Smart Governance for Smart Industries

Wojciech Cellary
Poznan University of Economics
Niepodleglosci 10
61-875 Poznan, POLAND
+48618569330
cellary@kti.ue.poznan.pl

ABSTRACT

In this paper, we present a vision of smartness as an environment in which humans and devices, visible and unseen, provide a wide range of e-services trying to make a person's life easier, more comfortable and more efficient. Economic and privacy issues are discussed as the most challenging. We argue that only direct income from consumers of e-services may guarantee sustainable development of smart industries. We present threats coming from smart industries and smart governance which may abuse trust of people who are served. We indicate the triple role of smart governance: first, to become smart and avoid a smartness gap between the public and private sectors; second, to boost smart industries, while third, and simultaneously, enforcing the codes of protecting privacy.

Categories and Subject Descriptors

J.1 [**Administrative data processing**]: Business, Government; J.7 [**Computers in other systems**]: Consumer products; K.4. [**Computers and society**]: Privacy

General Terms

Management, Economics, Security, Human Factors

Keywords

Smartness; smart government; smart governance; smart industry; economy; internet of things; compute continuum; e-services; privacy; customization; trust; discrimination

1. INTRODUCTION

There is no common consensus about what "smart" really means in the context of new technologies, the information society and e-economy. Although this term has become fashionable, it is also broadly used as a synonym of almost anything considered to be modern and intelligent. In this paper we propose the following concise vision of smartness:

A servant surrounded by servants, which may be a configuration of both humans and devices, from both public and private sectors.

While the word "servant" evokes images from aristocracy to slavery, it is used in this paper with good will. In the evolving smart environment, a person or system will be surrounded by or embedded within "servant systems", which are the smart systems supporting or acting on behalf of a person or system that makes his/her/its life easier and more comfortable through its provided services.

The evolution of smart societies and economies begins with data, continues through e-services, and leads to improved quality of life. Hence, the essence of smartness is converting data into innovative e-services that help improve the quality of life.

Data are the key of smartness, because if there are no data, there are also no e-services. There are four sources of data that may feed e-services:

- Data coming from sensors and devices, e.g., cameras, deployed in the environment of people, e.g., homes, buildings, stations, streets, roads, etc., as well as coming from user oriented devices such as smart phones and wearable electronic devices;
- Data provided by individuals via social media and web/mobile applications;
- Data collected by public authorities, including open data [6];
- Data collected by private companies.

e-Services may be classified in two different and independent ways. The first classification concerns initiation of e-services. We distinguish between e-services initiated by customers and e-services initiated by providers. In the first case, a customer explicitly invokes an e-service when he/she wants it. In the second case, an e-service is initiated when an e-service provider supposes that a customer needs its service. The second classification concerns the scope of e-services. We distinguish between e-services whose scope is limited to digital world only, and e-services which join together digital and real worlds [5]. From the smartness point of view, the most promising but challenging are e-services initiated by e-service providers that join together the digital and real worlds. Such services are aligned with the emerging concept of Compute Continuum [2], encompassing notions of the Internet of Things [1] as well as mobile and wearable devices.

The Internet of Things is composed of ordinary things (or objects) with embedded sensors and actuators that enable these "things" to communicate with each other without a direct human interface or control. More conceptually, the Internet of Things is comprised of unseen device servants that surround individuals trying to make their environment comfortable and adapted to their individual needs. The Internet of Things is complemented by different mobile and wearable smart devices, such as Google Glass for example, which are visible, and remain under the direct control of their owners. Within the concept of the Compute Continuum, both visible and unseen devices may cooperate to deliver a large variety of e-services.

Key technologies that support e-services are: filtering and knowledge extraction and exploration including big data analysis. Filtering enables the acquisition of those data from a data

ICEGOV2013, October 22-25, 2013, Seoul, Korea

repository which are relevant for a particular e-service. Knowledge extraction consists of inferring facts that previously were not explicit in the data repositories. Knowledge exploration consists of discovering relationships between facts that previously were not known and rules applying to their evolution.

Another key target of e-services is the development of applications of mass customization. Mass customization of e-services permits businesses to improve their quality and better adapt their services to the precise needs of a customer in a given time and place. It is also is a way to improve business profitability, because massively customized services may generate bigger revenues. A way to achieve mass customization is modeling customer behavior, including profiling. A model of customer behavior permits the business to forecast the customer's needs and preferences and to offer him/her customized e-services in advance.

