Discreet City: Protecting Privacy at Large Scale

Discreet project Technical Report – TR-2006/05/29

Georgios V. Lioudakis, Sofia Kapellaki,
Eleftherios Koutsoloukas, Nikolaos L. Dellas,
Chrysa Papagianni, Christos Katsigiannis,
George N. Prezerakos,
Dimitra I. Kaklamani and Iakovos S. Venieris

National Technical University of Athens,
School of Electrical and Computer Engineering
9 Heroon Polytechniou str.,
15773, Athens, Greece

e-mail: {gelioud, sofiak, lefterisk, ndellas, chrysa, chkatsig, prezerak}@telecom.ntua.gr,
dkaklam@mail.ntua.gr, venieris@cs.ntua.gr

Smart City,
Privacy,
Privacy Regulations,
Context aware services,
Surveillance and Monitoring Systems,
Privacy-aware middleware

Recent advances in mobile communications, location/sensing technologies and data processing are boosting the deployment of context-aware services and smart spaces creation. This is reflected in urban environments by the smart-city vision, a city with advanced ICT and surveillance infrastructures offering to citizens a diversity of services. Nevertheless, privacy risks and threats ambush, since collection and process of large amount of personal data occur. Although technology enables the collection of data, its protection against abuse is left to data protection legislation. However, privacy and security requirements, other than being general and abstract terms to be regarded as legislature issues, should be brought down in the technological reality and carefully accounted for in devising technical solutions. In order to limit the disclosure and misuse of citizens' personal data, this report introduces a distributed unit of trust, as a mediating entity that manages, in a privacy respectful manner, the exchange of private data.

Contents

1. INTRODUCTION

The future scope of services provided in the context of cities with advanced IT infrastructure is built on the vision of the smart city, a city mirroring for its citizens the community, commerce, healthcare, government and entertainment activities into the electronic domain. A smart city is built around a rich framework of online services which reflect the activities that are available to a citizen in the real world. The different actors participating in this service provision chain are the inhabitants or visitors of the city, suppliers and consumers of tangible and intangible goods, municipal departments, schools, libraries, hospitals, transportation organizations etc. Taking into consideration the diversity of actors it can be easily assumed that users can enjoy a lot of different kind of services ranging from simple information retrieval e.g. regarding social activities in the boundaries of the physical city, to e-government and e-commerce type of services. The huge set of online services, specifically those that concern sensitive social areas like healthcare, increases the flow of personal information towards targets over which the citizen has no control. Even though the smart city vision has a strong impact on the way that Information and Communication Technologies will affect the citizen's life style and day to day activity, it also has a strong impact on the citizen's privacy rights. More than a century after the first essay identifying that privacy, as a fundamental human right, was endangered by technological advances [1], never before in history the citizens have been more concerned about their personal privacy and the threats by emerging technologies [2].

This heightened awareness for privacy issues is mainly due to the ubiquity, the invisibility and the processing power of computation, communication and monitoring devices which make up the distributed infrastructure of a smart city. With a densely populated world of smart and intelligent but invisible devices, no single part of the citizens' lives will by default be able to seclude itself from digitization. The oncoming mass deployment of context-aware and personalized services [3] and the advanced monitoring and surveillance techniques [4] aiming at improving public safety demand, collect, store and process a large amount of personal data. Moreover, Data Mining [5] which promises to efficiently discover valuable, non-obvious information from large databases is very vulnerable to misuse and may compromise privacy by combining personal data from heterogeneous resources.

So far, the vague notion of privacy is situated in the realms of legal and social studies. Nevertheless, all laws and legislation, as well as privacy codes require enforceability, the origins of which may be twofold: self-regulation of the corresponding organizations and industry that collect and process personal data, on the one hand, and deployment of the technical means for enhancing privacy on the other. Self-regulation concerns the restriction of practices according to fair information principles. However, it is often seen as a bothersome bit of overhead, both economical and administrative, while monitoring and verification is needed in order to be effective. Besides, there are numerous cases where privacy invasive technologies are in practice opposed to well-stated privacy policies. Consequently, apart from privacy protection by legislation and codes of conduct, the enforcement of legal requirements by means of privacy enhancing technologies is very important. For that reason, the European Commission, with its leading relevant Directive [6], encourages the development and use of privacy enhancing technological measures as an essential complement to legal means.

