When Mundane Objects Become Smart: Challenges of Standardizing the Internet of Things

Julia Suozzi

jpsuozzi@gmail.com

University of Virginia

Spring 2018

Abstract

The purpose of this essay is to address the need for standards in modern communication, explain the challenges in creating these standards, and propose various solutions to these challenges. With the evolution of the Internet of Things (IoT), everyday objects have transformed into connected devices that are vulnerable to a host of attacks. In order to protect users, standards must be put into place. Although necessary, standards are extremely complex to develop due to their sociotechnical nature. Challenges in this process include market definition, determining what and when to standardize, organizational responsibility, and international competition. First, market definition must be considered due to the nature of standards compliance. Businesses comply with standards when there is a market associated with them and that market is well-defined. Since the IoT does not have such a monolithic market, how should standards be created? The next major challenge is knowing what to standardize and when it is appropriate to do so. This paper will explore approaches as described by members of the government, industry, and academia. Responsibility is also a major challenge of standardizing the IoT. With so many organizations holding stake in the process, who is truly responsible for taking the lead? This question brings up issues of organizational politics, as each group has their own agenda and mechanism for reaching consensus. Lastly is a discussion of international competition. Many organizations involved in IoT standardization have international participation. Each of these nations has a fundamentally different view on issues such as "safety," "privacy," and "security," making it difficult to reach global consensus. This issue is explored using the recent US-China trade war. In order to better understand these challenges and discuss potential discourse, a case study based on interviews with key IoT stakeholders is presented, focusing on the Internet Engineering Task Force, the Institute of Electrical and Electronics Engineers, and the National Institute of Standards and Technology.

When Mundane Objects Become Smart:
Challenges of Standardizing the Internet of Things

In July of 2017, the FBI issued a warning to parents about the dangers of internet-connected toys saying that consumers should "consider cyber security prior to introducing smart, interactive, internet-connected toys into their homes" (Leamy, 2017). This warning was released five months after two major events occurred concerning connected toys. First, the German government banned the My Friend Cayla doll, an internet-connected device that was found to be susceptible to hacking. Second, half a million user profiles were leaked from a data breach of the CloudPets database, with many of these users being children (Matthews, 2017). These episodes indicates a series of new security concerns in a changing world where daily, mundane objects are turned into "smart technologies," in this case, "smart toys." These toys are not as simple as placing a chip inside a Barbie doll; rather, they are connected to the Internet of Things (IoT), the vastly integrated network where physical objects are embedded with advanced electronics, software, and sensors for interoperable data communication. These smart products, though they satisfy consumer demand for remote access and communication with these devices over the internet, automatically open ports on home routers, presenting a vulnerable surface for those with malicious intent.

These smart objects sit at the boundaries of old and new technologies, having both the most mundane, innocent features along with unknown cybersecurity threats. These devices then pose a series of challenges in IoT standardization, specifically, how to develop standardized frameworks for such large scale and increasingly growing global networks that allow integration of both traditional and advanced technologies embedded in one device. To understand the challenges of standardization and their potential solutions, this paper presents a sociological study based on my interviews with various key IoT stakeholders, in particular the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), and the National Institute of

Standards and Technology (NIST). At IETF, several working groups spanning multiple areas develop IoT-related protocols, which are directly used by standards-developing organizations (SDOs). Their work is heavily focused on internet protocols and networks, which are fundamental to a secure communication infrastructure for IoT. IEEE is also directly involved in IoT standardization. Of its 39 societies organization-wide, 22 are involved in IEEE's initiative on IoT including the IEEE Standards Association (IEEE-SA) which formally creates standards. NIST on the other hand is a scientific research institute and an agency of the US Department of Commerce. While they do not formally create standards, their work provides a foundation for other SDOs.

What is the IoT "market?"

An immediate challenge in IoT standardization comes from the lack of "a well-defined market" for smart devices. Traditionally, standards are produced for clearly-defined purposes in response to market demand. For the IoT, as Geoff Mulligan, a member of the IoT Directorate Group from IETF, pointed out, "what isn't the Internet of Things?" Currently, there is no such monolithic "IoT market," but instead a mixture of well-established companies such as Google, Facebook, Amazon; rising startups such as Ayla; and traditional industries such as kitchen appliances and lighting. Given such an open, unbounded, and diverse network, how, then, should standards be created?

The scale and level of integration required in IoT standardization poses challenges to device labeling, coordination, and identification, which further trigger the concern about data privacy and ownership. In addition, given the number of devices involved, a robust standard infrastructure thus leads to higher production costs, resulting in more expensive products. Depending on the device, consumers may or may not agree to pay the premium on a product just because of security. For example, consider an internet-connected toy versus a smart scale. Many

more consumers are likely to pay more to protect their children than to keep their weight private. The cost concern may contribute to another layer of instability in the already messy "smart market."

