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. 2

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

Our last column teed-up a two-part spotlight on key economic challenges to "sensing and actuating" privacy and security in the IoT: (1) information asymmetries in the IoT market; (2) monitoring and enforcement incentives; and, a brief intro to (3) cost-benefit uncertainties. This month we close the loop by delving deeper into (3) the costs and benefits and (4) incentives.

Uncertainty of Costs and Benefits

It is difficult, perhaps impossible, to quantify all of the costs and benefits flowing from strategies to either protect privacy and ensure security in the IoT, or to proliferate the free flow of data. Estimating costs of enhanced privacy and security to businesses can be straightforward, for example, the costs of adopting additional processes, contractual transitive risks, restrictions on storage, etc. Also, estimating the economic benefits to businesses for collecting and sharing data and optimizing device connectivity (which is to say minimizing or ignoring privacy) may be feasibly translated into monetary terms. For example, benefits can be calculated as increased revenue and reduced information costs for firms. However, estimating costs can be more difficult because:

- Some harms to consumers may not be legally enforceable or directly translatable in monetary terms; and
- Some harms are contingent (e.g., with better privacy and security, e-commerce may be stronger since consumers may hold-back demand/participation for fear of privacy and security risk).

Matching economic value flows is problematic over time since there are many actors and the effects are diffuse, which is to say they are not limited to a particular user whose personally identifiable information (PII) or system is or is not protected.

Cost-Benefit Considerations

To begin, there has been a dearth of economic cost-benefit analysis on the implementation of privacy and security risk management in the IoT.[1] Defining the variables required for such calculations is fundamental to such analyses. The value calculation is challenging when quantification is not easily measurable in terms of increased revenue from sales, cost of compliance, or physical impact to person or property. Economic harms related to privacy have traditionally not been measurable as a commodity, especially in Europe (and in some U.S. states) where privacy is a fundamental right not subject to proof of harm standards for enforcement. So, developing acceptable thresholds of quantity and quality of impact on individuals is nebulous at best. We can quantify benefits to a company and partially the privacy costs to firms, but there is little accounting for the privacy cost to individuals or even society.[2]

A key variable is who accrues the benefits and costs as between stakeholders, where the comparative benefits to industry and consumer-users of collecting data for product/service improvement is center stage. What about when the marginal benefit of the IoT to consumers is low and costs (of privacy and security) are speculative? Another important variable is the duration of time over which cost and benefit is accrued.[3] The analysis will be perverted if costs and benefits of security and privacy that are long term, latent/indirect, ongoing and/or cumulative are not considered as much as those that are near term, direct, one-time, and/or independent. With advancing analytics, data can become more valuable to building algorithms, models, and derivative information from the accumulated data, all of which carry both innovation and privacy and security implications.

Articulating the attributes of what is being bargained for is important. Are users paying IoT developers, manufacturers, sellers, integrators, and/or retailers (IoT stakeholders) for goods and services with PII? What is the relative cost and benefit of physical/biometric, logical, psychological, emotional, and financial identifiers? Are those implicitly exchanged by users for IoT stakeholders' responsibility for the stewardship of that data, and if so what are those costs? If the benefits of collecting and actuating data accrue to society, what is the concomitant cost of obligations to the persons who are paying via the use or disclosure of his/her data? What about externalized costs that accrue to society such as threats to democracy, such as we have seen with online data?

Advances in cyber security governance may be instructive with regard to privacy. The framing of risk decisions as gains or losses can have a measurable influence on risk attitudes of individuals and groups responsible for privacy risk management decisions at organizations. Management can view security and consumer privacy as an organizational cost to be subtracted from the budget, or as an investment with a business value return. The chosen view might increase or diversify the organization's willingness to invest in privacy and security management.[4]

IoT Privacy and Security Benefits Considerations

The degree to which benefits can and will be quantified for inclusion in the cost-benefit deliberation varies. Whether firms actually make this cost-benefit calculation is an open question. In sum, organizations' benefits from embracing IoT privacy and security risk management range from enhanced risk control to support critical compliance and governance, to increased operational efficiency. Some of the prominent benefits to Industry and consumers to avoid or minimize security and privacy risk include:

- Reduced legal (regulatory and liability) risk
- Reduced data breach costs
- Enhanced consumer trust and reputation
- Reduced threat vectors to users
- Protection of social welfare, fairness,[5] and demonstration of corporate social responsibility
- Business opportunity and competitive advantage

It is worth reflecting on the last benefit since it is likely to fire C-level synapses that drive most organizations' calculus. Embracing privacy and security risk management as a business opportunity rather than a cost center challenges the (prevailing) belief that unimpeded data collection and seamless intercon-

nection is a net benefit to revenue or business interest, and supports the notion that the anticipatory benefit of unadulterated collection is unproven and unjustified. Some companies may value privacy and security as a selling point, either by offering it as a service or product from which to generate revenue, or by leveraging it to create market differentiation and accrue financial benefit. Under this rationale, industry may be missing an opportunity to develop tools and services that allow user control of preferences and expectations when it assumes an antagonistic posture toward privacy and security.