In this technical report, the issue of privacy is examined through a combined prism, mixing up law and engineering. The initial thoughts that provoked the proposed idea follow. There are established regulations and related organizations. There are users/consumers that have privacy related concerns. There are service providers that are obliged to follow regulations and treat data in specific manner. But who guarantees for the latter? There is a huge gap between the laws that are written on a piece of paper and an implemented solution that ensures their application. Thus, an architectural idea is presented, derived from work-in-progress within the IST DISCREET [7] project that tries to fill this gap by implementing the regulations and offering a large scale solution ready to be applied. The main concept of the introduced architecture is the development of a unit of trust, which acts as a privacy mediator between users, networks, service providers, monitoring devices and authorities. This mediating architecture protects and keeps the data separated for the provision of services or as input from monitoring systems and ensures that only absolutely necessary information will be disseminated to certain targets. The proposed architecture adopts all the adequate security mechanisms that may contribute to the safety of data. Moreover, it intermediates between data sources and data collectors, comprising a transparent layer of trust and eliminating the overhead for privacy protection that would otherwise be required.

The rest of this report is organized as follows: Section 2 introduces the smart city concept. Section 3 provides some insights on the legal aspects of privacy and section 4 summarizes the privacy concerns raised by the citizens of a smart city. In section 5, a middleware architecture conceived on the basis of privacy legislation is proposed, aiming at providing privacy by technical means. Section 6 concludes this work.

2. CITIES AS SMART ENVIRONMENTS

The notion of city and community exists for centuries. Currently - and as technology advances - a new kind of city / community had emerged, the so-called info-city, with the goal to facilitate the life of its dwellers and improve its quality. A new kind of virtual urbanization recently has started to thrive [8]. As Ferguson et al state in [9] "…an information city…" can be seen as "…a large Internet-based site offering a range of online services, including access to social environments, community services, municipal information, and e-commerce to its info-habitants...". In an attempt to broaden this definition we make a step further and also include context-aware, highly personalized services as well as monitoring and surveillance ones, thus defining an advanced kind of info-city, a smart city. The perspective outlined here is that of a city with advanced IT infrastructure and surveillance/sensor networks on top of which a multiplicity of city related services is offered from/to a number of different actors.

We may divide the services offered in the context of a smart city in three different types; Internet-based services offered by the city municipality, Internet-based services offered by 3rd parties and services exploiting devices such as cameras, sensors and radio frequency identification tags (RFIDs) [10]. E-government services may be offered through an Internet portal simplifying thus bureaucracy procedures like certificates issuing. Moreover, special public interfaces may be offered by the city portal fostering public participation and community discussions. The city may minimize the administrative overhead digitizing e-procurement processes while it can provide advanced cultural and educative services like electronic lending libraries, virtual museum tours and virtual lessons. All the above services are offered in a way fully tailored to the user’s profile and context.

3rd party services follow the same provision pattern with the difference that they are not under municipal management. The city portal acts as their entry point within the boundaries of the info-city. Retail shops obtain their virtual space at the city e-mall, galleries are exposing their exhibitions, special communities are provided with the opportunity to expand their activities at a parallel virtual plane through dedicated e-spaces that can be easily discovered and accessed. The same concept can be applied in the cases of collaborative working and e-learning. The municipality may also provide the infrastructure for the deployment of a inter-hospital medical information repository/system for the prompt retrieval of relevant data when necessary. The city may provide the means for several other public activities like entertainment or news. Again context and profile information is exploited for service personalization.

