ICPE2013
The 5th International Conference on
Information Capital, Property, & Ethics
Tsurumi University

Submitted on: October 30, 2013

The Internet of Things: Privacy, Security, and Legal Challenges

John N. Gathegi
School of Information, University of South Florida, Tampa, USA.
jgathegi@usf.edu

Abstract:

The Internet is an essential backbone that allows the creation of a ubiquitous digital environment, enabling various multimedia to work seamlessly together. Already, a trend in Internet-connectivity of non-traditional devices is emerging, creating a world of new intelligence around us, the so-called ambient intelligence or the "Internet of Things". The Internet of Things suggests major challenges in, among other areas, privacy, security, and the law. This paper focuses on the likely impact of the Internet of Things in these areas, and concludes that the notions of privacy, security, and even the law are going to be stretched considerably in attempting to meet the challenges spawned by this new environment.

Keywords: Privacy, Security, Legal, Internet of Things

Introduction

Advances in communication technologies, computing, and computer programming has facilitated the creation of a ubiquitous digital environment that allows various multimedia to work seamlessly together. The Internet is an essential backbone that allows this digital environment to become a reality. We are already beginning to see a trend in Internet-connectivity of non-traditional devices, creating a world of new intelligence around us (Gathegi, 2013). The "Internet of Things" is a not-so-new phrase that is re-emerging for how common devices are now enabled to connect to a data network, a concept described as inter-device internetworking (Gershenfeld, Krikorian, and Cohen, 2004).

Medaglia and Serbanati (2010), Kortuem et al., (2010), and Kopetz (2011) describe the Internet of Things as based on the idea of creating "smart objects" by embedding technology (such as enhanced-intelligence Radio Frequency Identification, or RFID) in physical things and then connecting them to the Internet, effectively creating a connection between physical and virtual objects (Medaglia and Serbanati, 2010). These smart objects are not only activity-aware in terms of understanding the world around them in relation to activity streams and events, they can also be policy-aware in terms of interpreting activities and events in relation to pre-defined organizational policies (Kortuem et al. 2010). Other terms that have been used to convey essentially the same idea are “ambient intelligence,” “ubiquitous or pervasive computing,” “ubiquitous networking,” or “invisible computing” (Wright et al., 2010). For the purposes of this paper, we will use the term Internet of Things because, while the other terms can sometimes be used in very specific ways, we want to make sure our meaning is broad rather than narrow.

Bandyopadhyay and Sen (2011) view Internet of Things as a world where physical objects are connected to enable them to be active participants on the Internet in terms of exchanging information about them and their surroundings. Thus, the essence of the Internet of Things is integration of disparate technologies such as embedded sensors, near-field communications (NFC) and real-time localization with communications solutions, applied to both physical and virtual worlds. This has impacts on such varied areas as transport and logistics, healthcare, smart home and business environments, as well as personal and social domains (Atzori, Iera, and Morabito, 2010).

Our focus in this paper is the impact implication of the Internet of Things in three major areas: privacy, security, and legal. While privacy and security are related in many ways, we look at privacy as the notion that individuals have some degree of control over the dissemination of their information. Thus, the fact that the interconnectedness of devices means an increase in the ways people are reachable, whether voluntarily or involuntarily, has implications both for loss of privacy and attendant security risks. Atzori et al. (2010) note that while most issues of privacy on the Internet arise out of users interacting actively with the Internet, those issues will arise with passive or no involvement in the Internet of Things environment. Kranz, Holleis, and Schmidt (2010) similarly point out some problem areas with the widespread use of smart objects in the Internet of Things environment.

In the Internet of Things environment, many devices will be able to communicate with each other and make decisions without human intervention (stopping a car before an accident, for example). However, not all such decisions will be harmless. The challenge then will be to fix legal liability for decisions automated systems make that cause harm to humans or other systems. But because of the global nature of the networked environment, a further challenge will be at what level to fix such legal liability. Weber and Weber (2010) argue that the Internet of Things is much too important to be left unregulated, but that international agreements will be hard to come by, because most Internet of Things users are private businesses and individuals. However, problems with the regulation/non-regulation of the current Internet environment continue to vex policy makers, academics, and Internet professionals.

