Citizens and device identification difficulties in digital cities

Carlos Lugani, Luis Vivas, Sonia Formia
LIA - Laboratorio de Informática Aplicada – Sede Atlántica –
Universidad Nacional de Río Negro
{clugani,lvivas,sformia}@unrn.edu.ar

ABSTRACT

This paper analyses the issues in the citizens and device identification in Digital Cities or Electronic Governance. It provides factors which take part in the identification process as well as the possibility or impossibility to keep people's privacy when they carry out their activities. It is also related to the devices either for interacting with people or providing services to different cities by means of systems.

We conclude our identification vision bearing in mind that the citizens must get involved to define their privacy limitations.

KEYWORDS

Digital cities, Electronic Governance, citizens, identification, privacy

1 INTRODUCTION

In the near future there will be so many systems of human recognition that it will not be possible for a human being not to be identified by any of them. There are both public and private systems that are developed to identify people, states to control their citizens and private to identify their potential customers. However, security systems are necessary regarding public security. In digital cities the limits between public and private aspects are not clearly defined, and in some cases there is no existence of such limits. For example it is not possible to differentiate the public from the private in cases of public places such as airports, buildings, transport stations managed by companies, as well as there are differences in cases of management of a country, state or county.

Additionally, the government outsources private companies to deal with security aspects so then, the monitoring and citizen's identification is not carried out by the government.

Smart smart cities will necessarily develop ways to identify their citizens to provide services such as transportation, IoT, Sensor Networks and Real-time systems, smart homes, crowd control and surveillance through CCTV circuits.

Citizens should be involved in security issues: registry access, public services identification, participatory environments and information about registered citizens, image and video preservation over time and any other information stored by governments. As well as information security and the actors who have access to the information, people activities and registers that are stored over time. [1]

2 IDENTITIES

The identity administration in the digital society context consists in the citizen`s identification necessary to provide different services or public security purposes.

Additionally, the identity administration is expected to be spread out to devices known as the Internet of Things (IoT) and to devices interacting with people but not connecting to the Internet. There is a wide devices variety both self-managed or interconnected (e.g. cars) [2], some of them provide different services to people and others so much embedded as artificial organs, robot arms, or devices intended to help disabled people.

Therefore, there is an improvement in people's identification and also there is an improvement in the devices providing services to those people. Even though the identification process is intended to identify people, from the human point of view, there is a lack of models or problems related to:

- The way people used to identify devices,
- The device capability to identify a person.

These two situations lead to the same difficulty, the general actor's identification and if taken into account the digital city premises, this situation should be solved to assure the correct use and the citizen´s identities.

Legal factors should be considered in a base of rights of the people taking into account that countries legislations are different but trying to generate a model to be followed.

Another issue is related to the information itself, which is done with these data? where is it processed, stored, communicated, exchanged and if it is reused, concentrated or related. All the above could be processed with or without citizens knowledge.

However, there is a variety of issues related to the outline that is introduced which will be discussed in future papers in order to present situations and possible solutions to be taken into account.

2.1 Citizen`s identification

Nowadays, the state of the art has moved forward into biometric people identification devices design. Such developments led in better ways of identification reducing false rejection rate and in non-intruding identification ways such as iris recognition, because the light emitted could have a harmful effect for the eyes. Therefore, mechanisms are developed in order to identify people with images, such as facial recognition, hand geometry, or body movement's patterns. [3] [4] This identification could also be extended to animals.

2.2 Devices identification

In order to allow the digital cities creation the devices connected to the Internet will increasingly grow. Even the devices interconnect among one another to build a network, such as the ones that are used for traffic and weather systems.

In the case of such devices, it is necessary to have a safe identification in order to verify that they are the original ones and

not a fake one that may cause problems or failures in systems or deficient services.

