Ubiquity, Interrupted? European Governance of the Internet of Things as an Emerging Technology

Mailyn Fidler, Stanford University

July 17, 2013

The Internet's transformative effects on society are well established. The Internet, however, is expanding and is on the cusp of establishing a ubiquitous presence in everyday objects. With a specific focus on European Union, my Stanford honors thesis analyzes the attempts of governance bodies to grapple with this emerging "Internet of Things" (IoT). As part of my research, from June 2012 through February 2013, I interviewed policy, industry, non-profit, and academic experts in Europe, China, and the United States about emerging government approaches to the IoT. This summary describes my main findings, and the full manuscript is available on request.

European Union

The IoT has been a political priority for the European Union. Even with the recent recession, interest and funding in IoT enterprises has not slowed, and the EU has invested 70 million Euros in at least 50 research projects since 2008. In addition to the EU's hopes that the IoT will bring economic benefits, particularly to small businesses and public institutions, the EU's interest in the IoT reflects its concerns about who controls emerging technologies. Indeed, EU officials have stated an ambition to build an IoT "that will bring about clear advantages for Europe." However, despite the EU's investments, a lack of legislative clarity, slow technical progress, and pressure from international strategic interactions threaten to slow EU efforts to develop a globally competitive, European-centric IoT.

The EU considers privacy a societal priority and has a history of regulating technologies to prevent privacy risks, as its Data Protection Directive indicates. The IoT is no different. The privacy risks the IoT presents, however, are discussed in the context of ongoing data protection reform in the EU. EU officials are debating how to author broad, technology-neutral guidance while, at the same time, many officials seem convinced that technology-specific guidance will be necessary. The EU's political prioritization of the IoT fuels attempts at lobbying for IoT-specific regulation, as the myriad, overlapping attempts at IoT guidance demonstrate. The IoT's advancement, then, is mired in this larger debate about the future of technology policy.

The EU's privacy focus leaves some IoT security questions without adequate attention, even as the EU legislative community continues to emphasize information security. For example, in the 2010 Cluster of European Research Projects on IoT, only 1 of the 33 funded projects explicitly investigated security. In a 2010 EU study on IoT standards, only 2 of 175 dealt with security. Wholly unaddressed, however, are issues of IoT cybersecurity. Neglecting this issue will disadvantage the EU as IoT devices become more prevalent and other countries gain IoT expertise.

The EU relies on the established, slow moving standards process but could lobby more aggressively for standardization. Instead, the EU debates the advantages of backing existing or new standards. Part of the EU's hesitancy in picking a side to support stems from a desire to select standards that will specifically benefit the EU's vision for the IoT as it develops. The EU

seems reluctant to play a leading role in the international IoT standards process unless it can guarantee the standard will benefit its internal IoT communities.

The debate about whether the EU should support a new, international IoT governance mechanism for the IoT has obscured other important aspects of the IoT debate. The controversy lingers as the EU considers its own internal guidance, leaving legacy "battle lines" and potentially constricting the set of options and language the EU can use to create this EU-level guidance.

China

China, like Europe, sees economic hope in the IoT. In 2008, China identified the IoT as a strategic industry and plans to invest $800 million USD in IoT by 2015. China also recognizes the potential for a boost in global power through dominating the IoT. An expert I interviewed indicates that China feels boxed out of many existing technological areas, and the IoT provides them with fresh innovation territory: "It's a new IT area, where China has the chance to develop cutting-edge technology, versus operating systems or semiconductors, where the barrier to investment is too high." Bi Ran, an engineer at the Network and Switching Research Department of the China Academy of Telecommunication Research (CATR) of the Ministry of Industry and Information Technology, comments that the "IoT is a political issue" and that China "wants some company to be the leader of IoT industry at an international level, so they are funding basic technology research."

China pursues its quest for IoT superiority by planning its own IoT standards regime as well as participating in global standards processes. For instance, China has stated that, by 2015, it will develop 150-200 standards for the IoT, a figure vastly more ambitious than any country or regional body working on the IoT. The government pursues this strategy because Chinese standards benefit Chinese companies, which will have priority access to China's large market as well as hefty government procurement contracts.

Concerns exist, however, that the Chinese government's enthusiasm is overshadowing the reality of the IoT's ability to benefit Chinese consumers. As China pursues national power through the IoT, it must balance the actual needs of people, such as the rural farmers it hopes will adopt the technology, with its fast-paced bid for international IoT prowess.

The United States

The IoT in the United States is characterized by late but strong entry of companies to the market and by recent, but minimal, interest from the federal government. Specifically, the federal government views the IoT largely as part of the ongoing privacy and security discussion in Washington, D.C. Complicating analysis of the IoT in the United States is that the "Internet of Things" is not a generally recognized term. In the U.S., the IoT is viewed as a natural evolution of American innovation rather than as a unique field.

The U.S. federal government focuses more on the ongoing general discussion of privacy's future in America than on the growing use and potential risks of any specific technology, including the IoT. However, in March 2013, Edith Ramirez, the newly appointed Chairwoman of the Federal Trade Commission (FTC), surprisingly designated the IoT as "one area that I'll want us to

examine" during her tenure. She commented, "there are significant and important privacy questions" associated with the proliferation of "everyday devices...capturing all sorts of information about how we behave." In April 2013, the FTC issued a call for public comments on the privacy and security implications on the IoT, due in June 2013, and scheduled a public workshop for November 2013.

The announcement is new enough that not much analysis exists about Ramirez's reasons for focusing on the IoT. However, her move could be an indication of the FTC's evolving, more aggressive stance towards privacy, a sign of a more privacy-aware culture emerging in the U.S., or a reaction to growing international interest in the IoT and trade pressure from EU's more restrictive privacy regime. Overall, though, the United States, content with its status as Internet innovation king, is still largely willing to let its entrepreneurs loose and handle possible policy and political consequences later.

The IoT and International Power Politics

The EU, China, and the United States each take distinct approaches to the opportunities and risks of the emerging IoT. The EU emphasizes the need for societal parameters on the IoT, China stresses the development of their own standards, and the United States currently relies on its traditional strength as a technological innovator.

These perspectives, however, can also be analyzed within the international context of cyber cooperation. The EU, faced with the IoT approaches of the United States and China—arguably the leading centers of technological innovation—may stand behind its social parameters and emphasis on new international governance mechanisms as a way of asserting alternative power. With such laws and institutions, economic activities involving the EU and the IoT would have to conform to EU-based standards. The EU, thus, compensates for technological disadvantages in innovation through social and governance parameters. Similarly, the United States and China are seeking to maintain or create their technical edge in new cyber technologies by encouraging unique standards regimes or more aggressive development environments.

Each governance body's attempt at dominating of the IoT demonstrates that international political competition plays a role in the decisions these governance bodies are making regarding the IoT. This geopolitical competition at such an early stage of the IoT's development could create international interoperability problems, with negative political, economic, and social consequences. How governments and societies navigate the technological and political aspects of the emergence of the IoT will determine if the IoT's benefits will be ubiquitously available or if the Internet's foray into the realm of things will be interrupted.