and best practices that can prevent or mitigate potential injury to consumers, business interruptions, and direct loss to organizations' economic well-being. This month is the first of a two-part spotlight on several dimensions of the economics that drive the implementation of those IoT privacy and security ordering forces. This column covers the asymmetries and monitoring & enforcement dimensions of IoT privacy and security economics, while part 2 in our next edition drills down into the cost-benefit and incentives aspects.

The dimensions of IoT privacy and security economics are as follows:

1. The market is characterized by information, control and bargaining power asymmetries that favor large platform providers over users (individual and organizations) and threaten privacy and security management in the IoT
2. Monitoring and enforcement of privacy in the IoT ecosystem is impeded by attribution and provenance challenges
3. There is lack of information about the ROI (costs and benefits) for security and privacy to different stakeholders; and
4. Misaligned incentives.

Asymmetries in the IoT Market

Stakeholders in the IoT market include IoT providers[1] on the supply side, and organizational- and consumer-users on the demand side. The market for IoT goods and services is characterized by information, control and bargaining power asymmetries that favor IoT providers' economic interests over consumers' management of security (confidentiality, integrity, availability "CIA" of data) and privacy (abuses of personally identifiable information "PII") risks in the IoT. One question looming large is whether privacy and security in the IoT will be a market failure that results in costs to society that call for stronger government intervention.[2] In other words, will the market for IoT, if left to itself, fail to reach appropriate ('socially-optimal') levels of privacy and security protection for consumers? If past is prologue regarding the Internet ecosystem, then the IoT market is doomed. Namely, there are marked data collection, control and bargaining power asymmetries as between key direct stakeholders[3] — the large web platforms (e.g., Google, Facebook, and Tier 1 ISPs) and individual consumers.

These market dynamics of the online Internet ecosystem, if extended to the IoT, presage privacy and security risks in the IoT. For one, information asymmetries are the rule online as manifest by the large platform providers' oligopoly on PII, and the general lack of user control of their data collection and management.[4] When it comes to Internet security, poor understanding of cyber risk exposure at the entity and systemic levels is the rule.[5] Individual and organizational consumers are unaware or fail to comprehend the risks and lack adequate technical and policy controls to abate them.

The IoT enables IoT providers with the ability to collect information in ways that users are likely to be unaware. For example, the below-the-radar rollout of biometric sensors and analysis-e.g., facial-, voice-, behavior, gait-, and sentiment-printing,[6] serve as indicators that information collection obscurity has new lines of sight in the IoT. Data that may not present as identifying can and is being linked and analyzed in ways that make it such. Lacking awareness, users do not even know that they should have an opportunity to exert control (via consent and choice) to the collection of their data. Few users even ask if or how well a product considers privacy and security. That data asymmetry is exacerbated by a largely unilateral control of the sensor devices, whereby consumers lack effective means to manage or limit the dissemination, analytics and actuation of that collected data even if they so desired. Consumers can place tape over cameras, for example, but in general cannot control what the camera records and how it is managed by associated apps, not to mention the zero-sum tradeoff with loss of camera functionality for other apps s/he may trust that rely on the camera feature.

In addition to physical control, IoT providers are likely to retain logical control over consumer data under a de facto presumption that the collector owns whatever the sensors collect. This 'possession is 9/10ths of the law' posture has allowed Industry to stake out an aggressive position of data ownership, accompanied by an implicit ransoming of convenience if such control is rebuked by users. This disproportionate assertion of authority by IoT providers is rivaled by the lopsided disclaim of responsibility that pervades software EULAs and Terms of Use/Service. These postures combine to further skew the bargaining position of users and threaten to obscure privacy rights and interests when collectors intermingle users' data. The online market for personal information is steeped in the notion that the collecting entity owns the information (e.g., credit records, drug prescriptions, medical records),[7] thereby exacerbating asymmetries, especially as data is increasingly fused to create derivative forms. The current market in the United States is not structured to ensure individual consent, notwithstanding that the effect of the General Data Protection Regulation (GDPR) and its U.S. state counterparts are projected to change this tide. As commenters have noted, our global privacy laws which are based on the Fair Information Principles (FIPS) are ill-equipped to address the systematic nature of information risk to individuals and their PII: they do not address information cost, worth, or ownership; they focus on individual injury and not societal harm; they provide limited

Editor's Note: This editorial is an abridged version of a section in a larger co-authored publication, Internet of Things Privacy Forum, "Clearly Opaque: Privacy Risks of the Internet of Things," (May 2018).

judicial and administrative interests (only allowing for inspection, challenge, and review); and, they do not afford property interest (dispose, use, store, sell).[8,9]

Challenges to Monitoring and enforcing Privacy and Security in the IoT Ecosystem

Another dimension of IoT privacy and security risk economics is the difficulty of monitoring and enforcing those rights and interests due to the challenges of attributing security deficiencies and tracking data provenance from its collection to use. The enforcement of regulation, law and policy is problematic in the absence of a provable audit trail from data collection by sensors through the web of devices, networks, platforms and databases to some harmful outcome. Sensors used to collect information may be controlled temporarily by a user vis-a-vis an application but it is hard to track and control the downstream use of the data.

