Issues in Information Systems
Volume 17, Issue IV, pp. 145-151, 2016

THE INTERNET OF THINGS: A CAUSE FOR ETHICAL CONCERN

Kyle Ebersold, The Hartford, Bryant University, kyle.ebersold@gmail.com
Richard Glass, Bryant University, rglass@bryant.edu

ABSTRACT

The Internet of Things (IoT) can be broadly defined as a global network infrastructure, linking uniquely identified physical and virtual objects, things and devices through the exploitation of data capture (sensing), communication and actuation capabilities. The control of objects in this highly integrated manner provides for effective uses in numerous applications, however the trend toward greater interconnectedness and more massive amounts of data raises many questions in the field of information ethics. This paper introduces a number of critical social issues pertaining to the IoT. In particular, this paper focuses on the threats to privacy and key governance issues that will need to be addressed to protect the privacy of individuals.

Key words: The Internet of Things, Information Ethics, Privacy, Governance

INTRODUCTION

The Internet is a nearly 50 petabyte data repository created by massive numbers of entries by individuals who either typed on a keyboard, pressed a button on a mouse or other device, took a picture, scanned a bar code, or otherwise performed a human interaction with a machine. Google CEO Eric Schmidt has pointed out that approximately every two days we now create as much information as we did from the dawn of civilization up until 2003 (Schmidt,2010). In spite of its impressive size, the Internet lacks the ability to connect back to the real-world in the direct way machine-to-machine (M2M) technology can. With the spread of the IoT and its ability to enable M2M communication, the amount of new information that will be created will dwarf the amount of data that is currently being produced on the internet.

The IoT can be broadly defined as a global network infrastructure, linking uniquely identified physical and virtual objects, things and devices through the exploitation of data capture (sensing), communication and actuation capabilities (Wikipedia, 2016). A primary goal of interconnecting devices is to create situation awareness and enable applications, machines, and human users to better understand their surrounding environments. The understanding of a situation, or context, potentially enables services and applications to make intelligent decisions and to respond to the dynamics of their environments (Barnaghi et. al., 2005). The IoT takes advantage of radio-frequency identification (RFID) and sensor technology that integrate extensively with our physical environment collecting and transmitting information across a computer network (Downes, 2013). With the IoT, the Internet is evolving into a more dynamic and integrated entity that provides for effective human-to-human (H2H), human-to-thing (H2T), and machine-to-machine (M2M)) interactions. IDC estimates that as of the end of 2013, there were 9.1 billion IoT units installed. IDC expects the installed base of IoT units to grow at a 17.5% CAGR over the forecast period to 28.1 billion in 2020 (IDC, 2015). The result is an explosion of information exceeding the current size of the internet by several times. Cisco predicts that the IoT will generate as much as 400 zettabytes (ZB) of data a year by 2018 (Cisco, 2016).

The control of objects in this highly integrated manner provides for effective uses in numerous applications for the home, personal use, work environments, and public sector applications such waste management, urban planning, sustainable urban environment, continuous care, emergency response, intelligent shopping, smart product management, smart meters, smart grid, and other smart events. However, this trend toward greater interconnectedness and more massive amounts of data raises many questions in the field of information ethics. For example the European Group on Ethics in Science and New Technologies asserts that IoT will bring a radical change

to the control that humans have over their environment by providing interconnected autonomous objects the ability to communicate with each other and take actions that impact the lives of individuals without those individuals being involved in the process (Freeman and Peace, 2005). The large increase in personal information that will become available, the potential loss of control over the information and types of actions that the IoT may initiate autonomously raises significant ethical issues related to autonomy of things and humans, privacy, security, freedom, liberty, equity, equality, justice, fairness, access, discrimination and others. The potential impact of the IoT on society should not be underestimated. The purpose of this paper is to bring to the attention of researchers and practitioners key ethical issues related to IoT with a focus on privacy and governance strategies that may be used to address the risks associated with the IoT.

INFORMATION ETHICS AND THE INTERNET OF THINGS

Information ethics is the branch of ethics that focuses on the relationship between the creation, organization, dissemination, and use of information, including the ethical standards and moral codes that govern human conduct in society. Areas of interest in terms of information ethics include privacy, moral agency, environmental issues and behaviors and problems arising from the information life-cycle. It stands on the edge of the fields of computer ethics and philosophy of information.

