Guidelines for Internet of Things deployment approaches –
The Thing Commandments

Edewede Oriwoh*, Paul Sant, Gregory Epiphaniou

Department of Computer Science and Technology
University of Bedfordshire
Luton, United Kingdom

Abstract

The Internet of Things (IoT) describes the interconnection of objects (or Things) for various purposes including identification, communication, sensing, and data collection. “Things” in this context range from traditional computing devices like Personal Computers (PC) to general household objects embedded with capabilities for sensing and/or communication through the use of technologies such as Radio Frequency Identification (RFID). This conceptual paper, from a philosophical viewpoint, introduces an initial set of guiding principles - also referred to in the paper as commandments - that can be applied by all the stakeholders involved in the IoT during its introduction, deployment and thereafter.

© 2013 The Authors. Published by Elsevier B.V.
Selection and peer-review under responsibility of Elhadi M. Shakshuki

Keywords: Internet of Things; Security; Commandments; Principles; Users

1. Introduction

The phrase “Internet of Things” was coined by Kevin Ashton [1] in 1999. Although the concept of interconnecting devices and people for various reasons has existed for much longer - i.e. via the traditional Internet and social networks - this model of interconnecting devices, people and everything else is relatively new and still in its introductory stages [2]. Control over these devices will be spread over a spectrum of stakeholders: owners, manufacturers, law enforcement, and participatory governments. This

*Corresponding author. Tel.: +447791415757.
E-mail address: edewede.oriwoh@beds.ac.uk.
control can be expected to take various forms; from “direct-touch” (physical) control to remote control or control via web browsers and the Internet. In addition to these is the prospect of ‘proxy control’ or ‘sequential actions’ (Table 1) i.e. a situation where a Thing causes an action in another Thing; for instance, a user’s alarm clock ringing causing their bed to vibrate in order to coax the user into getting up in the morning (see Figure 1).

Table 1. The 3 ways by which Things can be controlled

<table>
<thead>
<tr>
<th>Methods of controlling Things</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Direct Touch</strong> - for instance, by flicking a switch to turn on the Kettle: Do A</td>
</tr>
<tr>
<td><strong>Remote Control</strong> - via the Web, PCs, mobile phones, tablets:</td>
</tr>
<tr>
<td>Send an instruction to the Kettle to Do A</td>
</tr>
<tr>
<td><strong>Learned action:</strong></td>
</tr>
<tr>
<td>e.g. a Thing tells itself - “Because it is 6am, I will do A”</td>
</tr>
</tbody>
</table>

Fig. 1. A series of triggered actions

There are already beneficial applications of interconnecting objects in an IoT in areas like emergency management, logistics, and medicine [3], [4], [5]. However, on-going research has exposed some privacy risks which have led us to ask some questions which we consider pertinent. For instance, how can the owners of Things be accurately identified? How do we know when a Thing (as opposed to a person) has done something wrong? Who is to blame for a Thing doing something wrong e.g. for committing a crime? What should a society’s expectations be of its government in relation to Things like sensors being deployed or the expectations by neighbours of their neighbours? Should neighbours always inform each other about the presence of sensors outside their homes? When is it permissible not to inform anyone about the presence of sensors? Also, who is supposed to have control and what is the acceptable amount of control various stakeholders should (or shouldn’t) have over certain Things?

We therefore conclude that there is a requirement for a set of principles that can guide the deployment and use of Things as they become part of the ubiquitous mesh of connected devices used every day in society. This paper is a positioning paper rather than a technical document; it is written from a philosophical viewpoint of the IoT whilst simultaneously providing a springboard from which future streams of technical, implementation-focused research may take off.

The rest of this paper is organised as follows: part 2 presents relevant work within the domain of IoT-related rights and responsibilities; part 3 is a discussion around various concerns about IoT technologies thereby highlighting the need for principles that guide the design, manufacture, procurement, ownership, management, governance and disposal of these technologies; part 4 introduces the contribution of this
paper, “The Thing Commandments” which have as their focus the rights and responsibilities of all the IoT stakeholders; part 5 discusses some further work and part 6 concludes the paper.