Based on the above observations, we may now present a more detailed vision of smartness:

Every person surrounded by human and device servants that know him/her very well, accurately predict his/her wishes in advance, and serve him/her in a personalized way.

Two fundamental problems with that vision of smartness are economics and privacy, which are discussed in detail in the two following sections. In Section 4 we briefly characterize the role of smart governance, while Section 5 concludes this paper.

2. ECONOMIC ISSUES

Since a person's quality of life is inherently related to his or her economic situation, smart industries must present a valid economic proposition as to their overall value in order to accomplish their mission to increase of quality of life. We often see increases in indices of the quality of life of a given society as a result of economic growth. The free market is a proven driver of economic growth. As we shift toward an e-economy, increases in the quality of life will be a result of e-economy growth. e-Economy growth means that e-services must be a part of economic activity in a free market. To contribute to the increase of the quality of life through e-economy growth, smart industries have to create jobs for human service providers. We may conclude that success of smartness will depend largely on financial models of e-services.

Currently, public e-services are financed from taxes and offered for free. The widely accepted and implemented idea is that public monies should provide for free access to public services. Commercial e-services have more complex and diversified business models. Roughly, they may be financed directly by consumers (pay-for-service e-services), may be financed by advertisers, or subsidized from taxes.

An e-service provider may of course mix the above models and may offer some services for free and finance them from the income of paid services [4]. Paid e-services create a healthy market because:

- Only useful and accepted e-services are paid for by customers;
- Competition in the market guarantees constant e-service quality improvement; and
- Valuable jobs are created especially for local young innovators.

While a paid advertising model generating income from ad hits is a very reasonable business model for big, worldwide players in the Internet, it is not so reasonable for local businesses that create most of local jobs. These smaller entities can often win grants or allocations from public sector funds to sustain them during their startup and initial phases. However, such grants typically do not provide the long term funding needed for sustainable development of small, local smart industries. Nor is it likely that small local startups will be able to attract sponsors for sufficient mass market advertising support. Only the pay-for-service e-services model provides the most real and healthy prospect of continuing funding for smaller smart industries.

3. PRIVACY

To be served in a smart way, servants have to know as much as possible about each person, while the essence of privacy is secrecy. Thus, from an individual's point of view a dilemma arises: smartness or secrecy? In other words, this dilemma may be expressed in the following way: how much should a person trust an e-service provider, taking into account the potential risk of betrayal? In business, privacy violations aim at identifying the susceptibility of a person to arguments and proposals.

We consider two cases. The first case arises when an e-service provider wants to identify as precisely as possible, and as timely as possible, the needs of a potential customer so as to serve him/her as well as possible. But, in this case, a potential violation of privacy may aim to discover the susceptibility of this potential customer to arguments for satisfying his/her need by an e-service provider. The purported desire of an e-service provider to be a perfect servant (by the way generating high income) may turn into an aggressive marketing attack which is annoying and unwanted. Still the prospective customer remains the master of this situation as he/she may accept or refuse an offer of an e-service despite arguments provided by the e-service provider.

The second case of privacy violations arises when an e-service provider aims at identifying the weaknesses of a potential customer. Knowing his/her weaknesses, an e-service provider may evaluate his/her susceptibility to arguments for accepting a worse business proposal than offered to other customers (which generates higher profit) or to exclude some customers from some business proposals to eliminate risk involved. This case should be classified as "betrayal", because a client accepts collecting and processing his/her private data believing in better service based on identification of his/her needs will be forthcoming, while he/she may actually become a victim, receiving worse service or exclusion from service based on identification of his/her weaknesses and susceptibility. Here, the customer is not in control of the situation, cannot know he/she has been denied or excluded or overcharged due to some secretive business analysis, and is, indeed, betrayed by improperly used e-data.

Smartness based on e-services coming from the compute continuum and classical e-services provided through the web is inherently replete with potential threats to privacy, such as the:

- Possibility of surveillance on a huge scale;
- Possibility of identification of people at any given point while doing any given task;
- Possibility of recording every human activity and its associated parameters that may be processed later;

- Possibility of profiling, i.e., classifying people according to different criteria basing on private data which may be incomplete or wrongly interpreted.

In general, the violation of privacy opens the possibility of influencing a person's actions via his/her environment and context using mechanisms that are essentially out of his/her control. Consequently, concerns about, and inquiries into the impacts on our human freedoms is justified.

