available at www.sciencedirect.com

ScienceDirect

Information Security Technical Report

Privacy and consent in pervasive networks

Nazir A. Malik, Allan Tomlinson[*]

Information Security Group, Royal Holloway, University of London, Egham, Surrey, United Kingdom

ABSTRACT

Pervasive networks and location based systems have the potential to provide many new services. However the user of these services often has to provide personal information to allow the service to operate effectively. This article considers the problem of protecting personal information in this environment, and reports on the legislative and technical efforts being made to protect user privacy.

1. Introduction

With the emergence and development of systems incorporating pervasive computing, users are able to access new forms of services on their personal devices. Location Based Systems are also gaining popularity, with new forms of services being devised based on the location information of the user. The ease of access, and increasing amount of data exchanged between the user and these service providers, has increased the risk of unauthorized use of the user's Personally Identifiable Information (PII). Current centralized security mechanisms are unable to provide the assurance of privacy to the users in such environments. Moreover, the diversity of regulations in different countries and lack of a cohesive structure to implement privacy mechanisms requires some of deliberation for cross border implementation. Many government agencies maintain records of each individual; credit card companies have records of every card transaction; mailing lists including telephone numbers are sold to anyone willing to pay the right price. Similarly social websites are changing their Terms of Service over time to allow use of the user's private data for advertisements and marketing. The user's data from archives may be used even if the user deletes the data or opts out by deactivating their account. Some protection is therefore required if the risk to unauthorized use of PII is to be mitigated.

2. Privacy and PII

Before discussing how PII may be protected, it is useful to examine what kind of data may be considered to be Personally Identifiable Information.

The European Union (EU) defines PII as follows:

> "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

In the USA, the NIST Guide to Protecting the Confidentiality of Personally Identifiable Information defines PII as:

> "Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

[*] *Corresponding author.*
E-mail address: allan.tomlinson@rhul.ac.uk (A. Tomlinson).

1363-4127/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2009.10.002

Given these definitions we can say that privacy means the protection of our personal information, for example: contact details; family history and medical data; credit card numbers; financial status and obligations; professional contacts and Legal information.

In today's information age, government agencies implement security measures and companies take competitive edge over others by collecting and filtering information. This information is either gathered from the organization's own resources or bought from others (Mccandless, 1997). This personal information is often linked to individuals via their identity. In the context of pervasive computing, identity is often used to authenticate and identify an individual user in public or private networks to gain access to the services provided. Thus a user may have multiple online identities with almost the same information associated with each of them. Consequently it becomes quite cumbersome to the user to have to manage a number of identities, each with their associated PII. This problem may be addressed by identity management systems. Identity management systems provide the individual user the ability to control when, where, how and to whom they provide their private information (Hansen et al., 2008) but they also pose an inherent privacy risks. There is an obvious burden of security and trust on any system that manages a collection of user's credentials and PII. Moreover, such systems present a valuable target to attackers.

3. Location information

In the pervasive computing environment, Personally Identifiable Information as defined above is increasingly being collected, used and exchanged by commercial and government organizations. In pervasive computing systems, location is becoming an important privacy concern for individual users. Location Based Systems (LBS) are increasing and new applications are being developed tailored to the need of individual users based on their current location. Once the location has been sent to the LBS, along with user's identification, the user cannot control or manage this information. Location Based Systems can use this information to locate and track the user's activity in place and time Bowen and Martin, 2007.

A number of ways can be used to estimate the position e.g. Global Positioning System (GPS), Global System for Mobile communications (GSM), Wi-Fi, Bluetooth and WiMAX. GPS has local receivers on the user's device and is the most common LBS. GPS is being used in vehicle navigation, PDAs, mobile phones and many other personal devices. Mobiles phones can use GPS or GSM signals to estimate the user's location. Hybrid devices are also being developed which can use any combination of these LBSs to provide a more accurate position estimate. An Enhanced 9-1-1 or E911 service (FCC Report, 2005) automatically associates a physical address with the calling party's telephone number, and routes the call to the most appropriate Public Safety Answering Point (PSAP) for that address. In EU, Directive 112 (Directive, 2002) requires the caller location information to be made available to the emergency services. The directive requires mobile phone networks to provide emergency services with whatever information they have about the location a mobile call was made. Based on E112, the eCall project was launched in EU to reduce the response time to accidents with a combination of an In Vehicle System (IVS) and infrastructure of PSAPs.

To provide a degree of location privacy, a number of masking techniques may be used with location information including k-anonymity (Sweeney, 2002), and pseudonymity (Jorns et al., 2007). Bowen and Martin (2007) have proposed the concept of a location information boundary to intercept the location information and masking it before release to the LBS.