Unmanaged data may be a liability insofar as it creates noise and obfuscates the relevant data from which value can be derived. The rationale is that data collection is smart for business because it reduces data bloat, the attendant inefficiencies, and the costs associated with holding onto data. Further, efforts to audit data for business efficiency purposes can be repurposed for additional cost savings related to legal compliance (e.g., GDPR data flow audit requirement). Assuming a protectionist attitude by obfuscating flows or gating the interconnection of devices to others in the IoT ecosystem, in the interest of capitalizing on future data value, may have near-term positive externalities for privacy and security risk management, although long-term cost and benefits to users is debatable.

IoT Privacy and Security Costs Considerations

As with benefits, the degree to which costs can and will be quantified in a cost-benefit calculation of IoT privacy and security risk management is undetermined. Considerations include:

Innovation and market competition: The most prominent argument related to the privacy and security costs to industry is that innovation will be stifled and the economic promise of the IoT will be impeded.[6] The contention is that compliance costs may well result in higher prices passed on to consumers, less useful products, and deterred competition and innovation, thereby exceeding any benefits of privacy management. Further, the adoption of disclosure control technologies, e.g., anonymization, aggregation, and other information flow speed bumps, will impose increased operational costs related to implementation and/or decreased revenues from failure to fully realize the value of the data. Even in the face of clear economic risk from lack of privacy management, some companies might decide that the benefits of opening up new markets or establishing platform dominance outweighs the cost of shirking privacy.

In addition, market competition may be negatively impacted. Data flow and interconnectivity restrictions may cause inefficiencies in sectors where companies have market power through platform dominance. This is certainly the case with the Internet-dominant content and service providers, e.g., Google, Facebook, Amazon, Apple, and the like, that have business models varyingly dependent on advertising that is predicated on user data. This may even hold in the case of U.S. network service providers, especially if revenue models expand beyond moving bits to capitalizing on the user content and metadata it controls to increase margins. IoT platform oligarchs are TBD at this point in time.

Finally, it is doubtful whether there is a market value for privacy and security, which is to say that neither the privacy buy side (users) nor the supply side (industry) care enough about either to render privacy or security a market differentiator.

Competing rights and interests: Privacy is not absolute, and there are competing, legitimate demands by government, industry and citizens for data collection, access and control such as government and corporate interests in national and enterprise security. Stakeholders in the health, medical and automobile industries contend that the widespread collection of data is essential to improve and realize the potential of healthcare, medicine, genomics, and the safety of autonomous vehicles.

Lack of countervailing benefits: Critics of a precautionary approach to privacy and security management point to the lack of evidence that consumer welfare will improve if practices and recommendations (e.g., data minimization, notice & consent) are adopted.[7]

Assumption of duty and liability: If the default expectation is minimal/no privacy and security in the IoT, companies that offer an expectation of privacy and security through some explicit or implicit warranty might expose themselves to data breach costs that did not previously exist. Given the uncertainty regarding privacy and security liability within IoT supply chains, organizations asserting data protection capabilities may be concerned about assuming duty and liability if security is breached or privacy is infringed somewhere in the supply and service chain. In an insecure and interconnected ecosystem, for example, developers may be reluctant to assure privacy when it is unknown whether manufacturers may release devices with default passwords or known vulnerabilities that would enhance the success of privacy and security threats. Small companies would especially be concerned about this cost since the financial severity could be devastating if they are the only ones in the chain 'selling privacy' and any number of entities in their supply chain, e.g., developers, manufacturers, integrators, and retailers, could potentially seek indemnification therefrom. In other words, the company making privacy or security assurances might be targeted by others in the chain who may be sued for breaches.