One of the remarkable features of the convergence of media technologies is that it has spawned a ‘remix culture.’ This may be in no small way attributable to the ease with which material can be copied, used, mixed, transformed, and recast. Many digital natives have come to expect that they will be able to take content from the web and manipulate it to suit their needs, often completely unaware of the rights issues involved. In the Internet of Things, corporations will be drawn into the remix culture, as it will often be necessary to combine different sources of data from different smart objects to make relevant decisions.

In this context, current copyright law will be stretched. The protection of software will come up against the protection of content, and the major challenges will arise in the attempts to protect multi-format, multi-media content and accessories or artefacts. If everything is communicating with everything else in the Internet of Things, the problem of identifying rights holders will intensify.

This paper examines these issues through a short survey of the state-of-the-art literature on the Internet of Things and legal analysis.

Privacy

Privacy is a hard concept to define, since it can be fairly relative to the starting vantage point. However, there is generally some sort of consensus that individuals should have meaningful control over their personal information. Europe is somewhat ahead of the United States in addressing and legislating on issues of the individual's ability to control personal information held by others. The European Union issued a directive as early as 1995 that protects individuals with regard to the processing of personal data held by third parties. However, most of the rules established by the directive were aimed at known third parties, to regulate their behaviour regarding the processing of personal data in their possession. In the Internet of Things, personal data can be held by systems that are not under the control of a single entity. Your fridge, for instance can hold personal data about you, as well as share it with your grocer, your power company, the fridge manufacturer, as well as other devices in and outside your house. The European Union approach would thus be very difficult, if not impossible, to implement in that kind of environment, and even there the EU in 2013 voted for new regulations to replace the directive that will have to wait for adoption by member states (Raywood, 2013).

The United States' approach to personal data privacy is to let the market self-regulate. Of course there are some exceptions, especially in areas such as medical, education, and credit information which have regulations specifically addressing the handling of personal information by third parties. Also, the touchstone of privacy in the United States is the notion of "expectation of privacy." If there is no reasonable expectation of privacy in a given situation, the individual is unlikely to prevail on a claim of invasion of privacy. Thus, in the world of the Internet of Things, where everything is connected to everything else, and where everything is constantly collecting and sharing personal data among devices, the notion of expectation of privacy begins to lose currency.

One of the vexing characteristic of the Internet of Things is that an individual does not need to actively interact with a device for it to collect data about the individual. Sensors, for example, can track an individual's movement from the moment she wakes up from the bed to the moment she arrives at the office, all during the day, and all during the night. In this scenario, loss of privacy becomes a real concern. Specifically, the fact that one cannot easily (if at all) disconnect from the data-gathering system becomes alarming. Already, with the wide use of mobile computing and phone, we seem to have a lost, to a large degree, the ability to be unreachable. If we can be reached involuntarily, our data can be captured involuntarily. Recent reports of wide-scale international surveillance among friends and foe serve to highlight the trajectory of the impending privacy problems.

The chief characteristic of the Internet of Things is that most (if not all) objects around us will be smart objects, that is, they are able to sense, collect and process data, and communicate amongst themselves. One of the complex problems is that the user may not always know when she is face to face with a smart object, and that there is an interaction going on. Whether the use of smart object is explicit or implicit makes a big difference (Kranz et al., 2010). In the former, the user is aware she is dealing with a smart object and is doing so to achieve some goal. In the latter, while the user may be aware that there are smart objects around, she may not be aware that there is specific data interaction going on between her and the specific object she is using, and is simply concentrating on using the object as a tool. This has prodded some scholars to advocate the proposition that not only should users be able to identify specific smart objects and the interactions going on, the smart objects should be able to identify specific users to avoid dealing with the wrong user (Sarma and Girao, 2009).

Security

Information security and privacy go hand in hand. Threats in the one area spill over to threats in the other. There are many areas of vulnerability in the Internet of Things that are a result of the characteristics of this environment. There are three such characteristics according to Atzori et al. (2010): components are often unattended which makes it easier to attack physically; most communication is wireless which makes eavesdropping possible; and most components are passive, low energy use, low computing resources, making it difficult to implement complex security solutions. The good news is that researchers are already at work trying to address some of these vulnerabilities (Weber and Weber, 2010).

