Network Perspectives on Privacy and Security in the Internet of Things: From Actor-Network Theory to Social Network Analysis

Yotam Shmargad
University of Arizona
yotam@email.arizona.edu

Abstract

Increasingly, everyday objects are equipped with sensors and processing capabilities. We are quickly approaching a world where objects "communicate" with us and each other, storing and sharing information about our actions and those of other objects. In this paper, I develop a framework to analyze the implications for privacy and security in these emerging "social" networks, which now include objects as nodes. Building on existing network theories and methods, I show how mapping out the information flows between consumers, devices, companies, and hackers can help to address concerns about the relationship between surveillers and the surveilled.

Introduction

Actor-network theory (or ANT), rather than a theory, is a set of tools and practices that give objects equal weight in social analysis (Law 2008). If we want to understand, for example, how the Portuguese reached India in the 15th century, we must consider the boats that were used in addition to the people who sailed in them (Law 1986). This approach highlights the importance of scrutinizing the "background," or context, of a situation or phenomenon. Understanding people is never enough according to ANT, because people are *always* situated in particular settings, which have their own unique characteristics and effects. By leaving out aspects of the backdrop to human actions and relations, we necessarily only have part of the story.

As the philosopher Graham Harman points out, the call to scrutinize the background is also found in Marshall McLuhan's now renowned quip, "the medium is the message" (Harman 2013). To McLuhan, analyzing the media that are used for communication is more important than understanding the specific content being communicated (McLuhan 1964). Knowledge about whether people are staring at their own personal screens (e.g. through their smart phones) or at the same screen (e.g. by watching television) is crucial to understanding what they are doing, even if they are watching the same show. With the advent of driverless cars, "smart" homes, and the Internet of Things, where everyday objects store and process information, the background increasingly *is* the medium.

For Harman, an object-oriented ontologist, objects have always been "smart" (Harman 2009). Moreover, they have usually been so in ways undetectable to humans. As objects are equipped with sensors and processing capabilities, what changes then is perhaps a better ability for humans to *scrutinize* their communications. This change is significant, because there are privacy and security concerns when information collected by everyday objects is made accessible. Such concerns are typically viewed from the perspective of institutional "surveillers" – the companies and hackers that can access the data (Crawford 2014).

In addition to concerns over "institutional" privacy, this paper also acknowledges threats that are closer to "social" privacy in their effects (Raynes-Goldie 2010), except with objects as voyeurs. I argue that, when we know objects are smart, we can become self-conscious of our actions independently of whether or not we think a human is watching. Timothy Morton, another object-oriented ontologist, calls objects "strange" because they are not completely knowable (Morton 2012). According to Morton, these "strange strangers" become even stranger as we get to know them. They may become stranger still as we learn more about what they know about us.

How Networks Shape Privacy

In his study of personal networks in Malta, Jeremy Boissevain relates the amount of privacy people have in their social environments to the underlying structure of their social networks:

> "people in the village… know too much about each other to be able to maintain the minimal distance – another term perhaps for privacy – necessary if close relations are to persist. Through their highly interconnected networks, villagers are always tugging at each other… because of the intimate contact (Boissevain 1974, p. 144)."

When networks are highly interconnected, or "dense", privacy is limited because people are readily informed about each other's actions. Anything said between two people quickly reaches other village residents. When objects are smart, collecting information about us and sharing it with each other, households become small villages. We can capture the extent of privacy in a networked household by studying its underlying structure.

Figure 1 shows how privacy varies with the connectivity of a connected household. Connections between objects reflect information transfer, both intentional (i.e. planned by humans) and not. On the left-hand side is a dense network, where all connections between objects exist. Privacy increases as a network gets more "sparse", in that information transfer between objects decreases. As is clear from the figure, centralized systems fall in between dense and sparse networks. By hacking a single device in a centralized system, information about other connected devices becomes available. However, unlike in a dense network, not any device has this vulnerability.