2. Related work

2.1. The RFID Bill of Rights

Simson Garfinkel [6] contended that there should be a set of recognised rights of individuals in relation to the proliferation of RFIDs and tagged items. He proposed five (5) RFID Rights which he called ‘Guiding Principles’. The Principles cover, among other things, individuals’ rights to know about the presence of RFID tags, what information is held on the tags and the right to have these tags removed.

However, whilst the Principles cover the rights of individuals with respect to RFID tags, we suggest that there should be recognition by all IoT stakeholders of their rights and responsibilities in relation to obtaining, owning/possessing, deploying and managing Things.

2.2. IoT-related Security and Privacy needs

Rolf, in [7] introduced a discussion about security and privacy needs with regards to the IoT. The discussion includes suggestions for using Privacy Enhancing technologies (PET) to increase security and privacy in RFID based systems like the IoT. In addition, a legal course of action is discussed and the European Commission’s (EC) Privacy Impact Assessment (PIA) [8] is introduced. This PIA was set up by the EC in response to its consciousness of the security and privacy issues related to the RFID and IoT.

Lastly, Rolf identified a set of requirements for meeting security and privacy needs in relation to the IoT and these are Resilience to attacks, Data authentication, Access Control and Client Privacy. The author concludes these requirements would have to be included into the risk management concept governing the general business activities of private enterprises that use IoT technology. This discussion was first introduced by [9] as part of a discussion around Distributed Object Naming System (ONS) – a system for locating information sources in RFID tag-based networks - and its impact on privacy.

2.3. The European Commission’s Privacy Impact Framework

The European Commission (EC) in 2011 came out with a Privacy and Data Protection PIA. The PIA is designed to serve as a guide for the design and operation of RFID applications including the IoT. Contributions were invited from the Commission’s Member States after which the PIA was drawn up.

This system of using this PIA places a large proportion of the responsibility for determining the risk to security and privacy on the organisation that plans to deploy an RFID application. However, our recommendations are more necessary than optional.

2.4. Communication Services - Rights of Users and Providers

The paper by [10] presents a discussion about the rights of users and providers of communication services. Two examples of these rights are the right to connect any legal device to a communications network (as long as the device causes no damage to the network) and the right of service providers to charge for the communications services that they provide.

In our work we cover discussions about individual, corporate and government rights, freedoms and responsibilities as well as discussions about policies and the legal system in relation to the IoT.
introducing the proposed commandments, we deem it necessary to present some concerns with respect to the deployment of the IoT. These include concerns about security, the legal system, accountability, control, etc., and they are briefly discussed next.

3. Existing and Envisaged IoT-related Concerns

3.1. Legal issues

New cybercrimes are typically triggered as new technologies are developed and unveiled. This can also be expected with the IoT [11]. The Law, for its part, tends to lag behind these crimes; indeed according to [12], by its very nature, Criminal law lags behind technology and this legal time lag is inevitable because of the inability of state and federal statutes to keep up with Internet developments. Also, Rolf H Weber in [13] and [2] manifests that there is a need for governance and legal oversight over how the IoT operates even now while it is at its early (formative) stages. As identified by [14], because of the far-reaching applications of the IoT in national and private systems, the legal and policy discussions around the IoT should be dealt with as important for its development. It is therefore important that the legal arm of society is better prepared and even contributes to the development of the IoT by setting guiding principles that stakeholders would be expected to adhere to. The governments and lawmakers should be ready and willing to modify existing laws or create new ones, in order to safeguard citizens from the dangers of mismanaged or hacked tag systems. For instance, in order to deal with some aspects of cybercrime, the UK government deemed it necessary to introduce the Computer Misuse Act in 1990 [15] although certain other cybercrime-related charges are still being brought under laws that already existed such as the Theft Act 1968 [16]. This can serve as a good precedent for dealing with IoT-related crime.

