A Privacy Preference Model for Pervasive Computing

Karim Adam
Computing Research Centre
The Open University
Walton Hall, MK7 6AA,
Milton Keynes, UK
E-mail:K.A.Adam@open.ac.uk
http://mcs.open.ac.uk

Blaine Price,
Computing Research Centre
The Open University
Walton Hall, MK7 6AA,
Milton Keynes, UK
E-mail: B.A.Price@open.ac.uk
http://mcs.open.ac.uk

Mike Richards
Computing Research Centre
The Open University
Walton Hall, MK7 6AA,
Milton Keynes, UK
E-mail: M.Richards@open.ac.uk
http://mcs.open.ac.uk

Bashar Nuseibeh
Computing Research Centre
The Open University
Walton Hall, MK7 6AA,
Milton Keynes, UK
E-mail: B.Nuseibeh@open.ac.uk
http://mcs.open.ac.uk

Abstract: *Widespread acceptance of e-government and m-government (and for that matter pervasive-Government) services will only take place when citizens are satisfied that personal data is stored, transmitted and processed with respect to their privacy. We compare and contrast data protection regimes found around the World and suggest that these have directly influenced the uptake of existing private-sector mobile services. Citizen uptake of e-government services will be encouraged by strong regulatory regimes dedicated to the protection of personal data. Consumers will entrust personal data where they can exert some measure of control over the release of that data to other parties. We examine a number of such controlling mechanisms and suggest a new privacy architecture intended for mobile service provision.*

Keywords: e-government, m-government, law, data protection, privacy.

1. Introduction

Increased penetration of mobile phones has made the development of mobile government services more attractive than ever before. By 2008 mobile Internet users in Europe will "*out-number nonusers 3 to 2"*(3G-UK, 2003). If this rise in mobile Internet use is to be matched by a corresponding increase in m-governance, there is a precondition that the privacy of the individual is respected and protected (Abie et al., 2004). A survey of deployed m-government applications (Sharma & Gupta, 2004) reveals that future pervasive government applications will not be significantly different; hence, privacy-related threats to the deployment of pervasive government services are *identical* to those currently considered by general pervasive computing research.

In this paper we consider how current data protection legislation and common law protect the user but may also inhibit services that benefit from location-aware technology. We look at a potential three-way conflict between the wishes of the user, the capabilities of the technology, and the local legal regime. First we consider how various national and international legal jurisdictions have attempted to incorporate the concept of privacy into legislation. Then we look at current privacy-enhancing infrastructures and the impact of our current research on these infrastructures. We describe our privacy preference model in section 4, and then conclude with a number of issues to be considered at the next stage of our design.

2. Legal Jurisdictions: laws affecting mobile computing

Laws affecting privacy and data protection vary from country to country. Four legal jurisdictions (or regulatory regimes) have been identified. They are:

1. States with strong privacy protection including location-awareness (EU and Japan);
2. States with strong privacy protection (e.g. Australia and Canada);
3. States with some privacy protection (e.g. the USA);
4. States with little to no privacy protection in law.

During the 1930s and 40s, IBM-Hollerith punch card technology was used by many European governments to process national census data. Following the outbreak of the Second World War, this information was used by the occupying Nazis to identify Jews for transport to extermination camps (Black, 2001). As a result of this and other human rights abuses, post-war Europe codified strict privacy protection through international treaty and national legislation. Article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR) (1950) explicitly states that every citizen possesses an intrinsic right to their privacy in both private and family life (subject to some restrictions). Most Western countries have followed suit, utilising OECD Guidelines (OECD, 1980), often cited as Fair Information Practices (FIP). The ECHR was one of the first ‘Bill of Rights’ documents to explicitly name privacy as a fundamental human right. West European democracies were early adopters of the OECD guidelines on privacy, influencing the development of European Community (EC) law on data protection and privacy.

The ECHR is only enforceable against signatory governments; to remedy this shortcoming two pieces of EC legislation extend privacy protection to incorporate individuals and non-governmental bodies:

1. **Directive 95/46/EC (1995)** ensures that users have access to all data held about them; that data is only collected with the individual’s explicit consent, and that it is destroyed when it is no longer needed for the original purpose.