The vast deployment of a network of cameras, sensors and RFID readers enables the provision of services beyond the traditional Internet based ones. The camera surveillance network can be seen as the means for ensuring citizens safety during their every day activities in the city [11] or for traffic monitoring. RFIDs on the other hand can act as identification means for entrance control in premises and public transportation means, user credentials holders, toll payment etc. In addition it should be mentioned that valuable context related and personalization information can be gathered through sensor devices and be exploited for the customization of the aforementioned Internet based services.

However major issues emerge both from a social and technical point of view even from this very short description of info/smart-cities. As an example we can mention questions such as whether smart cities tend to estrange people, what is the quality level of the offered information and services and whether they indeed meliorate users’ life or not. From a technical point of view, public interfaces [12], tools and easy integration of services on top of smart-cities (backward compatibility and interoperability) are serious prerequisites for their proper and evolvable operation. Last but not least, taking into consideration the vast amount of private, personal and confidential information that is being circulated among parties in such environments, privacy is an issue that needs to be addressed urgently.

3. LEGAL ASPECTS OF PRIVACY

Privacy is recognized as a fundamental human right by the Universal Declaration of Human Rights of the United Nations [13]. It is protected by relevant legislation in all the democratic countries throughout the world.

The first data protection act was adopted in 1970 by the West Germany state of Hesse [14], firing the trend of adopting privacy legislation. The first influential text was the US Privacy Act [15], adopted by the Congress in 1974. Nowadays, the European Directive 95/46/EC [6] enforces a high standard of data protection and it is the most influential piece of privacy legislation worldwide, affecting many countries outside Europe in enacting similar laws. The Directive, in effect since 1998, requires all member states to implement legislation to protect the right to privacy, with respect to the collection, processing, storage and transmission of personal data. Among the objectives of the Directive is the free flow of personal data between the European countries, as well as the restriction of personal data transfer only to countries outside Europe that have enforced an appropriate level of data protection.

The Directive reflects fundamental principles, as codified by the Organization for Economic Co-operation and Development, in 1980 [16]. This codification was a significant milestone, as OECD principles lay out the basis for the protection of privacy. With respect to lawfulness and fairness, personal data must be collected only for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Processing of data should take place only if it is necessary and the data owner has unambiguously given its consent, while, in every case, all the appropriate security safeguards must be provided. Moreover, personal data should not be further retained or disclosed to third parties, except with the knowledge and explicit consent of the data owner.

Technological advances pave the way to relevant legislation to adopt new arrangements, for conforming to the new reality. In Europe, the Directive 95/46/EC is particularized and complemented with reference to the electronic communication sector by the Directive 2002/58/EC [17], which imposes explicit obligations on network and service providers to protect the privacy of users' communications. Furthermore, there is a number of official EU Opinions, Working Documents and Studies that refer to technological advances, such as the use of biometric features, high-tech surveillance mechanisms and RFIDs. Similarly, in the U.S.A., the Computer Matching and Privacy Protection Act of 1988 [18] amended the Privacy Act by adding certain protections for the subjects of Privacy Act whose records are used in matching programs.

Data protection legislation worldwide, where available, naturally defines some exceptions, exemptions and restrictions concerning the scope of the aforementioned principles. In the general case, e.g. in Europe, for purposes of national security and defense, public security, the prevention, investigation, detection and prosecution of crimes and other reasons of common advantage, the collection and processing of personal data may be enforced by the authorities. Lawful interception is currently a common denominator for all the regulatory frameworks for the protection of privacy in electronic communications

Especially, the USA Patriot Act of 2001 [19], received *to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools and for other purposes*, enables the authorization for increased surveillance, far surpassing previously permitted incursions on personal privacy. The Patriot Act defines enhanced surveillance procedures, relaxing the rules for intercepting wire, oral and electronic communications and collecting personal data.