3.2. Concerns about Accountability, Liability, Rights and Responsibility

The number of devices connected to the Internet is expected to reach 50 billion by 2020 [17]. This proliferation of connected devices would definitely create some control concerns for governments and privacy concerns for citizens. Introducing discussions on rights and responsibilities at the development phase of the IoT is pertinent and is what our work aims to do.

As an example of responsibilities, governments might be expected to indicate clearly to their citizens (e.g. through the use of signs) where they have deployed tags in public places (see Figure 2 for an example notice in a pool in a public park).

3.3. Concerns about Trust

Some concerns about trust include those expressed in [18] where the authors identify concerns that deployed RFID systems could encourage widespread surveillance of members of the public without their knowledge or consent. They also argue that data produced by the system might be re-used for a second purpose also without the consent of those whose data was collected.
3.4. Regulation and Control concerns

There are a number of questions around regulation and control over the IoT. Questions like who, if any one body should control the IoT? Is it to be self-regulated or government controlled? Should there be a body governing the IoT? For management and marketing purposes, it may be deemed necessary to introduce a system for storing records of all tagged (or IoT-enabled) objects. This is similar to the system where customers who purchase contract (mobile) phones and lines are registered on to the provider’s database. If a system like this is introduced and customers’ details are collected as part of the purchase process, then access to these records would have to be strictly controlled.

3.5. Privacy concerns

There are already concerns about the deployment of devices that can be communicated with over IoT-enabling technologies like RFID. The US started solely issuing the new e-Passports to its citizens since August 2007. This passport has an integrated RFID chip embedded into the back page of the passport; the chip digitally holds relevant information about the passport assignee for security reasons [19]. When grouped according to their source of power, RFID tags can be active, semi-active, or passive and they can be awakened and read by RF readers at adequate distances from them - some from distances of several meters [18]. However, the research to determine the best way to secure this communication link (i.e. indiscriminate awakening and reading of tag data by just any reader) is still on-going and has not yet produced a widely accepted result. Therefore, although RFID is beneficial since its design enables automatic and time-saving identification, the benefits of being automatically identified may not outweigh the potential disadvantages for an individual. Also, the time-saving benefits of being able to identify the contents of a traveller’s suitcase by scanning and reading all the tags attached to each item - without the requirement of opening the suitcase - will not eliminate the fact that erroneously tagged items could be allowed through a border checkpoint.

In addition, [20] highlights tracking as a problem with the use of tags arguing that the identifiers provided by tags - which are usually predictable - can make it possible for associations to easily be established between tags and their owners. The same paper argued that privacy is one of the issues that are still to be addressed before a major roll-out of RFID systems.

Given the existing issues around the deployment of the IoT, we introduce some suggested commandments that might address them. Some of them may come across as obvious whilst others may be points of contention and probably encourage meaningful debate.
In order for this work to reflect currently applicable reality, some assumptions were made in drawing up the commandments and they are pointed out at this point in the paper. It is assumed that before these principles can be adopted:

1. Interoperability has been achieved between various vendors’ devices and there is a common set of protocol(s) being used to enable communication and interoperability between Things. Also, IoT and WoT Standards have been agreed upon – [21] posits that technical protocols have now been standardized to acceptable levels.

2. It is contended by [22] that security and privacy, as well as regulations and social concerns need to be investigated and properly addressed in order to encourage the acceptance and adoption of the IoT by society. They also identify 4 facets for consideration in order for security and privacy concerns to be adequately addressed: 1) Socio-ethnic, 2) Legislation/Regulation, 3) Economical Market and 4) Technologies concerns. This paper assumes that society has largely accepted that these spimes ([23], [24]) are now part of everyday human life - or, at least, that society is willing to work, live with and accept them.