   This directive has possible consequences for location-aware computing. For example, a user enters an area offering a service to which they must subscribe; must the user give explicit permission for the release of personally identifiable data for each new instance of the service? It is possible that this law may protect users, but it is insufficiently flexible for them to effectively utilise the inherent advantages of mobile technology.

2. **Directive 2002/58/EC (2002)** anticipates some measure of technological change. It extends Directive 95/46/EC into the telecommunications sector and makes explicit mention of location-aware technologies. The drafters of this directive were considering second and third-generation mobile telephones, but it is so drafted that it effectively prohibits the use of location information without the user's explicit informed consent.

> Directive 2002/58/EC requires that equipment and service providers offer a simple free-of-charge method for users to temporarily hide their location information. The directive also controls the use of cookies in web browsers which can be used to recover the browsing activities of an individual user.

European privacy laws attempt to implement 'transitive closure' whereby data may only be exported from one country to a second country possessing an equivalent data protection regime; or where the exporter has entered into a special data protection contract with an importer willing to provide equivalent protection to that found in the directives.

Japan has amongst the greatest take-up of consumer-level pervasive computing (in the form of location-aware mobile telephone services). It was one of the first countries to define privacy regulations for pervasive computing. Early market certainty resulted in increased business confidence and thus a wide proliferation of services. Similarly, thanks to well-established regulation, consumer confidence in new services was higher than in a completely unregulated arena.(Milberg et al., 1995)

Canada and Australia have also instituted strong privacy laws, although without explicit mention of location-aware computing. Like the EU and Japan, each country has instituted Information/Privacy Commissioners with the power to take both punitive and retributive action against privacy violations.

American legal commentators have considered privacy (*"the right to be left alone"* (Warren & Brandeis, 1985)) as a "natural law" or residual right since the late 19th Century. Initial discussions were prompted by the rise of a newspaper industry invigorated by the widespread use of photography. A consensus has been that the right to privacy has always existed, but had never been formally incorporated in statute (most notoriously privacy is not explicitly mentioned in the Constitution of the United States). Supreme Court decisions suggest that the 9th, and to some extent, the 3rd, 4th, and 5th amendments to the United States Constitution provide some measure of personal privacy protection.

Privacy protection in the United States consists of a patchwork of legislation at both state and national levels covering distinct, narrow domains; including websites aimed at children (The Children's Online Privacy Protection Act, 1998), financial sites (Gramm-Leach-Bliley Act, 1999), health insurance sites (The Health Insurance Portability and Accountability Act, 1996), and certain baffling collections of data such as archives of videotape rentals (Video Privacy Protection Act, 1988).

Heavy resistance to any form of privacy regulation has been driven by the data processing industry itself. Instead, the US has relied on a process of self regulation (e.g. TRUSTe (2004)) as an alternative to statutory protection. In almost all cases, self-regulation has left the individual with virtually no mechanism for redress of violations.

Unlike other Western countries, the US does not possess a comprehensive national data protection law, the closest equivalent to a national privacy commissioner is the Federal Trade Commission (FTC). The FTC can use existing unfair trading legislation to take action against a business that violates a posted privacy policy; however such violations are difficult to prove in court proceedings and the FTC has only chosen to act in a very small number of cases. The most notable case was against GeoCities in 1998 (FTC, 1998) which was found guilty of misrepresenting the purpose for which it was collecting data from both adults and children. Despite several high profile violations of the TRUSTe standards by Toysmart (attempted), Microsoft (Office 98), and RealNetworks (RealJukebox) (Bronski et al., 2001), their TRUSTe certificate has never been revoked.

Given the weak standards set for simple online privacy protection, there is no immediate prospect of legislation in the US either affording any privacy protection or impediment to location-aware computing. Worldwide, regulations requiring mobile telephone networks to provide location information to emergency services (e.g. E-911 in the US, E-112 in Europe (Globallocate)) are likely to affect how privacy-enhancing technologies can be applied.

Pervasive-Government services obviously need to be aware of the current regulatory regime so that they can be made legally compliant. Certain regimes require explicit notice to and consent from the user before services can be provided. This will constrain how services are delivered. The very nature of pervasive-Government suggests moving between regulatory regimes will be a sufficiently common occurrence that users must be assured that their personal level of protection will be maintained as they cross the invisible borders between regimes. We next discuss some existing research work in privacy control technologies.

