Research Methods Sketch Essay - Privacy in Context

Matt Adair

s3204584

Introduction

My thesis research refers to a scenario in which an internet-of-things (IoT) device transmits inaudible near ultra-high frequency sound that is picked up by a mobile phone. The phone is running an application with a background process designed to respond to this signal by initiating an internet connection and sending personally identifiable information (PII) to a webserver. An IoT device is thought of as being a small electronic device with sensory capabilities and is connected to the internet. The device can then be combined with another object for the purpose of adding extra functions to it. So, for instance, a kettle becomes a water boiling device that is connected to the internet so that it can generate and send data about itself and its environment to either the owner's phone or to the manufacturer's web service.

A key element in this scenario are the IoT beacons which are unique not only in their technical capabilities but in allowing "themselves to vanish into the background" (Weiser 94).

These hidden beacons and their associated networked processing systems are designed to perform so that together "they can anticipate human needs based on information collected about their context" (International Telecommunications Union 21). My project and exegesis will use this scenario as the basis of an investigation that examines the key processes and technologies involved as well as a reflection on the problem of privacy within this context.

To form an understanding of how this research can progress from a technical implementation to an academic reflection I will need a suitable method to generate and consider responses. Specific sections of my research will be examined in this essay that deal with the concept of privacy. Initially it was thought that my research would only be concerned with the particular context of IoT beacons and how privacy concerns may arise from it. But as my research progressed, it became apparent and necessary to investigate other contexts that may help inform how my research can consider these issues.

Common Themes

One of the major areas of research for my thesis is the concept and definition of privacy within technologically mediated communications. My research has focussed primarily on the analysies of academics, theorists, commentators and the legal professions within the European Union and the United States. These two locales have their own historical and cultural contexts that inform ideas and opinions formed around privacy, it's definition and use. For example the EU may be influenced by its desire to amalgamate into a single unified economic union from a "people of dissimilar backgrounds and cultural assumptions" (Bostrom 49). The US on the other hand, has a rich history of legislating and protecting privacy not only via constitutional law but also via key court cases such as *Katz v. United States*.

The context of technology involving computers, data collection and storage has been the impetus for several implementations of privacy laws. These laws, such as the *Privacy Act of 1974,* were direct responses to concerns raised by academics and the wider community. However, according to some research, privacy is increasingly infringed and eroded indirectly and legal protection against these privacy violations cannot be codified effectively by current law. In order to investigate this, policy research has considered not just the "collection and usage practices" but also the "basic values that are challenged by the changes brought by a networked society" (Fischer-Hübner, *et al* 6) in which the historical division between public and private may no longer be relevant.

By contrast to such research that demonstrates concern, some of the loudest oppositional voices to any perceived privacy violations are the opinions of Eric Schmidt and Mark Zuckerberg. The business model of the two companies they represent rely on the ability to gather personally identifiable information of their users. Responses such as "maybe you shouldn’t be doing it in the first place" ("Google CEO On Privacy") and "privacy was no longer a social norm" (Johnson) reflect the interests of those who stand to benefit from the progressive erosion of privacy. Given the popularity of the services offered by these two companies it must be acknowledged that the user may not be concerned about privacy in this context. A further consideration is that these same CEOs have also given expression to the idea that people are prepared to relinquish some of their privacy and that they show a "willingness to engage in their own exploitation" (Baym 2) for the chance of some beneficial return.

Issues and Questions

A crucial first step in my research is to develop a coherent definition of privacy. This definition necessarily arises in the "context not only of place, but of politics, convention, and cultural expectation" (Nissenbaum 137). Each of these contexts can be either "sweepingly defined" or "finely drawn" (137) and this broad range may influence how privacy is understood. From here Nissenbaum offers a jurisprudential analysis of the historical context in which the "public and private define a dichotomy" that has "proven useful in legal and political inquiry" (137). However, an observation of human behaviour has demonstrated that we are "not only crossing dichotomies, but moving about, into, and out of a plurality of distinct realms" (137). To determine a theory of privacy therefore requires an acknowledgement that the dynamic ways in which people interact may not suit neatly definable categories.