When and what to standardize? Different approaches from government, industry and academia

It is clear that searching for a "one-size-fits-all" solution will be extremely difficult. Different stakeholders share different perspectives regarding when and what to standardize. Dr. Yaw Obeng, a research chemist from NIST, shares a different perspective. He argues that it is important to implement a robust, cyber-infrastructure and standards framework preemptively for smart device connection in order to mitigate the potential risks of internet-connected devices (Y. Obeng, April 11, 2018). This requires standardization mechanisms for identifying and measuring the robustness of devices in order to find those that are insecure, as well as securing those vulnerable devices. This infrastructure, as Obeng argues, will provoke not just compliance but will also help companies gain public trust in their products. However, Adam Drobot, chair of the IoT Activities Board at IEEE, stated that standardization of the IoT can only occur when the market and technology become more mature and stable. He argues that without substantial growth and some backing upon which to base standards, nobody will follow whatever guidelines are put into place. Coming from industry, he expressed concern with a top-down approach and argued that it is too difficult to standardize when nothing has actually gone wrong. Rather, industries would prefer IoT standards be put into place in response to attacks when it is clear what to standardize for. Another bottom-up approach is proposed by Scott Peppet, a professor of law at the University of Colorado Law School (2014). Instead of implementing a top-down cyber-infrastructure network or waiting until something goes wrong, Peppet suggested that the standardization problem be

divided into a series of smaller actions. For example, the definition of "personal information" should be extended to include data obtained from IoT sensor devices. These "smaller actions" may be the responsibility of regulators and legislators such as the Federal Trade Commission who, according to Brill and Jones (2017), has "statutory authority" over "matters of information privacy." When considering opinions from academia such as those of Peppet, Brill, and Jones, it should be noted that such academics are granted tenure credit for publishing papers. In order to prepare for the future of the IoT, Michael Richardson argues that academics should instead receive credit for doing "real work," which may include contributing to the development of standards (March 2015).

Which organization is in charge?

Stakeholders' various approaches raise another challenge for IoT Standardization: who should take the lead in standardization? Which organization should be responsible to make the rules? According to Adam Drobot, there are over 300 SDOs involved in IoT Standardization around the world, including IEEE and IETF. As mentioned earlier, the IEEE-SA is the official standards-making group within IEEE, but 22 of IEEE's 39 societies are involved in the initiative on IoT. The IETF also has an IoT Directorate Group which promotes communication amongst the IoT IETF working groups, as well as with other SDOs (G. Mulligan, March 21, 2018). In other words, no single individual, company, or organization has the solution. Instead, shared responsibility and division of labor is required for effective IoT standardization.

Meddeb (2016) argues that organizations should unify their efforts and create standards cooperatively. This approach, while enticing, is difficult to accomplish. Based on my interviews with IETF, IEEE, and NIST, many organizations do interact with each other, however, this interaction is often on an individual basis. The critical challenge is to understand the organizational

cultures. Each organization standardizing in the IoT space has their own agenda and mechanism for reaching consensus. Looking first at the IETF, Geoff Mulligan stated in his interview that "IETF is run almost like an anarchy" where anyone can show up and "vote." To express their level of interest on an issue, attendees will make a humming noise where a louder volume denotes stronger interest. The main purpose of this process called "humming" is to get a rough consensus on an idea or implementation, but it also serves as a way to hide identity. On the contrary, IEEE uses a more formal voting process. When someone initiates an action for a standard, each individual gets one vote and "discussions go on until all opposition ceases" (A. Drobot, March 28, 2018).

This question of responsibility indicates that the purpose of IoT standardization is not just to develop a robust technical solution. Rather, it demands cross-institutional communication and coordination. In order to achieve collaborative standardization, protocols should be put into place to facilitate communication among organizations involved in standardization.

International competition

Meeting the requirements of cross-organization communication requires international participation, which adds another layer of complexity to reaching a consensus. Each IoT committee/work group from various SDOs has members from Europe, North America, and recently Asia. The primary issue is to generate a unified definition, codification, and framework toward the notions of "safety," "privacy," and "security" under such a "large variability in the views of those issues around the world" (A. Drobot, March 28, 2018). Due to the associated social and culture values behind these terms across nations, the problem of defining them has made IoT standardization a prolonged negotiation process over not just technical topics, but also broader societal and diplomatic issues among international stakeholders.