3 Privacy-enhancing, preserving and protecting technologies in pervasive computing

In the last decade there has been an increased interest in privacy-related research in pervasive computing. A number of privacy-preserving, privacy-enhancing, and privacy-protecting technologies have been proposed, some of which have been implemented in mobile devices (e.g. (AT&T, 2003)). Ackerman (2004) describes these technologies in four broad categories, namely: *encryption and security mechanisms, anonymising mechanisms* (Beresford & Stajano, 2003; Gruteser & Grunwald, 2003)*, infrastructures* (Hong & Landay, 2004; Langheinrich, 2002; Yamada & Kamioka, 2005) *and labelling protocols* (Cranor, 2002).

Jiang et al. (2002) categorise privacy-protecting technologies into three types: *prevention, avoidance,* and *detection*. The authors also separate the lifecycle of personal data into three phases: *collection, access,* and *second use*. The three types of privacy protection mechanism together with the three lifecycle phases combine to form a 'design space' of privacy solutions divided into nine two-dimensional zones. Jiang and his colleagues further stress that previous ubicomp privacy research has explored only a small portion of the entire design space; primarily preventive mechanisms for the collection and initial access of data. They point out that there is the need to explore other areas such as controlling the second-use of personal data, and measures for detecting unauthorized access of personal data.

Under Ackerman's classification, infrastructure-based privacy-protecting technologies usually make use of a combination of the technologies listed above. We will therefore limit our discussion to a number of such infrastructures used in pervasive computing.

The Confab System (Hong & Landay, 2004) provides a framework for end-users and application developers to manage privacy within pervasive computing. Confab is probably the most recent and most advanced privacy-sensitive architecture (Ackerman, 2004). Confab's architecture is based on a decentralised approach for building control and feedback mechanisms as well as a form of 'plausible deniability' allowing for exceptions to the emergency services. Although Confab is robust and supports a wide range of pervasive computing applications across pessimistic, optimistic and mixed-initiative environments; it only supports relatively simple privacy preferences (Ackerman, 2004). For example, pessimistic pervasive computing applications rely on users configuring their privacy preferences beforehand. However, research has shown that there is a clear requirement for these preferences to be easily set and/or re-used across a wide range of specific scenarios.

Langheinrich (2002) discusses a privacy awareness system, or *pawS*, supporting privacy in pervasive computing. *pawS* mechanisms support the principles of notice, choice, consent, proximity, locality, access and recourse. An example of *pawS* is as follows; Bob uses a wirelessly networked mobile device and a set of codified privacy preferences. He enters a busy business centre and encounters various location-based services, most of which require the exchange of some measure of personal information (e.g. location, identity, etc). As soon as Bob approaches any of these services, one of the centre's privacy beacons uses a wireless communications channel (such as WiFi, Bluetooth or IrDA) to notify Bob of the service, as well as the P3P-encoded (Cranor, 2002) privacy policy of the service. The privacy assistant on Bob's mobile device compares his configured privacy preferences with the privacy policy of the service. Each party uses a database to maintain a record of the negotiation, data disclosure and the service provided (if it is provided at all).

Yamada and Kamioka (2005) proposed an Encapsulated Mobile Agent-based Privacy Protection (EMAPP) model where a *privacy proxy* encapsulates a user's privacy preferences, personal data, and a mobile agent into a *privacy capsule.* The mobile agent only allows access to the private data inside the capsule if the service requesting the data has a matching privacy policy.

It can be argued that setting privacy preferences is not a perfect solution, but qualitative studies conducted by Consalvo et al. (2005) suggest that pre-formulated preferences are useful for users at least at an initial stage in their use of mobile services. Privacy preference models would seem to be necessary in order to facilitate the use of privacy-preserving infrastructures.

4 Proposed Model

All systems make an assumption that users have either; predefined privacy preferences (Yamada & Kamioka, 2005); or that they support simple privacy preferences which may not accurately reflect existing social settings (Hong & Landay, 2004); or are downloaded from a trusted third party such as a consumer interest group (Langheinrich, 2002).