3. Some governments and major corporations and various companies have identified various reasons to spy on their citizens and employees using various methods – some such methods are highlighted in [25] hence driving the need to introduce guiding principles that governments would be expected to be aware of and be guided by.

The aim of this paper is to introduce a set of principles that can be applied to this “ThingNet” (InterNetwork of Things) - so that even as devices are being manufactured and tagged and/or embedded with identification, communication and sensing technology and capabilities, the long-term recognition of the implication of having an intelligent “Thing” as opposed to an ordinary thing, is recognised by the stakeholders including the manufacturers, the consumers and the governments in places where Things exist and are being used.

The recognition that objects are becoming connected and interconnected [26], [27] and the recognition that there is a need for an overarching set of principles, has fed the drive to introduce the “Thing Commandments” which should hopefully serve as a starting point and feed into discussions around the privacy, security, rights and responsibilities of the public, governments and vendors when it comes to the IoT and all connected Things. If there are no guiding principles, there is a potential for the rights of governments, vendors and individuals to be stretched too far or even, conversely, for their responsibilities to be diminished.

4. The Thing Commandments

In this section we present the proposed commandments.

Your Thing is your Thing. This commandment argues that Things belong to, and are the responsibility of, their owners and, by inference, so are the actions of Things. So, for instance, if an owner, say Osas, did not send a specific request to a Thing to carry out a specific action, say, for example, to “Open the front door” (a direct and immediate action A) or even a derived action e.g. do ‘A’ if ‘B’ happens else do ‘D’ (i.e. based on what it has learned), then Osas cannot assume that any negative action that his Thing carries out will be excused without expecting any form of reproach to himself as the owner. This way, if a crime involves a Thing, the owner, identifiable by a label on or, incorporated in the Thing, bears some responsibility for the “actions of the Thing.”
Also, because of how easy it may be by design for Things to be accessible by unauthorised (but somehow authenticated) users, it does not mean that successful unauthorised access is permitted. There is an analogy in wireless networking: just because a Wireless Access Point (WAP) is not adequately secured by an owner, breaching it (e.g. by piggy-backing) by a skilled person is NOT automatically acceptable.

Illegal access: If anybody or entity accesses or controls any Thing without the permission of the owners, such access must be regarded as illegal. [28] presents an excellent argument on how the new applications of RFID technology in transponders can introduce privacy risks. They contend that the objects that are permanently embedded with transponders could be used by individuals in public places where they may have little or no control over who can access them. The UK Computer Misuse Act (CMA) 1990 was introduced to deal with crimes that involve, among other things, unauthorised access to computer systems and, RFID tags and sensors, although they might have little computing capability, are by extension, computing equipment and this law can be extended to include them.

Your Thing should have a relationship with all your other Things: All Things that belong to a particular person should belong to a Thing Network and be easily and uniquely identifiable to each other and by each other. The aim of this “trust” relationship is to enable security by ensuring that rogue Things attempting to become part of a someone’s Personal ThingNet (PTn) - analogous to the Personal Area Network in traditional networking - would be denied access because establishing that relationship would require certain criteria to be met. These criteria can be based on a system of Authentication, Authorisation and Accountability (AAA) and may incorporate existing AAA solutions. Although [29] argues conversely that NO device (i.e. tagged) should be fully trusted by another in order to avoid the situation where every single device stands as a single point of entry to a network, we argue that this trust relationship, is essential for Things to be able to identify and verify the identification [30] of each other. In order for this relationship to be established, a strong but manageable system of authentication and authorisation would have to be put in place.

Your Things should be able to identify communication between each other by the use of an established method: This way only trusted communication would be permitted between Things. Therefore, any unauthorised “imposter” Thing that tries to communicate with an established network would be detected and such communication would not be allowed.