Misaligned Incentives

A significant knock on the effect of the information asymmetries discussed in Part I[8] is the perversion of incentives to manage privacy and security risk as between users and IoT providers. This is evidenced, for example, by the well-documented discrepancies between users' stated and revealed preferences, colloquially known as the "privacy paradox."[9] Users may have an interest in better management of their privacy and security in addition to the promised utility of IoT devices. IoT providers, on the other hand, are motivated to collect as much data as possible not only because of its real and potential value (e.g., product improvement for optimizing revenue and decreasing costs), but also it may simply be cheaper to collect, copy and share data than it is to delete or refrain from collecting data. However, this incentive misalignment is obscured in the market: the information, control, and bargaining asymmetries that leave users unaware of or apathetic to privacy and security risks thwart the signals of users' stated motivations. Market perversion is the end result, a façade of aligned incentives between industry and users, contributing to a dearth of competition for privacy and security in the market. Providers in the online data marketplace do not compete on privacy, and only slightly for security, and at the moment there are few signals that this will change with the IoT. If that is the case, users will have few real choices for privacy and security and therefore will not be able to select IoT providers based on security or privacy risk features.

Furthermore, as industry invests in the collection, use, and disclosure of data and is not incentivized to fully consider the security and privacy impacts of those actions on users, it creates negative externalities, another hallmark signal of a failing market. A breach of sensitive data in the IoT often harms the data subjects more than the company that lost the data or the one in the supply chain responsible for the insecurity that lead to the data compromise. Reminiscent of the tragedy of the commons problem, IoT providers are not incentivized to consider privacy and security risk management amidst the free flow of data, interconnectedness of devices, and relative lack of privacy and

security forcing functions. Additionally, users whose connectedness puts fellow individuals' privacy and security interests at risk may lack motivation to seek privacy-sensitive and security-sensitive products and services (or stop using those that are invasive) because they may not experience the negative impacts that would raise awareness. Thankfully, the Golden Rule is future proof, so presumably social norms will be a forcing function in this regard.

In short, the lack of incentives for embracing privacy and security risk management include:

- Uncertainty of security and privacy benefits: lack of data ownership and responsibility across data flows and the IoT supply chains.
- Lack of technical education and awareness prohibits privacy and security overseers from asking the right questions and seeking proper solutions.
- Uncertainty of IoT liability exposure.
- Lack of an effective market mechanism to address privacy and security: data breaches have become normalized and breach fatigue has taken hold, so the fear of breach and its after effects is a diminished forcing function.
- The fungible aspect of many IoT technologies: cheap, short shelf-life devices or components leave original device manufacturers no reason to update devices.
- Indirection with users: most relationships in the IoT ecosystem are B2B (business-to-business), not B2C (business-to-consumer).

There are, however, a diverse range of potential incentive mechanisms for sensing privacy and security risk and actuating their management, such as: standards and best practices; regulation and laws requiring data disclosure, transparency, sharing, and secure practices; developer-level privacy and security principles by design; insurance for small and medium providers/developers; and technical and legal supply chain accountability mechanisms.

In summary, just as sensors and actuators effectuate data in the IoT, risk economics effectuate privacy and security risk controls in the IoT. 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. Key economic challenges to sensing and actuating privacy and security in the IoT include: information asymmetries, incentives, uncertain costs and benefits, and enforcement. We still have an opportunity to avert Groundhog Day relative to how security and privacy has played out on the Internet stage by tackling these issues head on in the development and deployment of IoT.

Erin Kenneally (erink@icsi.berkeley.edu) is a currently a program manager in the Cyber Security Division within the U.S. Dept 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 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] This is largely the case with cost-benefit analysis of security, which in many circumstances is a prerequisite to achieving privacy. However, recent research finding that the cost of insecurity outweighs connectivity's benefits may be prescient for IoT privacy, see e.g., Zurich, "Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures."

[2] Data breach class actions have not adequately made consumers whole. Federal circuit courts are split on whether Identity theft claims that rest on increased threat rather than actual fraudulent use are deemed too speculative to meet standing requirements, as are damage pleas related to fear and emotional distress that result from vulnerability to a future attack.

[4] See, e.g., Mersinas, Hartig, et al, "Measuring Attitude Towards Risk Treatment Actions Amongst Information Security Professionals: An Experimental Approach", Conference Paper, June 2016.

[5] Ensuring that consumers who bear the costs of collected PII also accrue the benefits is important to reducing negative externalities that can lead to market failure.

[6] See, e.g., CSIS Report - Managing Risk for the Internet of Things: Executive Summary https://csis.org/publication/managing-risk-internet-things; Jane Bambauer, "The Perils of Privacy as Property: The Likely Impact of the GDPR and the CCPA on Innovation and Consumer Welfare, Testimony before the Senate Judiciary Committee (March 12, 2019); https://www.accenture.com/us-en/insight-industrial-internet-things-growth-game-changer.aspx.

[7] See, e.g., Dissent of Commissioner Wright, FED. TRADE COMM'N, THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD Report.

[8] 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.

[9] See, e.g., FTC Harms Workshop, Panel on Measuring Information Injury (December 2017).