4. Privacy regulations

Government bodies are also developing legal safeguards to PII. The Organization for Economic Co-operation and Development (OECD) provides guidelines for protection of privacy and trans-border flow of personal data, which was adopted in 1980. In response to these guidelines many countries have legislated to protect personal data and its use. Varying levels of regulations exist in different countries and different governments are considering various laws to protect privacy and location information. For example, in the USA, the Communication Act of 1934 amended by the Telecommunications act of 1996 (Communications Act of 1934) mandated that customer proprietary information can be used only for the services requested by the customer. Separate privacy laws exist for different sectors.

Also in the USA, the Health Insurance Portability and Accountability Act (HIPAA) was made a law by US Congress in 1996 which caters for handling of medical information and helps to keep the information private. The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, ''Requires clear disclosure by all financial institutions of their privacy policy regarding the sharing of non-public personal information with both affiliates and third parties''. Children's Online Privacy Protection Act (COPPA) of 1998 is another US law which applies to online collection of personal information from children under 13 years of age. It gives the outline to be included in privacy policy of the website as to how to seek the verifiable consent of the parent or guardian and the steps required to be taken to protect the data. The Wireless Communication and Public Safety Act allowed Federal Communications Commission (FCC) for using location based systems and services. Location Privacy act ''require providers of location based services and applications to inform customers, with clear and conspicuous notice, about their policies on the collection, use, disclosure of, retention of, and access to customer location information''.

In the European Union (EU) the 1995 data protection legislation was passed to be applied across 27 EU member states. This legislation is an attempt to ensure the protection of personal data and flow of information between EU states. The data protection act prohibits the processing of personal data without the explicit consent of the owner of the data unless explicitly allowed legally. The EU has also funded technical research initiatives such as Privacy and Identity Management in Europe for Life (PrimeLife). This is a research project funded by the European Commission's 7th Framework Programme for bringing sustainable privacy and identity management to future networks and services (PrimeLife). The project will expand the 6th framework program Privacy and Identity Management in Europe (PRIME) that enabled the user their legal rights to control personal information in online transactions.

Canadian laws are similar to EU having a baseline to protect the use of personal data. The updated legislation Personal Information Protection and Electronic Documents Act (PIPEDA) provides the necessary legislation for protection of personal information and electronic documents. The Australian privacy law (Privacy Act, 1988) deals with the privacy of personal information. Part III of the law outlines legislation about information privacy. All these regulations provide guidelines for the protection of PII, which refers to information that uniquely identifies or locate a single person. Laws similar to COPPA have been passed in Australia and Canada.

5. Privacy standards and architectures

In addition to the legislative work on privacy protection, there is an increasing technical response to this challenge. A number of standards designed to protect privacy on the Internet are now emerging. Due to the increasing number of services using location information, the Internet Engineering Task Force (IETF) has established a working group, Geopriv. This group will develop representations of location information in Internet protocols, and analyze the security/privacy requirements. An internet Draft (Geolocation Policy) document, geolocation policy, expressing format for privacy preferences and location information was made available on 12 July 2009. The W3C Platform for Privacy Preferences (P3P) enables to express privacy policies in a standard format and provides specifications for the websites to present their data collection and enables users to understand about data collection, data usage, and their consent for opt-in or opt-out.

The IT industry is also responding to the challenge: IBM for example, has developed an Enterprise Privacy Architecture (EPA). The aim of this architecture is to allow the use of personal information while maintaining the need for privacy. It gives an enterprise the ability to implement the privacy regulations and choices of individual users. EPA is broadly divided in to three areas: Privacy Regulation Analysis, Management Reference Model and Technical Reference Model.

5.1. *Privacy regulation analysis*

Privacy regulations are normally written in legal format and vary from country to country. So there is a need to address the problem by managing regulatory summary tables and regulation rules tables. A regulatory summary table uses a cohesive terminology to form applicable regulations whereas a regulation rules table identifies enterprise data and legal restrictions on its use (Karjoth et al., 2002). The scope of privacy regulations are described by the business use phases of Collection, Retention, Processing and Use (CRPU). The privacy regulation analysis is done on all stages of the privacy architecture.

5.2. *Management reference model*

The IBM Enterprise Privacy Architecture model describes the key elements of infrastructure necessary to support the privacy objectives of the enterprise. The top three layers describing strategy, controls and practices, as shown in Fig. 1, form the Management reference Model. Strategy defines the high level policies and regulations which are applicable in a particular enterprise. The strategy will also outline the protection and security requirements of private information to achieve the objectives. Controls define the processes to enforce the policy derived from strategy and a practice defines how the policy will be incorporated in the processes.