Most privacy-preserving technologies have little or no consideration for the regulatory regimes of users. We therefore propose modelling a set of preferences to include *noise* & regulatory regimes (or data protection jurisdictions).

Noise is metaphorically defined as the intentional, or unintentional, manipulation or transformation of data preventing the true information in the data from being revealed. Noise includes, cloaking, blurring, anonymity (or pseudonymity), hashing or encryption, and lying (also termed plausible deniability (Hong & Landay, 2004) or benign deception). We divide noise into five types:

1. *anonimizing*: hiding the identity of the user;
2. *hashing*: disguising the identity of the user
3. *cloaking*: making the user invisible;
4. *blurring*: decreasing the accuracy of the location (and possibly time); and
5. *lying*: giving intentionally false information about location or time.

A number of challenges must be overcome in the design of a privacy-preference model. One of the most important is the creation of a language in order to express these preferences. P3P (Cranor, 2002) specifies a machine-readable language (based upon XML) for describing web site privacy policies; as well as a protocol for retrieving these policies from remote web sites. P3P has inherent limitations of application in the pervasive computing environment (Langheinrich, 2002) and therefore, is not suitable for expressing privacy preferences in pervasive computing.

A P3P Preference Exchange Language – APPEL (Cranor et al., 2002)) *specifies a language for describing collections of preferences regarding P3P policies between P3P agents*. With APPEL, users are able to express preferences using rule-sets and through intelligent user agents; automated *or semi-automated* decisions can be made by matching user privacy preferences with P3P-enabled privacy policies of web sites. Most of APPEL's syntax and semantics are based on the P3P 1.0 specification, which has its inherent limitations (see (Electronic Privacy Information Center, 2000)). An extension of APPEL and/or expressing privacy preferences in conjunction with Geopriv (Schulzrinne et al., 2004) or PDRM (Personal Digital Rights Management (Gunter et al., 2004)) could effectively tackle potential implementation and deployment bottlenecks. Two of these extensions are: Geopriv and PDRM.

The Geographic location and privacy (Geopriv) system (Cuellar, 2004) is based on a subset of XML called the Geo-location Privacy Policy Markup Language. Geopriv allows users to define rules for privacy control with respect to their location information. These rules are held on a location server and are used to restrict the redistribution of personal data and govern the resolution of location data within certain limits. Location data, published in various location servers, can be securely transferred only to authorized users following a successful authentication.

Since the Geopriv location server can regulate the spatial resolution of location data, the system can be used to introduce an element of noise into private data. However, since technology alone cannot manage privacy (Schilit et al., 2003), the Geopriv system is not in itself, a total solution. Rather it provides a basic architecture upon which more powerful and flexible systems can be built (e.g. see (Gunter et al., 2004)). Geopriv is still a work in progress and as such still needs to undergo rigorous evaluation in realistic trials.

Gunter et al. (2004) describe how Personal Digital Rights Management (PDRM) can be used to express personal data (and corresponding policies for the use of such data). PDRM is akin to Digital Rights Management (DRM) used to protect intellectual property from piracy. With PDRM, personal data owners are able to license their private information. The proposed PDRM model uses eXtensible rights Markup Language (XrML) to express privacy rights and uses P3P to encode XrML contracts. A typical contract consists of the following:

- The identity of the mobile device being tracked;
- The user/subject of the location data;
- The party receiving rights on the location data;
- The validity period of the contract;
- The P3P privacy policy;
- A list of acceptable actions;
- The digital signature of the user/subject.

We propose to apply our privacy preference model to the EMAPP architecture. Systems such as the *pawS* or P3P-based models have a limitation to the extent that, once access is granted to the use of personal data, this data may flow out or copied from the original location (privacy proxy) to a different location such as the service proxy. Data passed on to a service proxy may then be used improperly after expiry of authorised use or copied from the service proxy by unauthorised third parties (Yamada & Kamioka, 2005).

Fig. 1 below demonstrates that our proposed privacy preference model is a complement to the model proposed by Yamada & Kamioka (2005). The key components of our model are:

1. The inclusion of noise (anonymising, cloaking, blurring, encryption, and lying) as a privacy preference;
2. Recognition of the Data Protection Jurisdiction (DPJ) as an important factor in influencing user privacy preferences in a pervasive computing interaction where participants have the freedom to cross regulatory borders;
3. The need to cater for mismatches between the privacy preferences of users and the privacy policies of pervasive services provided by governments or private organisations.