Jeroen Van Den Hoven, a member of the Ethics IoT Subgroup of the European Commission, Delft University of Technology highlights specific ethical concerns related to the IoT (Wachtel, 2012):

1. **Ubiquity and pervasiveness**. The user is engulfed and immersed by IoT and there are no clear ways of opting out of a fully-fledged IoT, except for a retreat into a pristine natural and artifactless environment, which will be hard to come by in the remainder of the 21st century.
2. **Miniaturization and invisibility**. The desk top computer as we know it will gradually disappear or will stop to serve as the paradigm case of a computing device. Computing technology will become translucent and has the tendency to disappear from human sight. So although the functionality is prominent and ubiquitous, it will for a good part be inconspicuous or invisible. This calls for special design measures to make the technology visible and amenable to inspection, audit, quality control and accountability procedures.
3. **Ambiguity and ontology**. The distinctions between natural objects, artefacts and human beings tends to blur as a result of the facile transformation of entities of one type into the other by means of tagging, engineering and absorption into a networks of artefacts. We will have to deal both practically and conceptually with ambiguous criteria of identity and system boundaries.
4. **Identification**: Electronic identity of things and objects achieved by tagging and networking of objects. We will have to get used to the fact that – apart from special and cherished objects and artifacts, many more and seemingly insignificant objects and artifacts will have unique identities. This feature is crucial for the idea of IoT. Who gets to assign, administrate and manage these identities, will access to them and to what they entail in a globalizing world is a non-trivial governance issue.
5. **Connectivity**: High and unprecedented degree of connectivity between objects and persons in networks. High degree of production and transfer of data.
6. **Mediation and autonomous agency**: The IoT environment provides ways of extending and augmenting human agency, even to the point that it may exhibit artificial and spontaneous and emerging agency. IoT environments may present spontaneous interventions in the course of human events which are not directly caused by human agents or operators and which are unforeseen and unexpected. Human beings will act in IoT environments together and in concert with artefacts, devices and systems, thus constituting hybrid systems.
7. **Embedded intelligence and extended mind**: Smart and dynamic objects, with emergent behaviour, embedding intelligence and knowledge function as tools and become (external) extension to the human body and mind. As is already the case to a certain extent with traditional computing artifacts, access the intelligent and data carrying IoT environment may come to be considered as necessary for human agents to get around. Similar to the info available through a mobile phone, and access to your Social Networking Site, people would feel cognitively and socially handicapped.

8. **Seamless transfer**: Interaction, information flow with IoT context will be effortless, with potentially very low transaction and information cost.
9. **Distributed control**: The locus of control and governance of IoT will not be a central one, because of its vast amount of nodes, hubs and data. It will see emergent properties and phenomena, and will have to be governed and monitored in ways adequate for its distributed nature. This has implications for the locus of accountability.
10. **Big Data**: IoT is the locus of tremendous data generation, storage and flow and processing at Exabyte level and beyond.
11. **Unpredictability and uncertainty**: Incremental development of IoT will lead to emerging behaviours without the user having full or even relevant knowledge of the IoT environment.

PRIVACY

Privacy, in the authors' opinion, is the most contentious ethical concern surrounding the Internet of Things. A key issue arises from the nature of the technology itself. To protect privacy, individuals should be able to provide informed consent regarding the information shared by IoT devices and the actions that these devices originate. However, the design of the IoT is predicated on the ability to use "smart" technology to make autonomous decisions and execute them in microseconds. Control in a world of numerous interconnected machines constantly talking to each other and observing the real-world environment will have a much different meaning than it does in terms of today's Internet devices. A critical impediment to the IoT development would result if users must give explicit permission for devices to function as intended. In order for the IoT to function, the locus of control must shift from the user to connected devices on the IoT (Wachtel, 2015). In a world where the promised interconnectivity through the IoT involves billions of smart human and non-human objects and transactions, consent may become an absurd concept (Curvelo, et al. 2014).

While large amounts of data was difficult to relate to individuals in the past, data collected from the physical world has currently become more and more relatable, and both regulators and the public pay increased attention to the protection of privacy and private data (Baldini et. al, 2016). Critical emphasis must be given to well-designed data protection at the design stage so that profiling is performed correctly and opportunities for corruption are as limited as possible. Data re-purposing (contextual integrity) should also be carefully monitored as large amounts of data may become deanonymized or repersonalized as the availability of so many data sets may create opportunities of data convergence that would defeat anonymity. Moreover, the enormous amounts of data present ethical issues in terms of harm prevention, equality, and moral autonomy.

