Privacy and Governance Considerations for the Internet of Things

George C. Polyzos,[*] Giannis F. Marias,[*] Nikos Fotiou,[*] Markus Fiedler,[§] Ralph Herkenhöner,[#] Hermann de Meer[#]

[*] Mobile Multimedia Laboratory, Athens University of Economics and Business, 113 62 Athens, Greece
[§] School of Computing, Blekinge Institute of Technology, 371 79 Karlskrona, Sweden
[#]University of Passau, 940 32 Passau, Germany

***Abstract*—The Internet of Things (IoT) is an emerging form of internetworking in which various real-world "objects" are interconnected. While the (IoT) opens the ground for new, innovative technologies, it raises significant privacy and governance challenges. This presentation aims at stimulating the discussion around the privacy and governance concerns in the IoT.**

I. Introduction

While the terminology "Internet of Things" (IoT) is ill defined, there is a general understanding that an "Internet of Things" means the linkage of objects (in most of the cases equipped with a Radio Frequency Identification/RFID chip) in an electronic network within an "Object Naming Service" (ONS).

The emergence of the IoT is seen as one of the key areas in the evolution towards next generation networks. The linkage of objects to networks and through them to themselves and the ability to communicate with these objects, open doors for new economic developments with great market potential and wide-ranging political, legal, and socio-economic (and in particular privacy) implications.

Research has been concentrated so far on the technical and economic aspects, in particular on the development of RFID technology, the design of an ONS and the possible commercial applications and services. But while there is a general agreement that an IoT has also far reaching political, legal, and social implications, there is only little research with regard to public policy issues such as governance and privacy with regard to the IoT and in particular the ONS service.

The purpose of this presentation is to discuss privacy and governance considerations in the IoT, as an extension of the generic discussion on the relationship between IoT and Networks of the Future presented in [1].

II. Privacy Considerations

Information in the IoT is normally linked to persons, activities, places, time and other everyday habits. It is essential to define scopes of information. Scopes will provide rules and policies for information reachability and limiting information dissemination. A private scope would define a Private Network (PN) where information is limited in that 'private' domain. A confidential scope may define access privileges on information transferred between two virtually interconnected PNs. A public scope would publish information to all (the public).

Because hard security and privacy countermeasures might be inappropriate to be used by or embedded in the 'things,' security and privacy should probably be enforced at the service level, i.e., where the ONS or DNS are used and when names and addresses are resolved and linked to everyday's habits.

Adversary models as well as mature and efficient Privacy Enhancement Technologies (PETs) related to the IoT lookup services have been addressed vaguely in the literature. More scientific and experimental work has to be done on privacy issues in ONS in order to avoid privacy threats to the service. PETs for ONS lookup service are required to achieve:

- **low latency**, since the ONS lookup needs to provide results in real-time;
- **scalability**, to fulfill the ONS lookup service's demand for scalability;
- **robustness** and reliability, since the system will need to support a very high transactions throughput.

Distributed solutions are probably best to achieve all of these three requirements.

A real challenge seems to be how to contain information disseminated that was obtained from or produced by the combination of (legally) available information from various sources (that seems inconsequential) and deduction, which might lead to the revelation of personal and potentially sensitive information. This becomes a real challenge in this environment because for the first time in human history events and information will be recorded at such large scales globally and will be tagged with time and location information, and many times in ways completely hidden to humans.

One approach to address this challenge, since limiting access to widely or publically available information is not realistic, is to consider approaches of information accountability [2].

Another challenge is dealing with location privacy in the IoT. Since every object is tagged and can be somehow identified by probing it wirelessly, location privacy is threatened in several ways. The ONS provides a naming service for objects using the Electronic Product Code (EPC) which is by its purpose a unique identifier. Thus, specific objects can easily be tracked globally by this identifier and therefore the object's possessor. Even if the EPC would be protected by using cryptography or anonymization techniques, the RFID chip it self could be identified by its "radio fingerprint"[7]. Even if we can overcome this "radio fingerprints", the probability of identifying (or at least linking local "sightings" of) a person by its combination of carried objects increases by the number of objects.

III. Governance Challenges

When it comes to governance of the IoT, we need to understand how it fits into the existing governance regimes and whether it needs a different form of governance altogether. For example, since the IoT is using the Internet addressing scheme and naming system, which is governed by ICANN, one must ask to what extent will the IoT be governed by ICANN principles. Some experts on the subject of IoT governance have gone so far as to state: Governance of the IoT will not/should not replicate the ICANN model or the ICANN debate [3], and when looking at the IoT, there is not yet sufficient evidence to let us know in what ways the governance would/should differ. One industry group, EPCGlobal [4] which has a focus on the RFID technology that makes up an integral part of the current concept of IoT, has already shown an interest in having a role in the governance of the IoT, but have not given a well-formed plan of a new governance model.

The European Commission has been concerned about the shape IoT governance will take for over one year. They have started to look into the needs for IoT governance; specifically [5], according to the European Commission, policymakers should also participate in the development of IoT alongside the private sector. Some challenges are indeed policy-related, as highlighted by the World Summit on the Information Society, which encourages IoT governance designed and exercised in a coherent manner with all the public policy activities related to Internet Governance.

Many questions concerning the implementation of the connection of objects arise, such as:

- object naming;
- the authority responsible for assigning the identifier;
- ways to find information about the object;
- how information security is ensured;
- the ethical and legal framework of the IoT;
- control mechanisms.

The European Commission also released an action plan for Europe on the IoT indicating the need for 'promoting a shared and decentralised network governance,' committing to follow *World Summit on the Information Society* (WSIS) principles in the governance of the IoT.

IV. The GOVPIMIT Project

GOVPIMIT (Governance and Privacy Implications of the Internet of Things) is a specific joint research project in the context of the NoE Euro-NF [6]. GOVPIMIT studies governance, privacy and security issues in the ONS service that support the IoT. Additionally, authentication via dynamic naming, flexible identity management for ONS in the IoT and dynamic creation of intranets are examined, since such services will enhance the security services offered by ONS beyond the DNSSEC standard. GOVPIMIT objectives can be summarized as follows:

- Integration scenarios of IoT with the Network of the Future and use case scenarios of links between IoT and the Network of the Future;
- Recommendations on policies and governance for the ONS service;
- Impact of policies and governance to ONS architecture;
- Analysis and evaluation of privacy and secure authentication and identity management.

V. Conclusion

Privacy and governance in the IoT is a multi-dimensional problem which involves various technological and socio-economics factors. The research in these areas although very active is still premature, as it has to satisfy a broad range of requirements.

References

[1] Doria, A., Fiedler, M., Herkenhöner, R., Kleinwächter, W., Marias, G.F. Marias, and Polyzos, G.C. "Governance of the Internet of Things," submitted for publication, 2010.

[2] Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., and Sussman, G.J., "Information accountability," *Commun. ACM* 51, 6, 82-87, Jun. 2008.

[3] Governance of the IoT will not/should not replicate the ICANN model or ICANN debate, http://twitter.com/bcute17/status/2189966433, accessed Dec. 2010.

[4] EPCglobal home page, http://www.epcglobalinc.org/home/ , accessed Dec. 2010.

[5] EU, Internet of Things http://europa.eu/legislation_summaries/research_innovation/research_in_support_of_other_policies/si0009_en.htm, accessed Dec. 2010.

[6] Euro-NF home page, http://euronf.enst.fr/en_accueil.html, accessed Dec. 2010.

[7] Jules, A. "RFID security and privacy: a research survey", IEEE Journal on Selected Areas in Communications, Vol. 24, Issue 2, pp. 381-394, 2006.