A frequent characteristic of privacy regulations is the definition of privacy authorities. To that respect, the European Commission requires the establishment of public Independent Supervisory Authorities at every Member State, in order to oversee the application of the relevant regulation. These authorities are provided with investigative, intervention and engagement in legal proceedings powers. Moreover, an independent Working Party with advisory status is formed, in order to opine to the Commission for every issue concerning data protection. Similarly, in Canada, the Office of Privacy Commissioner is established, in order to advocate for the privacy rights of Canadians. The Privacy Commissioner works independently from any other part of the government to investigate complaints from individuals with respect to the federal public sector and the private sector.

4. PRIVACY THREATS AND CONCERNS

For the provision of the advanced services of a smart city, the collection and use of user private information is ineluctable and, thus, privacy threats ambush and privacy concerns arise. Ideally, a citizen of the smart city would want a system that preserves its anonymity and guarantees security and confidentiality, while, at the same time, is able to exploit his preferences so he can enjoy personalized service provision. Furthermore, the citizen accepts surveillance as safety preservation means while at the same time he doesn't desire the privacy violation that occurs.

Surveys have proved that users consider service providers untrustworthy; inconvenience in implementing privacy policies, the trend of outsourcing several services and business procedures providing this way access to personal information to third parties and the economical and administrative bridging of companies that leads to probable information linking are the main reasons for this mistrust. Even for companies with good intentions, the enforcement of privacy policies is sometimes quite difficult, since a large amount of privacy violations happens by companies' insiders.

The mass deployment of cameras and their increasing capabilities [11] along with sensors and RFID tags constitute a severe threat to citizens' privacy. These devices in combination with the growing popularity of location-based services formulate an omnipresent web of tracking. Moreover, a human-subject of surveillance is almost never notified about the fact of being monitored.

It is impossible for the individuals to control the fate of their personal data from the time that they are provided or collected; there are no guarantees about the duration of the retention, the disclosure and the processing. The deficiency of technical means, ignorance, malicious purposes, lack of monitoring and verification lead to limited enforcement of the law. In addition, legislation defines several exceptions in data protection that – without proper handling – may be exploited for personal data abuse. Moreover, the complexity of data flows among involved actors as well as the fact that communication channels are not always secure lead to data leakage at several levels, both social and technical.

Summing up, the flip side of providing advanced services and public safety infrastructures is the potential invasion of privacy. Questions like who *monitors* all the different actors that collect, store, have access and might misuse the private information, who *controls* the trust levels of the actors participating in this chain of private data exchange, and who *prevents* the data combination stemming from different sources that might reveal users' private information constitute serious concerns.

5. PROPOSED FRAMEWORK

The issue of privacy responsibility distribution in the large scale context of a smart city is discussed in this section together with a technical proposal for a privacy strengthening middleware, which enables a city to be not only smart but also discreet. The proposed framework extends the responsibilities of privacy authorities, who are offered with a software tool to actively protect the citizens' privacy. The requirements and design approach of this privacy enhancing middleware is presented in subsection A, while a tentative architectural design in subsection B.

5.A Requirements and design approach

Our proposed approach to a privacy protecting system takes the form of a thick middleware layer which defines a secure domain for private information to flow and be processed inside. The middleware's main concern is to mediate between the sources and the consumers of private information. Two fundamental definitions are required here; first of all what constitutes private information, in other words what should be protected by the middleware, and second, a formal description of the privacy threats inside smart city contexts. These two fundamental definitions are not an issue that could be answered by technical design alone but they require the contribution of the relevant regulatory framework. The technical tools that make up the design of a privacy protecting middleware are more or less common among privacy protecting systems. They employ policy frameworks for advanced access control, they encapsulate sensitive data inside cryptographic data structures and they apply common security tools at the networking layer like encryption and firewalls. However existing systems are lacking in two ways. First, in the formal conformance to privacy protecting legislation, since existing systems take regulations into account but they have not been designed centered around them. Second, existing systems lack in their scale; most of them cover only narrow stripes of the complete privacy issue, like privacy during web surfing or restricted in the context of a corporate intranet. However privacy handling at the small scale requires the self regulation by means of restriction of practices according to fair information principles from the service provider's side alone. This also restricts the control that privacy authorities have over the self-implemented privacy policies of individual providers. The intelligent city vision requires a broader view on the issue of privacy with technical solutions that implement the regulatory framework in the widest possible scale in order to protect citizen's privacy both in active (service provision) and passive (surveillance) use cases.

