ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Internet of Things: Navigating the Changing Waters

Technology, Privacy, and eCommerce



In today's expanding technology marketplace, the hottest topic, commodity, and, at times, area of controversy is the Internet of Things (IoT). Also of interest is its ever-present companion, the large volume of consumer data the IoT utilizes. Although many businesses are already involved in the IoT as part of their product portfolio, ultimately, if any business uses a smart device, it's impacted by myriad issues circling the IoT and big data. The IoT is, undoubtedly, a source of tremendous promise, solutions, and revenue. Like any golden goose, however, as the technology develops and becomes more entrenched in the daily life of consumers, the concerns — both legal and otherwise — and risks to consumers rise at a rapid pace. Businesses are faced with regulations that aren't keeping up with the speed at which the IoT technology is developing and gaining momentum.

Maintaining privacy in a changing environment

A 2014 Pew Research study recently reported that 91 percent of Americans agree or strongly agree that consumers have lost control over how personal data is collected and used. This is a staggering statistic for companies in the IoT space actively collecting and using personal data, bolstered by the fact that the IoT space is rapidly expanding. Research firm Gartner forecasts that 6.4 billion connected things — physical devices, vehicles, buildings, and other items — will be used worldwide in 2016. This number is up 30 percent from 2015, and will reach 20.8 billion by 2020. This exponential growth needs to be met with new privacy solutions. Aaron Haggarty, senior vice president and general counsel of ForgeRock, explains, "the rapid growth of the IoT and the digital economy is posing enormous challenges to businesses and the public sector in terms of protecting personal data privacy and building trusted relationships. Consumers need to know that while current tools enable organizations to meet previous well-understood compliance requirements, these tools are clunky and take an all-in approach." He continues, "With this changing environment, there is likely to be an increased awareness amongst consumers for new approaches to privacy and security."

Perhaps the solution for both consumers and companies is to change the way both sides approach privacy. The alternative is trying to use existing solutions meant for older technologies and perpetually trying to fit a round peg into a proverbial square hole. As Haggarty explains, “while the practice of privacy is an increasingly mature discipline, traditional consent tools are unable to live up to customer and business demand for new data privacy options. Further, consent language hasn’t kept up with newer options for engaging with online data-sharing flows that involve web API access authorization and the ‘Share’ paradigm. In response, companies like ForgeRock are signing on and actively supporting ‘User Managed Access’ — an open standard developed in the market to help consumers retain control of their data and allow them to decide when and with whom to share their most sensitive personal information.” This approach will, hopefully, continue to expand as it allows consumers to have greater control. It also increases the likelihood of corporate compliance, because the leaders in the IoT space were integrally involved in creating the new standard.

Security by design

Regardless of the type of IoT device businesses are dealing with, keeping the data of consumers secure has definitely become a top concern. This is especially true for businesses in the European Union that are facing the looming General Data Protection Regulation (GDPR) regulations and their financial ramifications. There has been an active increase in both awareness and activity in terms of cybersecurity, preventing breaches, and ensuring vendors are vetted properly. Businesses know that they are one security breach-related public relations disaster away from significant revenue loss. With this — among other reasons — in mind, they are rapidly trying to get ahead of the eight ball. Businesses that do this successfully focus on designing IoT products with security in mind from the very beginning. By doing so, they create the most beneficial products possible for their customers, and stay on top of the security game.

As Olga Rodstein, head of legal at Electric Imp, Inc., explains, “security remains one of the top concerns for IoT customers, particularly larger industrial clients who need a solution that would enable them to scale rapidly to millions of connected devices without jeopardizing the security of data that flows through. So any IoT market entrants (and there're quite a few entrants now who call themselves ‘IoT’) need to be mindful of this concern and ensure that security is not treated as an afterthought.” Electric Imp is an example of an IoT company that treats security as a top priority. “What gives our customers comfort is the fact that we recognized from the start the importance of security and built it into the very core of the Electric Imp platform architecture,” says Rodstein. The concern for security goes beyond product design. “In addition, IoT customers may be subject to various industry or government regulations so IoT vendors may be expected to help customers meet these compliance obligations,” explains Rodstein. “This may include designing an appropriate security audit or testing program that would meet a customer's need for compliance without at the same time creating an undue burden for the IoT vendor. These terms should, where appropriate, be addressed contractually and it's important for both sides to agree on allocation of liabilities that may arise from such obligations."