To illustrate the model, consider the following scenario.

Bob (resident in the United Kingdom) uses his mobile device for various services, some of which are government services (e.g. paying local taxes), whilst others are the commercial location-based services such as friend finder or interactive tour guide (or place finder).

Bob has just arrived from the US where he felt it necessary to set very strict privacy preferences as some measure of protection against the relatively low levels of privacy protection offered by legislation. The UK offers relatively strong privacy protection legislation that also considers location information.

In the UK Bob's mobile agent (which has encoded DPJ privacy laws for each of the four major regulatory regimes mentioned earlier) adjusts his privacy preferences to reflect the laws of the UK.

Bob's mobile agent avoids *false positives* whilst trying to access services in the UK whose privacy policies presumably obey the strong regulatory laws. False positives occur when an unnecessary alarm is triggered for an event which should be considered privacy-friendly or privacy neutral. Bob might want to anonymously access a local council service via his mobile device, but he should be able to do so without compromising privacy preference settings that block targeted advertisements from retailers.

Whilst accessing a service, the mobile agent migrates into the privacy capsule and executes the relevant rules for use of personal data. User privacy preferences are then compared with the privacy policy of the service. If there is a match, then it is presumably safe to exchange personal data and access the service. In the case of a mismatch, our proposed model uses the idea of an *economic trade-off* originally proposed by Acquisti (2002). This model generally defines the utility of completing a transaction (which may or may not involve the release of personal information) as a function of the expected benefits of completing the transaction; the expected benefits of maintaining private information; their associated probabilities of occurrence, and the cost of using a particular technology, which may or may not be a privacy enhancing technology. However, "*because privacy intrusions are very specific and very much context-dependent*, Acquisti's *abstract model has to be "calibrated" for specific scenarios"*(Acquisti, 2004) within our model.