As quickly as smartness is understood as a customized interconnected environment of servants, the question arises of one's risk of betrayal by these servants. A simple case of betrayal is selling acquired personal data to a third party. These data may be legally acquired for a given purpose that customers agreed to. But clearly, also using such data for another purpose without the customer's consent should be characterized as betrayal, even if in some countries it is still legal. A more advanced case of betrayal consists of selling conclusions derived from analyzed personal data to a third party. Such conclusions may take a form of recommendations, e.g., this potential customer is not trustworthy, exclude him/her from your business; or recommendations to worsen the conditions of a business offer to that potential customer – surmising from the usurped personal data that he/she will accept the terms anyhow due to personal circumstances. Such conclusions and recommendations provide a new basis for discriminating that may be called: analytic distrust. Personal data entrusted to a servant to receive a better service are analyzed to sell distrusts to third (and fourth?) parties, including ones leading to discrimination based on big data analytics against the person. This kind of customized discrimination will be particularly difficult to fight, because an individual customer is defenseless – moreover, probably will have no idea that analytic distrust has been sown against him.

Smartness, without trust and punishment of betrayal will be not tolerated by people. Therefore, new regulations are required to protect privacy not only against illegally acquiring private data but also against illegal processing them. A world-wide consensus is required on what private data are and which are the rules of their collection, storage, distribution, and processing.

4. THE ROLE OF SMART GOVERNANCE

The challenges to governance are threefold. First, it is necessary for governance to be smart – to apply smart technology to perform governmental tasks so as to avoid the expansion of a technology applications gap between the public and private sectors. Second, it is necessary for governance to boost smart industries, which are the most promising part of the economy of the future [3],[7]. Third, in performing both of the above functions, governments are also expected to set and enforce rules of privacy protection wherever possible through the "privacy by design" approach.

Having those rules, governments should enable a free market of data of different kinds: some general not personal, some personal but anonymized, some personal but pseudonimized, finally some personal but under strict control of the people whom they concern. Next, governments should support the establishment of a free market of e-services, both simple and compound requiring cooperation of different actors from both public and private sectors. Finally, governments should encourage smart industries to earn money from paid e-services, and to turn the profits into development and increases in the quality of life of its constituents.

5. CONCLUSIONS

Smartness is a great evolving system of interconnected smart servants that takes advantage of current information and communication technology to improve quality of people's lives. However, smartness cannot be allowed to evolve naively without considering its potential for perpetrating new threats or damages, especially ones like customized discrimination or analytic distrust. Preventing those threats and damages requires new regulations on a global scale, as smart e-services are not constrained by national borders. It is also necessary to embed smartness in local economic activity, because it is difficult to talk about the quality of life of a jobless people.

Enthusiasts think that smart e-services can change world in this century as much as electricity did in the last one. This is possible, however, only if governments will be aggressive and pro-active in setting the right rules to take advantage of smartness while preventing its threats.

6. ACKNOWLEDGMENTS

I would like to thank very much Dr. Louis E. Freund, Professor of Industrial & Systems Engineering from San José State University, San José, CA, USA for inspiring discussions and comments improving this paper, as well as for a proof that geographical distance between people exchanging thoughts is not a barrier for useful collaborations.

7. REFERENCES

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

[2] Buchholz, D. and Dunlop, J., The Future of Enterprise Computing: Preparing for the Compute Continuum. *IT@Intel White Paper*. 2011.

[3] Cordella, A., Willcocks, L., 2013. Government Policy, Public Value and IT Outsourcing: The Strategic Case of ASPIRE, *Journal of Strategic Information Systems* (to be published)

[4] Estevez, E. and Janowski, T. 2013. Electronic Governance for Sustainable Development – Conceptual Framework and State of Research, *Government Information Quarterly*, Vol. 30, Supplement 1, (Jan. 2013), Elsevier, pp. S94-S109.

[5] Issarny, V., Georgantas, N., Hachem, S., Zarras, A., Vassiliadist, P., Autili, M., Gerosa, M.A. and Hamida, A.B. 2011. Service-Oriented Middleware for the Future Internet: State of the Art and Research Directions, *Journal of Internet Services and Applications* 2 (1), pp. 23-45.

[6] Janowski, T., Pardo, T. and Davies, J. 2012. Government Information Networks – Mapping Electronic Governance Cases through Public Administration Concepts. *Government Information Quarterly*, Vol. 29, Supplement 1, (Jan. 2012), Elsevier, pp. 1-10.

[7] Johnston, E. Governance infrastructures in 2020. 2010. *Public Administration Review*, Vol. 70 Supplement 1 (Dec. 2010), pp. s122-s128.