Despite their reported concern, at this point in time, consumers are not actively engaging in managing their privacy and security en masse. IoT companies can lead the charge by actively considering security when designing their products. Mary Vincent, the entrepreneur in residence at SK Telecom and long-term advisor to companies in the IoT space, explains, “I credit Gary Davis of Intel with a list of the straightforward points companies must address when designing their products. While there are many things consumers should be doing with respect to wearable and mobile device security such as changing default passwords, turning off Bluetooth when not required, reading privacy policies, and being constantly aware of permission settings, they just don’t do this with

sufficient regularity.” Vincent acknowledges that companies have a responsibility to remedy these lapses. “IoT companies can help bridge this gap by including certain safeguards as part of their product design such as requiring stronger passwords, only collecting the data necessary to deliver the service, and using multi-factor authentication and communication whenever possible,” she says. “In this way, companies can lead the charge and build consumer confidence by teaching consumers how to actively engage in protecting their privacy. It’s really a win-win.”

Gaining and maintaining trust

Businesses are daunted by the financial ramifications of a security breach, but perhaps an even greater threat is losing customer trust. Companies spend countless dollars and hours building a good relationship with their customers. Given the type of data IoT devices store, analyze and transmit, consumers are becoming both more aware of and concerned with their sensitive information landing in the wrong hands. The delicate balance between maximizing an IoT product’s revenue potential and maintaining the hard-earned trust in today’s environment is more precarious than ever.

This is an issue that Harry Gottfried, senior corporate counsel at GoodData, has spent a great deal of time thinking about. "We live in a society with competing values and ideas about vast data collection programs and we seem to always have an institutional tension between personal privacy concerns of consumers and commercial interests that use data to advertise and market products using myriad modes and methods. We have witnessed large scale data hacking and abuse by companies we use and ostensibly trust on a daily basis, whether it is your bank, your grocery and consumer goods stores or the health care systems we use,” says Gottfried. In order for the IoT to strike the right balance, Gottfried believes, “businesses will have to gain or maintain the trust of their customers by using the data collected in prudent, transparent, and efficient ways that ultimately serve the best interest of the consumer.” The key to continued relationships between companies in the IoT space and their customers lies in companies having an inherent drive to go above and beyond the current minimum standards.

Clearly the IoT phenomenon is here to stay and that is most definitely a good thing. The emerging technologies allow consumers access to real-time information, automated products, and seamless interaction in way that was unfathomable in the not-too-distant past. The key for companies is approaching both privacy and security in a different way than the established status quo. The undeniable reality is that consumer demands with respect to these issues will increase as awareness about risk grows. The companies that will ultimately come out on top are those already planning to be at the forefront of addressing challenges without sacrificing consumer trust.

Olga V. Mack



Fellow

CodeX

Olga V. Mack is a fellow at CodeX, The Stanford Center for Legal Informatics, and a Generative AI Editor at law.MIT. Mack shares her views in her columns on ACC Docket, Newsweek, Bloomberg, VentureBeat, Above the Law, and many other publications.

Mack is also an award-winning (such as the prestigious ACC 2018 Top 10 30-Somethings and ABA 2022 Women of Legal Tech) general counsel, operations professional, startup advisor, public speaker, adjunct professor, and entrepreneur. She co-founded SunLaw, an organization dedicated to preparing women in-house attorneys to become general counsels and legal leaders, and WISE to help female law firm partners become rainmakers.

She has authored numerous books, including Get on Board: Earning Your Ticket to a Corporate Board Seat, Fundamentals of Smart Contract Security and Blockchain Value: Transforming Business Models, Society, and Communities. She is working on her next books: Visual IQ for Lawyers (ABA 2024), The Rise of Product Lawyers: An Analytical Framework to Systematically Advise Your Clients Throughout the Product Lifecycle (Globe Law and Business 2024), and Legal Operations in the Age of AI and Data (Globe Law and Business 2024).

Katia Bloom



Commercial Lawyer and Associate General Counsel

ForgeRock

Katia Bloom is a fast-paced and strategic commercial lawyer. Currently, she is the associate general counsel at ForgeRock. Previously, she headed up legal for Avira, Inc., was a founding partner at E Squared Law Group, advising many start-up clients and was in-house counsel at Anesiva. She is actively involved in the Association of Corporate Counsel and a number of organizations promoting

women in the legal profession.