5.3. *Technical reference model*

The Technical Reference Model provides privacy at the transactional level, where the enterprise collects and uses personal information. This model relies on Object, Data and Rules models to build applications and to determine privacy relevant data and its handling.

Within the academic community there is a wealth of research on privacy enhancing technology. One technique widely discussed is the use of unlinkable pseudonyms to provide pseudonymity. Pseudonymity is an approach normally used in personalized systems to give the user a degree of anonymity while still being able to recognize the user in various sessions. However, the disadvantage of pseudonymity is that many privacy laws are not applicable when the user is using pseudonyms. Interactions requiring financial transactions and the shipment of physical goods cannot be completed while using pseudonyms and the true identity of the user is required to complete such transactions. Another approach to providing user privacy is to use the largest permissible common subset, which means that the common personalization methods in different laws be applied. The idea can be implemented if a small number of jurisdictions apply. However, if the areas of jurisdiction increase, the resulting common subset may become very small and not applicable. Different versions of the system can be tailored according to the different countries, and the countries having common laws can be combined using the common subset but the

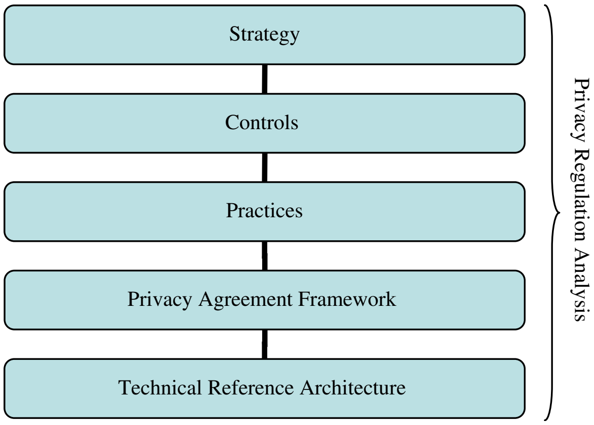
Strategy
Controls
Practices
Privacy Agreement Framework
Technical Reference Architecture
Privacy Regulation Analysis

Fig. 1 – IBM Enterprise Privacy Architecture.

approach will not be scalable as the number of countries will increase (Wang et al., 2006).

An approach to enterprise wide enforcement of privacy promises is proposed by Powers et al. (2002). This approach describes a framework for managing collected personal data and enables enterprises to implement their privacy promises, to collect and manage user preferences and consent, and to enforce the privacy promises throughout the enterprise. The core of the architecture is the privacy management server which provides a rules processing engine and also produces audit logs. Privacy rules are enforced by privacy monitors, which protect the PII by monitoring the data going in and out of the monitored system. When a user submits their PII, the monitor will track the PII and the user consent for the use of data, and privacy policy at the time of submission of data. If the policy changes over time, new consent should be taken from the user to abide by the new policy.

Wang et al. (2006) have proposed a Product Line Architecture (PLA) for handling privacy constraints in web personalization. In this architecture a User Modeling Server (UMS) acts as central repository to store personal information, which represents the user characteristics and behaviour, and applies user modeling methods to extract assumptions about users. The architecture consists of external user-adaptive applications which query the UMS for user information to provide services to end users. A Directory Component acts as repository for user models, where the user model represents individual privacy constraints along with characteristics, behaviour and inference about the users. A User Modeling Component (UMC) Pool is a set of UMCs containing user modeling methods. A selector selects only those UMCs which are allowed to operate under a user's current privacy constraints. It can select optional UMCs to give optimal personalization. Privacy Boolean Expressions determine whether the associated UMC will operate under a certain privacy constraints or not. Privacy constraints are the laws governing the user and individual's own privacy policy.

Controlling access to the system plays an important role in protecting the privacy of the stored data and PII. Security technologies for access control are normally implemented by 'Allow' or 'Deny' rules which are low level implementation rules. Privacy rules and legislation are not normally defined in low level implementation rules. Rather, the context of access needs to be ascertained which fulfils a particular business process for which the data access is allowed. Therefore, the implementation of privacy policy needs low level implementation together with the context for which the data access is being given. The owner of the PII's consent must also be considered before giving the 'Allow' or 'Deny' decision. This may be implemented by opt-in and opt-out policies for a specific data subject's PII. Similarly, if the terms of policy are changed over time, new consent must be acquired from the data subject for opt-in or opt-out based on the new privacy policy. If the user does not wish to opt-in to the new privacy policy, the he should be governed by the privacy policy for which he has given the consent instead of the new policy.