With these requirements in mind we anticipate a middleware comprised of a sophisticated policy framework that will orchestrate a number of privacy components, each with individual responsibilities with regard to specific privacy issues. The policy framework, which is considered the heart and soul of the middleware provides an implementation of the regulatory framework that describes what aspects of user privacy need protection. The actual policies deployed inside it constitute a mapping between the legal conditions that flag a privacy concern (a "trigger") and the technical solution invocation that best offers a mitigation action (a privacy component). User input into a service or recorded data transmission and storage is first assessed by the policy framework for possible privacy risks which triggers privacy components to enforce the privacy principles that regulations define. This approach covers the first requirement, the role of regulations, since the system's design evolves around a legislative-technical work that will translate regulations into triggers and privacy components and express them in policy rules.

The scaling requirement on the other hand is not sufficiently satisfied by merely requiring a distributed technical design approach, since scaling here refers to the broader issue of distribution of responsibilities. A distributed privacy protecting middleware able to address the broadest possible privacy concerns in a smart city requires components in user terminals, service providers, network operators and private IT infrastructures. Even though each actor is responsible for maintaining the middleware in its own infrastructure, the broader privacy goals are only met if the middleware components cooperate across provider/operator domains. The scaling requirement therefore refers to the establishment of trust between the actors, between users and the provider's or operator's infrastructure, between providers and operators, between operators. Trust here could only stem from a commonly accepted actor that would take the responsibility of verifying that individual infrastructures implement the regulatory directives as expected to ensure cross-domain privacy for citizens. In a smart city environment this actor would be the city public authorities.

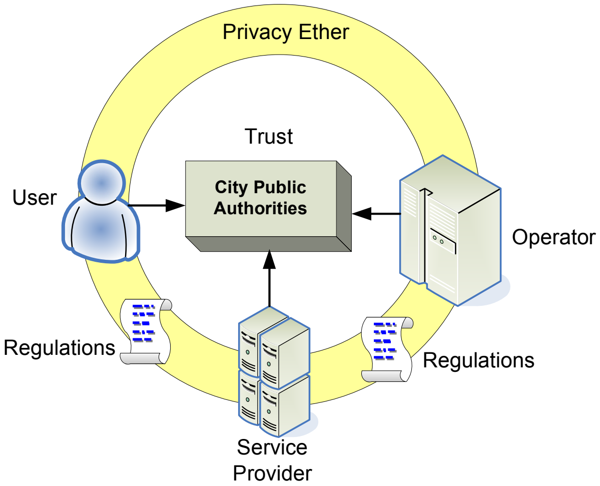
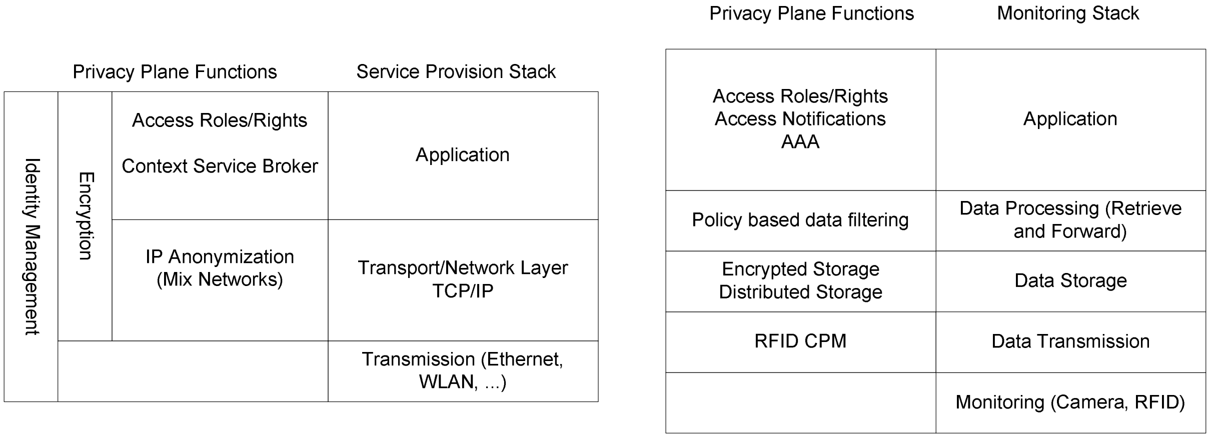