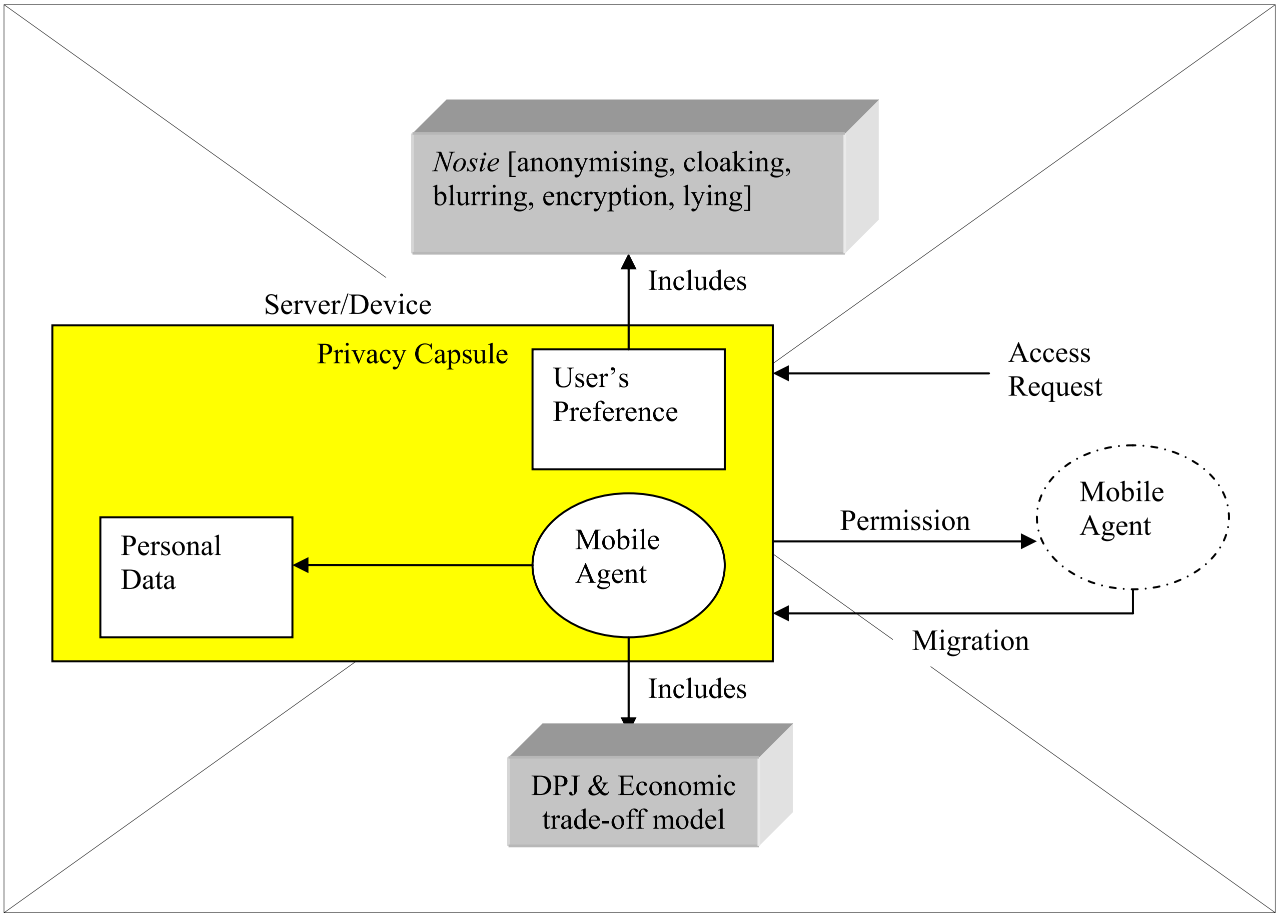

Fig. 1:Modified EMAPP Architecture (adapted from (Yamada & Kamioka, 2005))

Using Topiary (Li et al., 2004), we were able to quickly design, prototype, and test our scenarios and key components described above. Topiary is a tool for prototyping location-based applications. With Topiary, designers are able to create a map that models the location of places, people, and things. The map is used to demonstrate scenarios that depict location contexts. Thereafter, these scenarios are used in creating storyboards to describe interaction sequences and then run the storyboards on mobile devices like PDAs. We have performed a number of heuristic walkthroughs with experts to test our design, details of which are found in (Price et al., 2005).

5 Conclusions and Future Work

In this paper, we have presented a privacy preference model designed for pervasive computing environments. We have shown that the range of legal regimes is such that a user should not, indeed *cannot*, be expected to understand an ever-changing regulatory environment. We have suggested a model where some understanding of relevant regulatory regimes is coded into a privacy-protecting proxy; users need only express their own privacy policy for an appropriate action to be taken under a given regulatory regime.

Our work contributes a privacy preference model accommodating regulatory regimes, as well as various forms of noise, such as cloaking, blurring, anonymity or pseudo-anonymity, hashing or encryption, and lying.

Ultimately, ubicomp take-up depends on privacy protection being made both trusted and usable. Our model is capable of providing high levels of protection from both invasive technologies and from fellow users, and represents an important step along this road.

Like many pervasive computing applications, usability issues are not readily soluble since evaluation is a difficult task at the conceptual phase. Therefore, we are currently undertaking a survey to determine which heuristics will be appropriate in order to create a heuristic walkthrough of our design. Furthermore, we are looking at extending existing evaluation frameworks for 3G m-government applications. Thus far, our designs have only been tested in the laboratory; our next step will be to undertake user evaluation trials of our design on live mobile devices.

6 Acknowledgements

We will like to thank Prof. Yamada Shigeki for his support with information on the EMAPP (as it was difficult translating the original Japanese version). We are also grateful to Prof. Alessandro Acquisti (for his clarification of the economic trade-off model), and Dr. Yang Li (for his tips on using Topiary to effect lying).

7 References

3G-UK. (2003). *European Mobile Ownership Saturation*, available from: http://www.3g.co.uk/PR/July2003/5619.htm

Abie, H., Foyn, B., Bing, J., Blobel, B., Pharow, P., Delgado, J., Karnouskos, S., Pitkanen, O., & Tzovaras, D. (2004). The need for a digital rights management framework for the next generation of e-government services. *Electronic Government, 1*(1).