The recent US-China trade war serves as the best example to understand the deep entanglement between IoT and international politics. Since February, friction between the United States and China over advanced technologies has been increasing, showing concerns from the US of losing the IoT competition. Acting on the recommendations of the Committee on Foreign Investment in the US, the federal government blocked the Broadcom-Qualcomm deal due to national security risks[1] to preserve the 5G chip manufacturing capacity in the US. The US Department of Commerce banned US companies from selling components to ZTE, a China-based multinational telecommunications equipment and systems company, which is the main provider of the Huawei Technologies Co., one of the top competitors in the global 5G/IoT industry. After falling behind on both 3G and 4G standards, China is fighting for both global leadership and to be the leader of 5G by developing a set of standards that better suit their nation's needs, particularly in the area of China 2025, a national strategic plan of utilizing IoT to upgrade manufacturing (Forbes 2018). China's rigorous efforts in IoT standardization have been manifested through their active participation in international standards bodies. However, the existing organizational cultures to overcome both cultural and language barriers in international standards-making remains to be a critical challenge for every SDO. Michael Richardson, an open-source developer and member of the IoT Directorate Group at IETF, expressed that diversity with respect to race and gender is also a concern for international standards-making that must be addressed.

Conclusion: Smart devices require smart organization and standards education

The world is changing and the integration of old technologies with smart technologies is a significant challenge in the realm of standardization. The case study herein demonstrates that creating IoT standards goes beyond inventing new technologies or writing documents. Through

[1] Qualcomm is one of the leading companies in 5G chip manufacturing; Broadcom is a Singapore-based developer and global supplier of semiconductor products who recently attempted to acquire Qualcomm

studying stakeholders' current practice of IoT standardization, this paper identifies several knowledge, organization, and policy barriers. In order to combat these issues, more communication must occur between stakeholders at both the organizational and the international levels. Therefore, standardizing the Internet of Things is about cultivating a new culture that allows cross-cultural communication and collaboration among innovators, regulators, industrial and private sectors, and consumers. Through increased communication, stakeholders can learn to appreciate the complexity of standards and reach consensus to secure modern communication.

Finally, as a fourth-year engineering student who has been studying IoT related technologies throughout my undergraduate career, standardization had never occurred to me as a subject of interest until I had the chance to meet IETF and IEEE staff. Adam Drobot from IEEE stated that this organization has a group called the Society on Social Implications of Technology. This group aims to educate technologists and engineers about the impacts of technology on society so that they can better practice social responsibility in engineering (IEEE). They often hold meetings relating to the impact on society in a global context such that international interests can be discussed and hopefully upheld.

In conducting this research, standardization has provided a new lens for me to appreciate the social complexities of engineering industry, which is important for any engineer to understand before beginning their career. Along with growing academic interests in IoT, I hope this paper provides a persuasive case to show the urgent demand to incorporate international standards education into engineering education.

References

Adam Drobot. (2018, March 28).

Brill, H., & Jones, S. (2017). Little Things and Big Challenges: Information Privacy and the Internet of Things. American University Law Review, 1183–1230.

Dr. Yaw Obeng. (2018, April 11).

Geoff Mulligan. (2018, March 21).

IEEE Society on Social Implications of Technology Membership. (n.d.). Retrieved April 27, 2018, from https://www.ieee.org/membership-catalog/productdetail/showProductDetailPage.html?product=MEMSIT030

Imagining the Internet. (n.d.). Best Action for Future? IETF 2015: Michael Richardson. Retrieved from https://www.youtube.com/watch?v=T5tvaBPnSiE

Leamy, E. (2017, September 29). The danger of giving your child 'smart toys.' Washington Post. Retrieved from https://www.washingtonpost.com/lifestyle/on-parenting/giving-your-child-internet-connected-smart-toys-could-be-dumb/2017/09/29/a168218a-a241-11e7-8cfe-d5b912fabc99_story.html

Mathews, L. (n.d.). The Latest Privacy Nightmare For Parents: Data Leaks From Smart Toys. Retrieved April 26, 2018, from https://www.forbes.com/sites/leemathews/2017/02/28/cloudpets-data-leak-is-a-privacy-nightmare-for-parents-and-kids/

Meddeb, A. (2016). Internet of Things Standards: Who Stands Out From the Crowd? IEEE Communications Magazine - Communications Standards Supplement.
Michael Richardson. (2018, March 27).

Peppet, S. R. (2014). Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent. Texas Law Review, 85–178.

The Internet of Things. (n.d.). Retrieved April 27, 2018, from https://www.ietf.org/topics/iot/

The U.S., China And Others Race To Develop 5G Mobile Networks. (n.d.). Retrieved April 26, 2018, from https://www.forbes.com/sites/stratfor/2018/04/03/the-u-s-china-and-others-race-to-develop-5g-mobile-networks/#2ab982415875