Figure 1. Privacy Ether

5.B Technical approach

Since privacy protection should work at many different layers at once, the privacy middleware should cover vertically a possible stack of service provision. The privacy components are stacked according to their targeted layer of protection and they form a security plane parallel to the normal service provision plane, figure 2(a) illustrates for a hypothetical context aware service provision use case.



(a) (b)

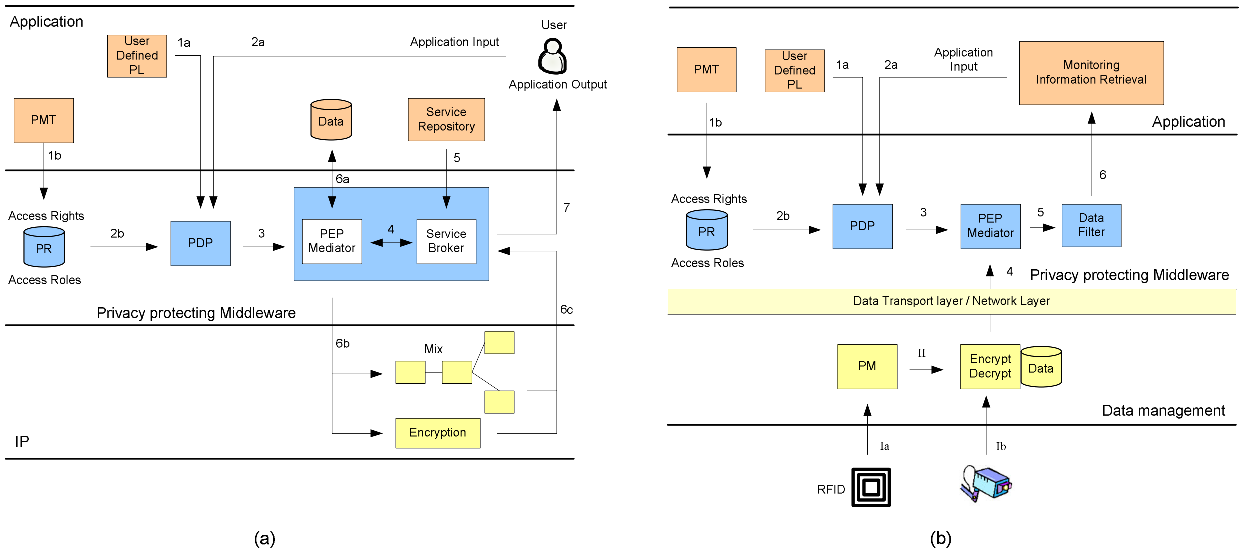
Figure 2. provision stacks and privacy plane