Ackerman, M. S. (2004). Privacy in pervasive environments: next generation labeling protocols. *Personal Ubiquitous Comput, 8*(6), 430-439.

Acquisti, A. (2002). *Protecting Privacy with Economics: Economic Incentives for Preventive Technologies in Ubiquitous Computing Environments.* Paper presented at the Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, UbiComp 2002.

Acquisti, A. (2004). Personal Communication.

AT&T. (2003). *Privacy Bird*, available from: http://www.privacybird.com

Beresford, A. R., & Stajano, F. (2003). Location Privacy in Pervasive Computing. *IEEE Pervasive Computing, 2*(1), 46-55.

Bronski, D., Chen, C., Rosenthal, M., & Pluscec, R. (2001). FTC VS. TOYSMART. *Duke Law and Technology Review, 0010.*

Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). *Location Disclosure to Social Relations: Why, When, & What People Want to Share.* Paper presented at the Conference on Human Factors in Computing Systems, CHI 2005, Portland, Oregon, USA, (to appear).

Cranor, L. (2002). *Web Privacy with P3P*. Cambridge, MA: O'Reilly & Associates.

Cranor, L., Langheinrich, M., & Marchiori, M. (2002). *A P3P Preference Exchange Language*, available from: http://www.w3.org/TR/P3P-preferences/

Cuellar, e. a. (2004). *Geopriv Requirements - Request for Comments: 3693*, available from: http://www.ietf.org/rfc/rfc3693.txt

Electronic Privacy Information Center. (2000). *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy*, available from: http://www.epic.org/reports/prettypoorprivacy.html

Globallocate.*Everything you want to know about E911 and E112*. Retrieved 21/04/2005, available from: http://www.globallocate.com/RESOURCES/RESOURCES_MAIN_f3.htm

Gruteser, M., & Grunwald, D. (2003). *Anonymous usage of Location-Based Services Through Spatial and Temporal Cloaking.* Paper presented at the First International Conference on Mobile Systems, Applications, and Services.

Gunter, C. A., May, M. J., & Stubblebine, S. G. (2004). *A Formal Privacy System and its Application to Location Based Services.* Paper presented at the Workshop on Privacy Enhancing Technologies, Toronto, Canada.

Hong, J. I., & Landay, J. A. (2004). *An Architecture for Privacy-Sensitive Ubiquitous Computing.* Paper presented at the Proceedings of the 2nd international conference on Mobile systems, applications, and services, Boston, MA, USA, 177 - 189.

Jiang, X., Hong, J. I., & Landay, J. A. (2002). *Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing.* Paper presented at the Fourth International Conference on Ubiquitous Computing, Goteberg, Sweden.

Langheinrich, M. (2002). *A Privacy Awareness System for Ubiquitous Computing Environments.* Paper presented at the 4th International Conference on Ubiquitous Computing (Ubicomp 2002), 237-245.

Li, Y., Hong, J. I., & Landay, J. A. (2004). *Topiary: A Tool for Prototyping Location-Enhanced Applications.* Paper presented at the UIST'04: Symposium on User Interface Software and Technology, Santa Fe, New Mexico, 24-27 October, 217-226.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM, 38*(12), 65-74.

Price, B. A., Adam, K., & Nuseibeh, B. (2005). Keeping Ubiquitous Computing to Yourself: a practical model for user control of privacy. *To appear in the International Journal of Human-Computer Studies*.

Schilit, B., Hong, J., & Gruteser, M. (2003). *Wireless Location Privacy*, available from: http://www-2.cs.cmu.edu/~jasonh/courses/ubicomp-f2004/papers/16-r12invi.lo.pdf

Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., & Polk, J. (2004, November 28). *A Document Format for Expressing Privacy Preferences for Location Information* [Internet Draft]. The Internet Society. Retrieved 26 January, 2005, available from: http://www.ietf.org/internet-drafts/draft-ietf-geopriv-policy-05.txt

Sharma, S. K., & Gupta, J. N. D. (2004). Web services architecture for m-government: issues and challenges. *Electronic Government, 1*(4).

Yamada, S., & Kamioka, E. (2005). Access Control for Security and Privacy in Ubiquitous Computing Environments. *IEICE Transactions on Communications, E88-B*(3), 846-856.