A related privacy issue is the potential for an individual to develop a feeling of loss of control over one's life that arises from the IoT's ability to transfer decisions that impact an individual's life to devices and algorithms and take action on those decision without the awareness of the individual while at the same time creating data that is largely invisible to the public. When the intentionality of delegated actions is not fully controllable by the user, this may lead to a compromise in a person's integrity and eventually that person's freedom (Van Den hoven, 2014).

IoT expression may occur through multiple "smart" technology solutions such as smart building control and energy systems, smart transportation options, and the smart grid. Privacy is about control—how you control data about yourself and your habits, and how businesses and other entities control that information as well. It is not just the amount of information that creates privacy challenges, but also about the insights that can be generated from sensors and information technologies. Outside of healthcare organizations and electronic medical records, government regulations are scarce around privacy. Business and others need to carefully consider how information collected by smart devices could be used for purposes that infringe on freedom in some way. For example, authoritarian governments could use information collected by smart cards to track and locate dissidents. In another application, smart building energy systems may open the door for surveillance applications by outside entities (SmartPlanet, 2014).

As IoT solutions are developed, people may get stuck in a monopolistic or oligopolistic service provider structure. If existing cellular networks are engaged in activities that would connect IoT infrastructure to the Internet, this

would likely increase the power of existing providers to supply their services at a higher cost to the customer. In health applications, IoT devices may directly increase health risks in a situation of failure. An Internet-connected pacemaker, for example, opens the door to many questions such as the security of such an essential life-support device and the amount of trust people may have in using it.

The terminology of "right to privacy" possesses intrinsic problems in itself because in American law it is a term with many different aspects and no universal meaning. In terms of physical and bodily integrity, most constitutional rights prevent against governmental invasion of the home or of reproductive activities. Personal data generated in the ordinary course of human activity, such as records of financial dealings, creditworthiness, social security identification, and medical history, generally is also protected. But privacy rights in terms of ubiquitous IoT technology are much more obscure. How data is collected and used in the world of new interactions created by the IoT have no stated privacy rights as of now—only ideas and beliefs. In some cases, privacy is ethically incoherent—pointing in several different directions and adopting disparate models to assign responsibility and control for data representations. Unstated rights of privacy currently tend toward treating personal data representations as constitutive of individuals with potential to treat them as information entities (Burk, 2008).

Moreover, rights to privacy are socially constructed (Berger and Luckman, 1991) meaning that they change over time as the influences of many human forces and institutions shifts, including those relating to technology, culture, and law. Rights and views to privacy include:

1. **Freedom**—the right to conceal our behavior protects us from punishment, discrimination, ostracism, and criticism. Individual liberty weakens if privacy diminishes freedom.
2. **Property rights**—should a "consumer profile" or "public profile" be considered property that cannot be used unless chosen by the owner to be sold about themselves?
3. **Informed consent**—the idea that we should not do things to others without their permission has a long history. This has important consequences for data collection without informed consent of a person being monitored.
4. **Personality development**—we need opportunities for private reflection and experimentation if we are to develop complex personalities. We must be able to try out attitudes and values in private so that we can reject them later without being permanently viewed and held to everything we have said and done in the past as they change. Individual consumer tailoring also freezes interest, preferences, and activities as they have been and disallows the opportunity for change in these areas to take place.
5. **Avoidance of discrimination**—protecting privacy prevents powerful people and entities from acquiring prejudicial information in the first place.
6. **Avoidance of defamation**—we should avoid false statements and groundless criticisms of others.
7. **Happiness**—generally, we think it is right to make people as happy as possible. Human beings usually seem happier when they have a zone of privacy—a chance for solitude.
8. **Equality of power**—Knowing information about people is a source of power. Protecting the rights of ordinary people to withhold information strengthens them against governments and large firms.
9. **Separation of zones**—many people believe that it is important to keep society carefully divided into zones such as the market, the family, the military, religion, politics, scholarship, and social relationships. Zones are distinguished by rules and expectations regarding privacy.
10. **Rights of association**—legal and moral rights exist to associate in voluntary groups. To "associate" is to share information only within the organizations that one joins. If information can be bought, the result could be a weakening of associations.