The recent EU project PLASTIC (The Plastic Project) provides the adoption of service-oriented computing for the B3 G multi-radio network. Trusted Architecture for Securely Shared Services (TAS3) project is aiming at a European wide impact on services based upon personal information, which is collected and stored at distributed locations and used in a multitude of business processes. The goal of TAS3 is to demonstrate user and service provider authentication and credential management, establishing trust between users, information repositories and service providers and data protection policies. TAS3 is developing a trusted architecture and adaptive security services to protect privacy.

6. Conclusion

Pervasive computing is still in its infancy and a lot of research is required before we see the implementation of real pervasive environment. Current research in pervasive computing is mainly focused on the service discovery, context acquisition, context categorization and context modeling. However the impact on privacy is being considered and some privacy schemes are emerging.

Even so, although privacy schemes are being implemented in some architectures, no generalized architecture exists in pervasive environment. Therefore schemes are implemented differently in each case. Moreover, the final implementation of the pervasive environment involves the use of devices by non-technical users and the implementation of privacy schemes needs to be transparent to the end user to enable them to give their informed consent.

REFERENCES

Bowen III CL, Martin TL. A survey of location privacy and an approach for solitary users. I:n proceedings of 40th annual Hawaii international conference on system sciences (HICSS); Jan 2007.

Children's Online Privacy Protection Act of 1998, http://www.coppa.org/.

Communications Act of 1934: as amended by Telecom Act of 1996, http://www.fcc.gov/Reports/1934new.pdf.

Directive 2002/22/EC of the European Parliament and Council of 7 March 2002, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ: L:2002:108:0051:0077:EN: PDF.

European Union, Directive 95/46/EC of the European Parliament, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN: HTML; 24 Oct 1995.

FCC Report on the deployment of E-911 Pursuant to Public Law No. 108-494, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-257964A1.pdf; 1 April 2005.

Geolocation Policy. A document format for expressing privacy preferences for location information, http://www.ietf.org/id/draft-ietf-geopriv-policy-21.txt.

Gramm-Leach-Bliley Act of 1999, http://banking.senate.gov/conf/grmleach.htm.

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf; Jan 2009.

Hansen M, Schwartz A, Cooper A. Privacy and identity management. IEEE Security and Privacy Mar/Apr 2008;6(2): 38–45.

Health Insurance Portability and Accountability Act of 1996, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

IETF Geographic Location/Privacy (geopriv), http://www.ietf.org/dyn/wg/charter/geopriv-charter.html.

Jorns O, Quirchmayr G, Jung O. A privacy enhancing mechanism based on pseudonyms for identity protection in location-based services. In: Proceedings of the 5th Australasian information security workshop (AISW). Ballarat, Australia; 2007. pp. 133–42.

Karjoth G, Schunter M and Waidner M. Privacy-enabled services for enterprises. In: Proceedings of 13th international workshop on database and expert systems applications; 2–6 Sept. 2002. pp. 483–7.

Location Privacy Protection Act of 2001, http://thomas.loc.gov/cgi-bin/query/D?c107:12:./temp/~c107Kjp3ZD.

McCandless M. Managing your privacy in an on-line world. IEEE Expert: Intelligent Systems and Their Applications Jan/Feb 1997;12(1):76–7.

OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

The Personal Information Protection and Electronic Documents Act (PIPEDA), 3, http://laws.justice.gc.ca/en/notice/index.html?redirect=/en/P-8.6/258031.html; Mar 2006.

Powers CS, Ashley P, Schunter M. Privacy promises, access control, and privacy management. In: 3rd international symposium on electronic commerce (ISEC), 18–19 Oct 2002. pp. 13–21.

Prime, EC 6th Framework Programme, https://www.prime-project.eu/.

PrimeLife, EC 7th Framework Programme, http://www.primelife.eu/.

Privacy Act, http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/; 1988.

Sweeney L. k-Anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 2002;10(5):557–70.

The TAS3 Project, http://www.tas3.eu/.

The Plastic Project, http://www.ist-plastic.org/.

W3C Platform for Privacy Preferences (P3P), http://www.w3.org/P3P/.

Wang Y, Kobsa A, van der Hoek A, White J. PLA-based runtime dynamism in support of privacy-enhanced Web personalization. In: proceedings of 10th international software product line conference (SPLC), August 2006. pp. 151–62.

Wireless Communications and Public Safety Act of 1999, http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.438.IH.