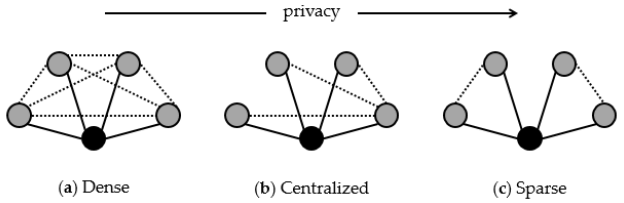

Figure 1. Extent of privacy in a) densely, b) centrally, and c) sparsely connected households. Black and grey circles represent people and objects, while solid and dashed lines represent person-object and object-object relations, respectively.

We can generalize this model in several ways. First, we can make connections between objects "directed" to be more precise about the directions in which information flows. Second, the nodes and edges may have "attributes" that capture certain characteristics about them. For example, we may want to acknowledge how sensitive the nature of data captured by certain nodes are or the ease with which certain edges can be intercepted. Third, in addition to mapping out relations between objects, we may also want to model their relations to those with access to the data they collect. Figure 2 depicts networks that model both the surveilled (i.e. those generating the data) and the "surveillers" (i.e. those with access to the data).

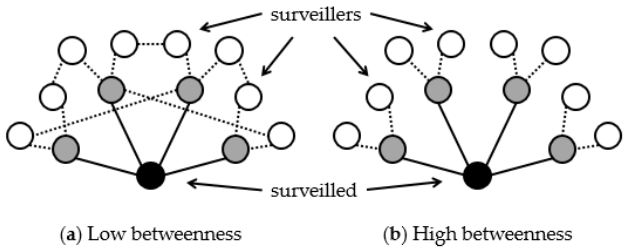

Figure 2. Networks of surveilled households and surveillers with a) low and b) high betweenness centrality. Solid lines represent surveilled-object relations while dashed lines represent object-surveiller and surveiller-surveiller relations.

When surveillers have connections to multiple objects, or to surveillers of other objects, they can get a more complete picture of the surveilled though the data they collect and aggregate. Privacy and security concerns will thus be elevated in such settings. The extent that a household is in such a highly surveilled environment can be captured with a network measure known as "betweenness centrality." Betweenness was originally constructed to measure "control" over information flows (Freeman 1977), so that we might expect households with limited surveillance to have high betweenness. Indeed, this is evident from the two networks in Figure 2. In the left network, many surveillers sit "in between" objects, implying that the household's betweenness centrality is low. The household depicted in the right network, on the other hand, is uniquely positioned between objects, so that its centrality is high.

Conclusion

The network modeling framework just described illuminates several possible interventions that can make it more difficult for surveillers to gather data about the surveilled. First, information flows between objects can be interrupted by limiting their sensing or processing capabilities. Second, relations between surveillers and objects can be interrupted. This can take the form of, for example, ensuring that different companies monitor the various appliances. Finally, information flows between surveillers can be interrupted. Prohibiting data sharing across surveillers ensures that the variety of data sources available to a single surveiller is minimized. By modeling the networks of information flows between people and things, the framework can allow researchers to study privacy and security over time and across households. This is increasingly pertinent as things become more intimate with us and each other.

References

Boissevain, Jeremy. " Friends of Friends: Networks, Manipulators and Coalitions, Oxford: Basil Blackwell, 1974.

Crawford, Kate. "The Anxieties of Big Data." The New Inquiry, May 30, 2014, http://thenewinquiry.com/essays/the-anxieties-of-big-data/.

Freeman, Linton C. "A Set of Measures of Centrality Based on Betweenness." Sociometry, 1977: 35-41.

Harman, Graham. "Everything is Not Connected." In Bells and Whistles: More Speculative Realism. Edited by Harman, Graham. Zero Books, 2013.

Law, John. "Actor Network Theory and Material Semiotics." In The New Blackwell Companion to Social Theory. Edited by Turner, Bryan S. Oxford: Blackwell, 2008, pp. 141-158.

Law, John. "On the Methods of Long Distance Control: Vessels, Navigation, and the Portuguese Route to India." In Power, Action and Belief. Edited by Law, John. London: Routledge & Kegan Paul, 1986, pp. 234-263.

McLuhan, Marshall. Understanding Media: The Extensions of Man, Cambridge: MIT Press, 1964.

Morton, Timothy. " The Ecological Thought, Cambridge: Harvard University Press, 2012.

Raynes-Goldie, Kate. "Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook." First Monday