Some examples related to personal devices are the mobile phones use, fully autonomous driving and homes connected to the Internet. [7]

In the fully autonomous driving case is important that the device stores the activities carried out, as well as informing about problems to the driver, since the information stored in vehicles could solve difficulties related to accidents

Additionally, the following situations information should be stored:

- Unlocking the devices, due to robbery attempt or interference. In these cases the device should send a signal to the user indicating the devices have not been unlocked, and for this reason it is no longer reliable or could have been duplicated, modified or deleted resulting in different consequences for the user.
- Interference or disruption in communication. This will not represent a serious issue unless these disruptions result in taking bad decisions during a journey.
- Attempts to misuse by intruders or fake users simulating to be the original ones.

There are also autonomous systems or systems network such as electricity, gas, water supply and tides control systems, etc. These systems will be increasingly interconnected to one another and with their users and in every case, it will be necessary the identity verifications existence among the parties.

2.3 Information related to citizens and devices identification management and storage

When dealing with management it is necessary to concentrate citizens, devices and systems information. One of the intelligent cities goals is to involve the citizens into the use and technology benefits. [5]

However, the access to information should be analysed considering that the different information amount over time leads to the behavioural patterns creation. For example: geolocations and services used by mobile phone and car or public transport, would be able to design a behavioural person pattern location. If this information is compared to someone else's information, it is possible to determine who the citizen has been with, for how long, where he has been, where he has gone, and the transport type he has used, leaving aside the fact of relating this information to payments or money use, included in state-of- the-art digital city.

3 RESULTS AND DISCUSSION

This paper purpose is not alarming on situations without solution, but to reach a first approach about identification citizen`s issues.

It should be taken into account the citizens identification mechanisms to be used by the government agencies and the rest of society. Considering the following topics: [6]

- Privacy,
- Identity,
- Digital identity,
- Data collection and management (including data aging)
- Identifying people apps,
- Citizen's rights.

People have no option related to personal identification carried out in public places. It is necessary to discuss if the citizens have the right to reject that its identity might be used by systems that are not strictly managed by the Government. However, this right must not take precedence over any national security control, or even the citizens might take the decision about what right is more important for them.

4 CONCLUSIONS

Presented here is an outline of potential ways data is collected on individuals, how it can be linked to identities and what types of problems this present. It was not the objective of this paper to mention existing regulations such as data protection, privacy cookie use on website, however the legislation on this matter should be analyzed when expanding this line of research.

The citizen`s participation, defining the scopes, limits, and related elements has been introduced. These topics is mainly experimental and by means of examples of use. Even though the technology available to develop digital cities and electronic governments exists, no citizen`s discussion or participation have been presented so they can get engaged in the model development that will benefit both the government and themselves.

"Participation requires citizens to be informed and engaged, and achieving this requires government to build capabilities in using appropriate tools for informing and engaging." [8] Therefore, it is essential the citizen's involvement before establishing statements and systems developments that could put at risk the privacy of people.

5 REFERENCES

[1] Yıldız M. 2012. Information Polity, vol. 17, no. 3,4, pp. 343-355 DOI: 10.3233/IP-2012-000284

[2] Milković H et al. 2016. A Real-World Implementation of IoT Automobiles. Journal of Future Computer and Communication Vol.5(6) pp. 222-228 ISSN: 2010-3751

[3] Unar J.A. et al. 2014. Pattern Recognition A review of biometric technology along with trends and prospects. Elsevier Volume 47, Issue 8, August 2014, Pages 2673-2688

[4] Iula A. et al. 2016. A Method for Biometric Recognition of Ultrasound Palmprint Based on Principal Lines. International Journal of Future Computer and Communication, Vol. 5, No. 1, pp. 13-17 doi: 10.18178/ijfcc.2016.5.1.435

[5] Fernandes, S et al. 2016. Electronic governance in Portugal: a silent pioneer. EGOSE 16 Proceedings of the International Conference on Electronic Governance and Open Society: Challenges in Eurasia. pp. 77-82 DOI 10.1145/3014087.3014108

[6] Lyon D. 2009. Identifying citizens: ID cards as surveillance. Polity Press. ISBN-13: 978-0-7456-4155-3

[7] Gubbi J. et al. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. Volume 29, Issue 7, pp. 1645-1660

[8] Cledou M. et al. 2013. ICEGOV 13 Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance, pp. 378-379 doi 10.1145/2591888.2591968