Usability and ease of use: It should be made relatively easy for users to configure Things and add new Things to or remove old Things from their ThingNet. If a user purchases a new Thing and wants to ensure it can communicate with their existing Things and vice versa, the user should be able to do so easily without having a special training or requiring the services of the specialist vendor. Vendors should be
required to make Things as pluggable and playable as possible. This commandment would ensure that vendors don’t make unreasonable amounts of profit from providing unnecessary Thing-related services to their consumers since some consumers would obviously start out by being “Thing luddites”. This commandment is especially relevant to Thing designers, developers and vendors. It is supported by the assertion in [31] that homeowners must be able to get devices on to their home networks by themselves without any assistance from “installers”. The rights of individuals have to be recognised even as these Things are being designed and deployed. The technology in the back-end and frontend has to be designed with the end users’ access needs and requirements in mind.

**All Things should be controllable by their owners:** It should be expected that all Things should be under complete or at least partial (shared) control of their owners. To meet this requirement, vendors and developers should ensure that all available technology in relation to Things is designed to be user accessible and user friendly as well as easily understandable. Rigorous tests and consumer surveys must be carried out to ensure that consumers are not just aware that they should be able to control their Things but that this is a requirement for owning Things.

**Every Thing must have an owner:** The owner must be clearly identifiable by some form of identification on, around or hard coded in the Thing. For instance, Things can be affixed with a sign that states they are the ‘Property of the Government of country X’. Any “Thing” with no identifiable owner belongs to no one and can legally be confiscated or destroyed. This commandment would prove especially useful for law enforcement agencies since it would most likely be up to them to locate the owners of misplaced Things. This way, hopefully, any crime committed by a Thing can be traced to the owners. There might be the need to detect ownership by scanning a code but that code must be easy to locate by (or accessible to) law enforcement.

**All Things (must) have owners even though not all owners (must) possess Things:** This commandment incorporates and introduces a caveat to the previous commandment; it can be re-phrased as the “The Right to Freedom from tags and tagging” which ensures the freedom of people and society from tags in every form.

**Refusing, disabling and destroying or disposing of Things:** This commandment introduces the rights of individuals to refuse all or certain Things e.g. implantable tags. RFID tags are being embedded inside pets, exotic animals and people [32], [33] but this paper posits that this should only be done with the consent of the individual concerned or an appointed guardian within legal limits. It also asserts that it must be possible and easy to disable Things even remotely. This commandment also requires that these Things should be easy to dispose of and the data within them completely destroyed. Bernard in [34] argues that, as a fundamental right of citizens, the ‘silence of the chips’ must be preserved and this supports all the arguments put forward by this commandment.

5. Further work

This conceptual paper outlined a set of principles for guiding various points of contact with the IoT. Whilst we are aware that the principles are not exhaustive, they provide a foundation from which further discussion and future research may follow. Some of this future research may include the implementation of a user-managed IoT (Smart) Home forensics system that is designed and deployed in IoT-based homes to carry out regular network monitoring and basic forensic tasks on behalf of homeowners. With such a robust system, users can be assured that they will be informed of who is attempting to access Things in
their home (see 4th commandment above, things must recognise alien communication) in their absence and this will contribute to a sense of safety and security and, consequently, greater acceptance of the IoT.

6. Conclusion

Typically new technologies - and, sometimes innovative applications of existing technologies - present exciting prospects and relevant uses to which they can be applied. The importance of introducing security at the early stage of the development of any technological advancement - including the Internet of Things - is well recognised by researchers as well as in industry. There are existing laws and new ones are being enacted to guide the use of technologies new and old and to ensure that any breaches in the use of technology is detected and appropriate action is taken to reprimand the culprit(s). It is therefore deemed important that as the IoT concept buds, relevant guiding principles that can feed into laws are introduced for application to this interesting phenomenon. This is what this paper sought to do – to introduce a set of such guiding principles for consumers, vendors, law makers and governments who deal with the Internet of Things. All recommendations on these principles are welcome and encouraged.

References

2010.