If we cannot simply refer to a clear and definable private sphere to provide a definition then it may prove useful to consider privacy from the perspective of the individual and the context in which they feel that it has been violated. Nissenbaum uses data mining and Radio Frequency Identification (RFID) tags, as examples of "public surveillance" (119). So far, developing a legal response to this has been hampered as "traditional theoretical insights fail to clarify the sources of their controversial nature" (119). Even without tangible policy being enacted, most research into this area suggests that there is a need to "articulate a justificatory framework for addressing the problem of public surveillance" (123).

Research into the impact of privacy incursions via surveillance, especially post-Snowden documents, has demonstrated that surveillance "significantly chills one's willingness to publicly disclose" (Stoycheff 1). This withdrawal has the potential to "pose a threat to democratic discourse" especially if an individual feels that they have "unpopular political beliefs" (2). Stoycheff analyses a recent internet based survey, in which only "57%" of respondants believed surveillance in this manner to be unacceptable. Notwithstanding the 43% who reported being unconcerned, surveillance, according to Stoycheff, remains important in "influencing conformist behaviour" (2). The idea that "public opinion is the opinion which can be voiced in public without fear of sanctions" (Noelle-Neumann 44) may seem far removed from an environment containing IoT sensors. However, technology can enable surveillance and it is the intention of my research to investigate whether the IoT is performing such a role by generating data that is utilised by either government or corporate actors to identify people and their characteristics. At the centre of this is the notion that there is an inherent conflict between the individual desiring privacy and the larger entities attempting or succeeding to infringe upon it.

Concerns around privacy are not just exclusive to the individual: there is a growing awareness of privacy issues and the need for a regulatory response by industry. Given that IoT devices "increasingly detect and share observations about us", industry is becoming eager to respond to the community desire for "appropriate security and privacy protections" (FTC Staff Report 55). This response would, presumably, have to balance the concerns of the individual and the commercial imperatives of a nascent industry. Commercial benefits are a consideration when the propagation of IoT devices are expected to provide for vast economic growth via the estimated "25 billion connected devices" (1). Commercial considerations may also explain the latest response from the US Federal Trade Comission which announced that "legislation aimed specifically at the IoT at this stage would be premature" (49).

A further complication arises when policy-makers seek to legislate based on a perceived need for privacy protections while normative behaviour in the wider community suggests otherwise. Consumers are complicit in privacy infringements when they use consumer-targeted technology that enables surveillance, tracking and observation. From the seemingly innocent baby monitor to the *quantifiedself.com* movement, we have actively sought out and engaged with technology that has enabled a "tolerance for watching and being watched, measuring and being measured" (Levy 79). Our participation in this is something that can "reshape our relationships across multiple domains of daily life" and this can incur additional "complex implications for privacy" (74).

Further Research

There are several concepts that have been revealed during the current phase of my research that require either a more in depth reading or a broader and more generalised study. This investigation has encouraged me to consider the different contexts technology can produce and how they may force us to rethink established social and legal norms around privacy. I have also become aware of a fundamental contradiction at the heart of contemporary privacy debates: that consumers often tacitly, if not explicitly, consent to privacy incursions thus undermining the very concept of privacy itself. The arrival of the IoT environment means that we can no longer simply avoid privacy invading technologies, they surround us. The contexts of their implementations are multiple and the subsequent responses from society are varied.My research requires consideration of this wide range of perspectives and responses in both the definition of privacy and its usage by various actors within technologically-mediated communications. The contrasting nature of these responses is one that goes beyond a simple application of context and may require, for example, a more philosophical analysis.

One future aspect of my research may involve an attempt to determine the difference between the definition of an individual's privacy and the concept of a right to privacy. Privacy for the individual might be understood as something tacit, often only apparent in a response to something external. When personal information is published on the internet without our consent we may conclude that this is a privacy incursion. Prior to this we may be unaware that an incursion is possible and undesireable.

