Ubiquity, Interrupted?
A Comparison of European, Chinese, and U.S. Governance of the Internet of Things as an Emerging Technology

Mailyn Fidler
Stanford University | B.A. Candidate Science, Technology, and Society
Honors Program | Political Science & Computer Science Focuses
mfidler@stanford.edu | 812.219.6749

Introduction

The European Union (EU) is a center of Internet of Things (IoT) innovation and serves as a convening point for the global IoT community. The EU is also a leader in establishing social parameters for technologies, such as privacy guidelines (Kesan, 2006). Currently, most IoT literature focuses on technical challenges or provides conceptual models for IoT policy and governance (Weber, 2010). Little has been published regarding the current state of IoT governance. This project analyzes the existing EU governance choices regarding IoT and identifies emerging governance trends in privacy, security, and standardization that may impact the global IoT community. The project compares European choices with Chinese and U.S. approaches to IoT. My findings include insights from interviews with over 40 IoT experts from European, Chinese, and American government, industry, and academia conducted during June through December 2012.

Global Dreams, Fragmented Reality

The EU has devoted considerable attention to IoT issues and has stated its ambition to be a leading player in the field (Weber, 2010). This project outlines the actions the EU has taken in the IoT realm starting with its investigation of RFID technologies in 2006. Despite these investments, the IoT in Europe is not emerging as the global infrastructure for the information society the EU desires (Smith, 2012). Rather, current and planned governance choices are creating a fragmented, sector-based system that may impede the growth of the socially-conscious IoT the EU envisions and may weaken its connections with the global IoT effort.

Analyzing Current EU Approaches to IoT Governance

This project analyzes the strengths and weaknesses of suggested governance schemes relating to IoT privacy, security, and technical issues. European privacy approaches to IoT are fragmented between 1) technology-specific communications/recommendations, and 2) broader legislation, including the data protection directive and its pending upgrade to a regulation. This fragmentation creates distributed and uncertain guidance. The EU calls for better IoT security technologies, such as light cryptography, but little real progress has been made to bridge the gap between policy makers and IoT innovators. Third, the EU has focused more on privacy and security than on technical issues, such as standardization. This difference in emphasis results in uneven progress across IoT governance, broadening the gap between policy expectations and technological realities and undermining the EU's desire to be the global IoT leader.

Analyzing Governance Trends

The project compares the EU's governance strengths and weaknesses to Chinese and U.S. approaches, including the Chinese emphasis on IoT standards and IoT's role in the emerging privacy debate in the U.S. Through this comparison, this project 1) identifies emerging governance approaches that may soon affect emerging technologies around the world, such as technology-neutral legislation, principles-based regulation, and accountability, and 2) presents arguments informed by the IoT case study for and against the use of these approaches as governance mechanisms for emerging information infrastructures.

Works Cited

Kesan, J.P., & Gallo, A.A. "Why are the United States and the European Union failing to Regulate the Internet efficiently? Going Beyond the Bottom-up and Top-down Alternatives." *European Journal of Law and Economy* 21 (2006): 237-266.

Weber, R.H. *Internet of Things: Legal Perspectives*. Springer 2010.

Smith, Ian G, ed. *The Internet of Things 2012: New Horizons.* Halifax, UK: Platinum Print, 2012.