Privacy also can be influenced by individuals and companies acting in a marketplace, parents when they set norms for their children, professionals when they establish rules of conduct for their peers, and software designers when they invent technology that either protects or erodes privacy (Levine, 2003). It is also important to note to that Generation Y doesn't have the same idea of privacy as older generations (SmartPlanet, 2014). Given all of these unique concerns and different views, where should privacy land in each of these spheres?

Governance Issues

At the 10th Meeting of The Internet of Things Expert Group in Brussels, a number of governance issues were presented for consideration (Van Den Hoven, 2014). These included:

1. Should governance be administered using an Internet platform, or are new platforms required?
2. Should IoT-specific legislation be required to govern privacy and security?
3. Should IoT legislation be a soft (non-binding) legislation or something more stringent?

No consensus exists on whether existing governmental bodies or new ones should govern IoT. As a result, no specific actions on policy are currently proposed as they are considered premature at this time. However, three major views have been observed to exist in terms of legal legislation relating to IoT technology (Wachtel, 2012).

1. Legislation is believed to potentially introduce considerable burdens and quickly become obsolete. IoT-specific legislation is, therefore, not suitable for consideration.
2. There is no one-size-fits-all prescription for privacy by default. Therefore, even general legislation is not suitable for consideration.
3. No decision on legislation or similar can be made at this time. More time is needed for further consideration.

As policy is developed, it should strive to maintain several objectives (Van Den Hoven, 2014).

1. **Policy should avoid the emergence of social injustice.** IoT assumes the societal divide between those who have and do not have access to Internet technology is a null factor. In truth, much debate still exists around the importance of this divide as it also creates a knowledge divide which separates those who have knowledge to master the new technology from those who are dependent on experts. Many argue that fair access to IoT technology and qualification of the citizens to use it, as well as alternatives for those who voluntarily do not want to engage with IoT, be included in the design of the new technology.
2. **Establish trust in the IoT.** Design of IoT devices and architecture must support users' ability to trust IoT. Effective technical functioning, protection of personal data, and ensured privacy and usable security management should all be included.
3. **Ensure the adequateness of IoT metaphors.** Researchers and industry must fairly represent IoT through metaphors that not only highlight its conveniences, but also its dangers. Metaphors used in discourse framing must also keep up with the development of the technology to ensure dissemination of the most accurate information as it advances.
4. **Creating a social contract between people and objects.** By using things in the IoT, people must delegate actions to objects. The actions being taken should be those actually intended by the user, and should not be deceptive in any way. Algorithms used may also be blind toward special needs of individuals, and these procedures must consider moral implications as they are designed and used.
5. **Allow for informed consent.** It is highly important in privacy scenarios for contemporary information technology that persons being exposed to the technology be informed that they are interacting with it in some way. Focus must emphasize making otherwise invisible IoT technology visible to those interacting with it for inspection purposes.

When governmental authorities do initiate efforts in terms of legislation surrounding IoT, it will be difficult to silo such decisions as the IoT is a global phenomenon. Based on current efforts, Europe appears most likely to be the first adopters of any such legislation. Other foreign actors would then have to follow suit.

In terms of organizations and ethically sound IoT technological advancement, those establishments most likely to adopt IoT technology in an ethically agreeable manner are most likely organic rather than mechanistic in culture and environment. In a 2007 empirical study conducted on information technology professionals' perceived organizational values and managerial ethics, organic organizations were defined as openly collaborate, creative, encouraging, sociable, relationship-oriented, equitable, empowering, and trusting. This is also the assumed norm for a democratic society. Mechanistic organizations were the other form under consideration, and were defined as cautious, task-oriented, rigidly structured, and maintained hierarchical values oriented toward centralization, pressure, power, and procedures. This form is generally regarded as more bureaucratic. The key finding of the

study was that moral reflection by employees tends to decrease as centralization (frequented by bureaucratic or mechanistic organizations) increases (Jin et. al., 2007). Mechanistic organizations are therefore most likely to desire IoT technology applied in a manner opposite that of the general public compared to organic organizations.