Another potential area of further research is the relevancy of privacy today. Primarily, this is visible in social media networks (ie: Facebook, Instagram, Twitter, etc.) where the users of a given platform provide content from their private lives for public display. This active participation reveals a significant shift: what may have once been considered to be the sanctity of the private realm is now a public commodity. Further research will explore the role of IoT devices in the public environment in the context of this new paradigm.

Implementation in Research

Defining the problem domain is one of the key stages that will determine the direction of my future research. Developing an understanding of the theoretical context as well as the implementation specifics is an important step in assembling a vocabulary of terms, definitions and meanings. This vocabulary will provide a framework through which to think about the problem itself. A key example of this is Nissenbaum's use of contextual integrity.

Within the body of research I have investigated, several articles have demonstrated the use of a descriptive analogy such as economic sociology (Levy 74), or curtilage (Ferguson 162). By utilising other theories it is possible to deepen an understanding of a problem by transplanting it into a different disciplinary field. This broadening may occur because of various new connections that are made between elements within the problem and responses from the theory.

Some of the research articles I have used have demonstrated new methods to explore concerns around issues of privacy. Some offer an historical approach which examine relevant histories for key terms and defintions in order to suggest scenarios where a particular defintion of privacy can be contested. This method of defintion and application is useful not only in demonstrating the relevancy of a particular definition but also by placing it within its context of use, it can provide a deeper understanding of what the definition is trying to articulate. The application of critical analysis in such a way is vital to my research into how privacy can be considered in an IoT environment.

Another key area that I am interested in pursuing is the intersection of surveillance and privacy via specific technology. For example, are the responses to privacy in areas such as social media also applicable to the IoT environment? The former sees people willfully and knowingly merge their offline and online identities in order to particpate in social relations. The latter inverts this relationship by positioning online devices in the offline environment that seek to communicate with us and our mobile phones. As IoT devices are propagated through the physical environment we are left to consider what course of action might be possible for those wishing to avoid this type of surveillance. And whether our ability to contest their use is possible if we wish to retain an ability to particpate in public life.

Works Cited

Baym, Nancy K. “Social Media and the Struggle for Society.” *Social Media + Society* 1.1 (2015): 720-23. Print.

Bostrom, Nick, and Anders Sandberg. *The Future of Identity.* Faculty of Philosophy: Oxford University, 2011. Print.

Ferguson, Andrew Guthrie. “The Internet of Things and the Fourth Amendment of Effects.” *California Law Review* 4.101 (2016): 101-76. Print.

FTC Staff Report. *Internet of Things: Privacy and Security in a Connected World*. Washington: FTC, 2015. Print

"Google CEO On Privacy". *Huffington Post.com*. TheHuffingtonPost.com, 18 Mar. 2010. Web.

International Telecommunications Union. *The Internet of Things*. Geneva: ITU, 2005. Print.

Johnson, Bobbie. "Privacy no longer a social norm, says Facebook founder". *The Guardian.com*.

Guardian News and Media Limited. 11 Jan. 2010. Web.

Katz v. United States. 389 U.S. 347. Supreme Court of the United States. 1967. Print.

Levy, Karen EC. “Relational Big Data.” *Stanford Law Review Online* 66 (2013): 73-79. Print.

Nissenbaum, Helen. “Privacy as Contextual Integrity.” *Washington Law Review* 79 (2004): 119-57. Print.

Noelle-Neumann, Elisabeth. “The Spiral of Silence a Theory of Public Opinion.” J*ournal of Communication* 24.2 (1974): 43–51. Print.

United States. Cong. Senate. *Privacy Act of 1974*. 5 USC Sec. 552a. S. 3418. 1974. Print.

Weiser, Mark. “The Computer for the 21st Century.” *Scientific American* 265.3 (1991): 94-104. Print.