Legal

That the law lags technology is a truism not worth belabouring. This is no less true in the context of the Internet of Things. One area of concern is the ability of the smart objects to communicate with each other and make autonomous decisions devoid of human intervention. Some of these decisions may even be so important that they save lives, but others may be quite harmful. The question of fixing liability for harmful decisions becomes complex where many smart objects in diverse places have played a role in the decision. Also, in the case of geographically dispersed objects, the problem of establishing jurisdiction might also loom large.

Suggestions have been made on the need for international and national laws to deal with the challenges brought about by the Internet of Things. Weber (2010) suggests that there is need for such legislation in three areas: users right to know that data is being collected, and the type of data being collected; certain areas where data collection is prohibited as a matter of social policy, for example, the prohibition on data-transmitting sensor-embedded beds or shower rooms); and minimum requirements for information technology security systems that protect consumer data.

Like privacy discussed above, the United States current model for legislation in this area is industry self-regulation. Europe, on the other hand, would like a more proactive approach. This situation is not helped by the current divergent views of regulation in the Internet of Things: those who think that it is much too important to be left unregulated on the one hand,

and those who think the Internet of Things is much too important to be regulated (Weber and Weber, 2010).

Other areas presenting legal challenges in the Internet of Things include the field of contracts and intellectual property. Peppet (2012), for example, is of the view that the notion that there is asymmetrical information between consumers and sellers who offer standard form contracts may be less applicable in the Internet of Things world where the consumer potentially can have all the information she needs, suggesting perhaps that the courts will more willing to enforce consumer form contracts as written.

In the intellectual property area, the fact that objects and devices are constantly communicating with other objects and devices will make it even more difficult than it is now to identify all the rights holders. This is complicated by the fact that there has been a noticeable rise in the so-called “remix culture” brought about mainly by the meeting of young digital natives and converging media technologies. Young digital natives often have intellectual property values that are often at variance with the existing intellectual property laws.

The idea/expression dichotomy in copyright law will also get foggier. This is because smart objects will not only be able to synthesize information (as in big data) and come up with new ideas (not protected by copyright), but will also be able to express those ideas in new ways (protected by copyright). This also has implications for the concept of Author. We will have to address tough questions of who an author is, whether a smart object is a new type of corporate author, what creation and publication means among smart objects, and perhaps even what it means to have protection for the life of the author plus 70 years.

REFERENCES

Atzori, L., Iera, A and Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805.

Bandyopadhyay D. and Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), 49-69.

Gathegi, J. (2013). Technology, convergence, and the Internet of Things in Diehl, S. and Karmasin, M. (Eds.). Media and convergence management. New York: Springer.

Gershenfeld, N., Krikorian, R. and Cohen, D. (2004). The Internet of Things: Scientific American, 291(4), 76-81.

Kopetz, H. (2011). Real-time systems: Design principles for distributed embedded applications. 307 Real-Time Systems Series. Doi:10.1007/978-1-4419-8237-7_13.

Kortuem, G. et al., (2010). Smart objects as building blocks for the Internet of Things. IEEE Inyternet Computing, 14(1), 44-51. Doi:10.1109/MIC.2009.143.

Kranz, M., Holleis, P., and Schmidt, A. (2010). Embedded interaction: Interacting with the Internet of Things. IEEE Internet Computing, 14(2), 46-53. Doi:10.1109/MIC.2009.141.

Medaglia, C. and Serbanati, A. (2010). An overview of privacy and security issues in the Internet of Things. In. Giusto, D. (Ed.), The Internet of Things: 20th Tyrrhenian workshop on digital communications. New York: Springer doi:10.1007/978-1-4419—1674-7_38.

Peppet, S. (2012). Freedom of contract in an augmented reality: The case of consumer contracts. UCLA Law Review. 59, 676-745.

Raywood, D. (2013). EU votes in data protection directive more than doubling potential fines. International Business Times. October 23, 2013.
http://www.ibtimes.co.uk/articles/516305/20131023/eu-data-protection-directive-approved-raising-fines.htm

Sarma, A. and Girao, J. (2009). Identities in the future Internet of Things. Wireless Personal Communications, 49(3), 353-363.

Weber, R. (2010). Internet of Things—New security and privacy challenges. Computer Law and Security review, 26(1), 23-30.

Weber, R.H. and Weber, R. (2010). Internet of Things: Legal perspectives. London: Springer.

Wright, D. et al. (Eds.) (2010). Safeguards in a world of ambient intelligence. New York: Springer.