Freeman and Peace (2005) make the point that our privacy is less protected now than ever before. The speed at which technology is evolving and the continual growth in its ability to gather and make use of personal information outstrips the ability of governmental agencies to develop applicable laws in a timely manner to ensure that intellectual property rights and privacy are protected in today's society. While information ethics in relation to IoT is the current subject of a very heated and multi-directional debate, one agreed upon matter does exist with great certainty is that a debate on the future values of living is necessary (Van den hoven, 2014). Without such crucial discussion, the IoT will arrive and affect our lives in highly intricate ways without regard for important privacy considerations and basic human values.

REFERENCES

Baldini, G., Botterman, M., Neisse, R. et al. Sci Eng Ethics (2016). doi:10.1007/s11948-016-9754-5

Barnaghi, P., Wang, W., Henson, C. and Taylor, K. (2012). Semantics for the Internet of Things: early progress and back to the future. *International Journal on Semantic Web & Information Systems*, *8* (1), 1-21

Berger, P. L., & Luckmann, T. (1991). *The social construction of reality: A treatise in the sociology of knowledge* (No. 10). Penguin UK.

Burk, D. L. "Information Ethics and the Law of Data Representations." Ethics and Information Technology 10.2-3 (2008): 135-47. ProQuest. Web. 22 Apr. 2014.

Cisco. (2014). Fourth Annual Global Cloud Index Study: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html?CAMPAIGN=GCI+2014&COUNTRY_SITE=us&POSITION=PR&REFERRING_SITE=PR&CREATIVE=PR+to+GCI+WP

Curvelo P. et al. (2014). The constitution of the hybrid world: EU Scientific & political report. *Publications Office of the European Union.*

Downes, L. (2013). "The Five Most Disruptive Technologies at CES 2013." *Forbes Magazine*, 12 Jan. 2013. Web. 22 Apr. 2014. <http://www.forbes.com/sites/larrydownes/2013/01/12/the-five-most-disruptive-technologies-at-ces-2013/2/>.W

Freeman, L., and Peace A. (2005). Information Ethics: Privacy and Intellectual Property. *Information Management 17* (31). ProQuest. Web. 22 Apr. 2014.

Frohmann, B. (2008). "Subjectivity and Information Ethics." *Journal of the American Society for Information Science and Technology 59*(2), 267. ProQuest. Web. 22 Apr. 2014.

IDC, (2015) Internet of Things: http://www.idc.com/downloads/idc_market_in_a_minute_iot_infographic.pd

Jin, K. G., Drozdenko, R. and Bassett, R.. Information Technology Professionals' Perceived Organizational Values and Managerial Ethics: An Empirical Study. *Journal of Business Ethics 7* (2), 149-59. Levine, Peter. "Information

Schmidt, E. (2010): http://techcrunch.com/2010/08/04/schmidt-data/

SmartPlanet (2014). Internet of Things Demands Rethinking of Business Ethics. *SmartPlanet. CBS Interactive, n.d.* <http%3A%2F%2Fwww.smartplanet.com%2Fblog%2Fbusiness-brains%2Finternet-of-8216things-demands-rethink-of-business-ethics%2F11435>.

Van Den Hoven, J. (2014). Ethics and The Internet of Things. *European Commission. Delft University of Technology, n.d.* <http%3A%2F%2Fec.europa.eu%2Ftransparency%2Fregexpert%2Findex.cfm%3Fdo%3DgroupDetail.groupDetailDoc%26id%3D7607%26no%3D4>.

Van Den Hoven, J. (2014). Fact Sheet - Ethics Subgroup IoT - Version 4.0. *European Commission. Delft University of Technology, n.d.* <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDwQFjAA&url=http%3A%2F%2Fec.europa.eu%2Finformation_society%2Fnewsroom%2Fcf%2Fdae%2Fdocument.cfm%3Fdoc_id%3D1751&ei=30lUUqnkMcep4APxwIGwDA&usg=AFQjCNG_VgeaUP_DIJVwSiPIww3bC9Ug_w&sig2=DEVquzOFpQWwjhMud5bXIg&bvm=bv.53537100,d.dmg>.

Wachtel, T (2012). IoT Expert Group Final Meeting Report. *European Commission. European Commission, 14 Nov. 2012*. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=1747>.

Wikipedia (2016). Internet of Things. Available at: http://en.wikipedia.org/wiki/Internet_of_things