The regulatory policy framework is located at the application layer, and orchestrates common privacy or security components. At the Network layer a Mix Network [20] component offers anonymous network connections while encryption based on a PKI infrastructure at the application layer and relevant encryption technologies on the network and transport layers (e.g. IPSec, SSL) strengthens the protection of the transmitted data. The Identity Management Component offers pseudonymity services to users, who are offered the capability of managing the level of disclosure of their networking fingerprints, e.g. MAC and IP addresses by utilizing anonymization and encryption services. Especially for context aware / personalized services, where a lot of personal information is delivered to the service provider, quite a few privacy considerations are raised since the service provider is not often a trusted entity. In order to resolve the dilemma of anonymity vs. personalization, the proposed approach is to inhibit sensitive information from escaping the protecting middleware's domain and requiring instead the service logic to migrate inside the protected domain and execute there. The Service Broker component offers this capability. Candidate enabling technologies are Mobile

Agents [21], enterprise scale service execution environments like J2EE [22] and web services [23] frameworks.

Figure 2(b) sketches the corresponding stack for a hypothetical surveillance scenario. Again the regulatory policy framework on the top application layer manages access to monitoring data that are collected and stored at the underlying layers. The privacy components in this use case are RFID scrambling devices, encrypted and distributed storage facilities for the recorded data, and data filters that act on the stored data and reduce the possible inferred private information from it (e.g. blurring people's faces from a recorded video of a security camera).

Figure 3 presents the layered components and their proposed interactions, in a typical personalized, context-aware service provisioning scenario (a) and a typical surveillance scenario (b).



(a) (b)

Figure 3. Interaction between privacy components

With reference to figure 3(a), the required policy framework is incarnated inside the middleware layer by the following components: a Policy Repository (PR) which accepts policies enforcing regulatory directives from a Policy Management Tool (PMT); a Policy Decision Point (PDP) [24], the middleware's core that performs decision making based on input from the PR and the user, either in the form of application input or in the form of defining a custom Privacy Level (PL); finally, a Policy Enforcing Point (PEP) [24] also named Mediator since it manages all privacy related resources under the command of the PDP. Personal information coming from the user (1a, 2a) is first processed by the PDP and is forwarded inside the PEP-Service Broker compound component (3, 4). Service logic is required to migrate where the information is (5), execute, possibly draw content (6a) and provide user output (7), all within the middleware's domain. Callbacks and service flow transfers are possible, but all service blocks that process private data are required to migrate inside the protecting domain, which ensures that information will not escape.

A quite similar approach is followed for the monitoring case, as illustrated in Figure 3(b). It should be noted that the level of data filtering, i.e. the privacy level under which information is provided to the application depends on the enforcement of the appropriate policy.

6. CONCLUSION

The recent technological advances in mobile networking, sensor networks, ubiquitous and context-aware computing are reshaping citizens' life, facilitating it and improving its quality. However, they put citizens' privacy at a serious risk, since they realize Ron Rivest's "reversal of defaults": what was once private is now public; what once was hard to copy is now trivial to duplicate; what was once easily forgotten is now stored for ever.

In this report, a framework for the protection of personal data within the context of a smart city is provided. The concept behind the framework is the integration of all privacy-critical functionality of the city's advanced IT services into a thick, privacy-proof middleware layer, conceived on the basis of legislation principles and deployed at city-scale by a municipal privacy authority. This way, the privacy concerns and threats are appropriately addressed, for all types of services.

The proposed framework minimizes citizen's mistrust towards services and service providers. Every piece of private information is filtered by the middleware, which undertakes the enforcement of privacy policies, eliminating the unauthorized access and misuse. The same principle applies for data collected by sensor devices; moreover, when the case of sensoring is surveillance, the citizen may be notified by an RFID that acts as a notification token.

By implementing the privacy principles formulated by the legislation, the proposed architecture has full control on the lifecycle of personal data. Thus, it provides guarantees for the purpose and the necessity of data collection and processing, the duration of their storage and the disclosure, along with the security measures for the availability, integrity and confidentiality of personal data. Furthermore, by applying the respective policies, it can accurately handle the exemption cases of emergency situations, lawful interception and every other case where - for the common welfare - personal data revealing must be enforced.