The ecosystem for IoT data is largely open and uncontrolled, such that knowing the source from which data is collected and further disclosed is problematic. This opacity includes the who- specific organizations handling the data, when- points in time when data is processed, and where- virtual and physical locations of data storage. Similarly, the confluence of hardware, software, and networks implicated in IoT ecosystems makes disambiguating between programmatic, environmental and adversarial sources of security deficiencies along the supply and value chain costly at best. Monitoring and enforcing adoption of privacy and security is nontrivial due to the sheer scale and complexity of the IoT data ecosystem, and the lack of transparency needed to understand data flows and interconnections. This poses an obstacle for investigations and administration of law and policy which rely on proof of causation or correlation of data compromise and misuse to responsible parties.

Uncertainty of Costs and Benefits

The degree of uncertainty surrounding the costs and benefits of implementing IoT privacy and security is another dimension to the economics that drive implementation. Actuating privacy and security in the IoT involves understanding trade-offs and calculating costs and benefits, both of which are still difficult to analyze. The cost and benefits of avoiding or minimizing IoT privacy and security risk, whether they be regulatory or market-based, must consider how those calculations pan out to users and IoT providers. This can be challenging because it is not necessarily a zero-sum proposition, where a benefit to users is necessarily a cost to a provider despite prevalent rhetoric that pits privacy and risk control as an enemy of innovation. In the face of inadequate information on costs and benefits for stronger (or weaker) privacy and security primary stakeholders are hard-pressed to justify investments in privacy and security management, via ROI or some other value calculation.

In summary we tackled two key economic challenges to sensing and actuating privacy and security in the IoT- information asymmetries and enforcement, and lifted the lid on the third challenge- cost and benefit uncertainty. Our next Column picks back up with a deeper dive into the IoT cost-benefit considerations and incentives that ultimately drive IoT stakeholders to implement privacy and security.

Erin Kenneally (erink@icsi.berkeley.edu) is a currently a program manager in the Cyber Security Division within the U.S. Department of Homeland Security Science & Technology Directorate. Her portfolio comprises cyber risk economics, data privacy, trusted data sharing and research infrastructure, and ethics in information and communications technology. She is founder and CEO of Elchemy, Inc., and served as a technology law specialist at the International Computer Science Institute and the University of California San Diego Supercomputer Center. She is a licensed attorney specializing in strategy, research and development, and execution of challenging and emergent IT legal risk solutions.

FOOTNOTES

[1] IoT providers is used as an umbrella term for manufacturers, developers, integrators, service providers, and retailers.

[2] See, e.g., Bruce Schneier, Security Economics of the Internet of Things (available at https://www.schneier.com/blog/archives/2016/10/security_econom_1.html)

[3] Noting that indirect stakeholders who control PII in the online, non-IoT environment include consumer data brokers and credit reporting agencies

[4] E.g., "The World's Most Valuable Resource is No Longer Oil, but Data," The Economist (May 2017); Cracked Labs, "Corporate Surveillance in Everyday Life", Data as the New Oil; Wolfie Cristl,"Corporate Surveillance In Everyday Life—How Companies Collect, Analyze, Trade, and Use Personal Data on Billions" (http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf).

[5] See "Cyber Risk Economics Capability Gaps Research Strategy," U.S. Department of Homeland Security, Science & Technology Directorate, Cyber Security Division, August 2018, doi: 10.23721/1460960, (https://www.dhs.gov/sites/default/files/publications/3950_CYRIE_Report_FINAL508.pdf).

[6] Evidenced by patent filings activity and commercial implementation.

[7] See U.S. Department of Health, Education and Welfare. Records, Computers and the Rights of Citizens. MIT Press, Cambridge, Mass., 1973.

[8] See, e.g., Hartzog, Woodrow. "The Inadequate, Invaluable Fair Information Practices." Md. L. Rev. 76 (2016): 952.

[9] Note that the US approach to privacy is fundamentally different than the EU which views privacy as a fundamental human right and requires individual's notice and consent for collection, use and sharing of their data.