ACKNOWLEDGMENT

This work is partially supported by the European Union, in the framework of the FP6 – IST Project DISCREET. The authors would like to express their gratitude to the consortium, for the fruitful discussions.

REFERENCES

[1] S. D. Warren and L. D. Brandeis, “The Right to Privacy”, *Harvard Law Review*, Vol. IV, No. 5, pp. 193–220, Dec. 1890.

[2] The European Opinion Research Group, “European Union citizens’ views about privacy”, *Special Eurobarometer 196*, Dec. 2003.

[3] B.N. Schilit, N.I. Adams, and R. Want, “Context-Aware Computing Applications”, in *Proc. of Workshop on Mobile Computing Systems and Applications*, Santa Cruz, CA, USA, 1994.

[4] R. Cucchiara, “Multimedia surveillance systems”, in *Proc. 3rd ACM Intl. Workshop on Video Surveillance & Sensor Networks*, Singapore, 2005, pp. 3–10.

[5] J. Han, M. Kamber, *Data mining: Concepts and Techniques*, NY: Morgan-Kaufman, 2000.

[6] European Commission, “Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data”, *Official Journal of the European Communities*, No. L 281, pp. 31–50, Nov. 1995.

[7] IST DISCREET, home page: www.ist-discreet.org.

[8] T. Ishida, “Understanding Digital Cities”, *Lecture Notes In Computer Science*, vol. 1765. Springer-Verlag, London, 2000, p. 7-17.

[9] D. Ferguson, J. Sairamesh, and S. Feldman, “Open frameworks for information cities”, *Communications of the. ACM 47*, 2 (Feb. 2004), pp. 45-49.

[10] R. Weinstein, “RFID: A Technical Overview and Its Application to the Enterprise”, *IEEE IT Professional*, Vol. 7, No. 3, pp. 27–33, May 2005.

[11] M. Bramberger, A. Doblander, A. Maier, and B. Rinner, “Distributed Embedded Smart Cameras for Surveillance Applications”, *IEEE Computer, vol 39 no.2,* Feb 2006, pp. 68-75.

[12] M. Chang, K. Jungnickel, C. Orloff, I. Shklovski, “Engaging the City: Public Interfaces as Civic Intermediary”, *Conference on Human Factors in Computer Systems (CHI 2005)*, Workshop organizer's proposal, Portland, OR, April 3-7, 2005.

[13] United Nations, “Universal Declaration of Human Rights”, http://www.un.org/Overview/rights.html.

[14] Gesetz- und Verordnungsblatt für das Land Hessen - Teil I - Nr. 4, Wiesbaden 12.Oktober 1970, 625ff.

[15] Public Law No. 93-579, 88 Stat. 1897 (Dec. 31, 1974), 5 U.S.C. 552a.

[16] Organization for Economic Co-operation and Development, “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, Sep. 1980.

[17] European Commission, “Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)”, *Official Journal of the European Communities*, No. L 201, pp. 37–47, Jul. 2002.

[18] Public Law No. 100-503, Oct. 18, 1988, 5 USC 552a.

[19] H. R. 3162, Oct. 21, 2001.

[20] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms”, *Communications of the ACM*, 24(2), pp. 84–88, 1981.

[21] T. Magendazn, M. Perdikeas, I. Venieris, “Agents”, in *Object Oriented Software Technologies in Telecommunications*, I. Venieris, F. Zizza, T. Magedanz Ed. John Wiley & Sons Ltd., 2000, pp. 137–170.

[22] Sun Microsystems Inc., “Java Platform, Enterprise Edition (Java EE)”, http://java.sun.com/javaee/

[23] E. Cerami, *Web Services Essentials.* CA: O'Reilly & Associates.

[24] A. Westerinen, et al., “Terminology for Policy-Based Management”, *IETF RFC 3198*, Nov. 2001.