A Formal Privacy System and its Application to Location Based Services[*]

Carl A. Gunter and Michael J. May, University of Pennsylvania
and Stuart G. Stubblebine, Stubblebine Research Labs

Abstract. *There are a variety of well-known models for access control developed for purposes like formally modeling the access rights on files, databases, and web resources. However, the existing models provide an inadequate representation of a number of concepts that are important when modeling privacy rights in distributed systems. We present an analog of the access control matrix designed to model such concepts. Our formalism, which we call a* privacy system*, empashizes the management of data and actions that affect the privacy of subjects. We motivate privacy systems, describe them mathematically, and illustrate their value in an architecture based on* Personal Digital Rights Management (PDRM)*, which uses DRM concepts as a foundation for the specification and negotiation of privacy rights. This illustration is carried out throuh a case study of a privacy-respecting system for location based services. Our prototype, which we call* AdLoc*, manages advertising interupts on PDAs based on their location as determined by WiFi sightings in accordance with contracts written in the DRM language XrML.*

1 Introduction

Privacy is a pivotal concern for data collected by and stored on computers. A variety of formal models have been proposed to characterize privacy based on cryptographic and information-theoretic critera, providing a rigorous definition of privacy. A closely related class of formal models formulate access control rules, which describe the rights of principals to perform actions and access data. These provide an abstract architectural perspective on privacy that can be supported by cryptographic techniques. Portions of what is needed are present in various formalisms. For instance, access control matrices provide an intuitive and fundamental model of the relationship between prinicipals, objects, and rights. Trust management systems provide a foundation for delegation, credentials, and decentralized operation. Role-based systems provide efficient ways to manage the relationship between principals and rights. However, the existing systems fall short on important issues like direct representation of the idea that data are *about* a specified principal whose privacy is at issue. They also fail to integrate the right range of basic concepts. The aim of this paper is to propose an analog of an access control matrix primarily aimed at the representation and management of

[*] Appearing in Privacy Enhancing Technologies (PET) 2004

privacy rights. This entails the problems of representing, negotiating, delegating, and interpreting rights in a distributed context. We make three contributions: a formal system as a conceptual aid for analysis and design, an architectural approach to enable development based on common software platforms, and a case study to illustrate its characteristics and prove its scalability.

Our formal system, which we call a 'privacy system', describes an abstract concept of rights of principals to create and manipulate objects related to a principal which we call the 'subject' of the object. While existing models often include the concept of an owner of an object, the concept of privacy relating to an object is different in subtle respects such as the ways in which rights flow from the wishes and legal rights of the subject even when the subject no longer has access to the object (indeed the subject may never have had access to the object). A privacy system is similar to an access control matrix, but differs in several key respects. It is an abstract representation of a distributed system where enforcement concepts like a reference monitor (which inspired much of the early work on access control matrices) are unrealistic. It only indirectly deals with the rights of principals on objects, focusing instead on the rights of principals on other principals. The primary concept of interest is the ability of one principal to enter with another into an agreement that affects the privacy of a third. The system is formulated to enable the composition of simple kinds of rights into more complex ones and to facilitate standard representation with XML syntax. This enables easy implementation and clean interpretation of the syntax used to describe abstract rights.

Our architecture is based on the representation of privacy systems using *Personal Digital Rights Mangement (PDRM)* as a foundation for negotiations. Digital Rights Management (DRM) refers to the specification techniques and enforcement mechinisms being developed by vendors of intellectual property to protect intellectual property from piracy. PDRM uses the same mechanisms to enable individuals to license their private data. So, if DRM can be used to specify that a piece of music can only be rendered 10 times from a single processor, then PDRM can specify that a private telephone number can only be used once for a specific purpose. DRM requires an extensible foundation to deal with diverse kinds of intellectual property in various sectors (ebooks, digital music, movies, *etc.*). The industries in these sectors have focused significant effort on designing a suitable framework. This framework provides a tantalizing fit with privacy rights, which must also deal with a wide range of sectors (medical, financial, *etc.*). Our prototype approach is based on the use of the XrML digital rights language with negotiated privacy rights derived from specific sectors. For instance, we will show how P3P, a specification technique for privacy on the World Wide Web, can be incorporated in XrML contracts.

Our case study is our most detailed example of how to apply our theory and architecture. In the near future, a collection of devices and protocols will provide location information about the growing number of people who carry them. In particular, triangulation of cell phones, GPS satellite services (especially in vehicles), and information based on DHCP (especially for WiFi), will open a new range of interesting *Location-Based Services (LBS)*. They will also raise a wide range of privacy issues. Emerging architectures for these location-based services will ideally provide substantial individual control. This will entail a new level of user configuration for the location-reporting mobile embedded devices. Software that respects privacy requirements will be a crucial aspect of design for mobile embedded systems for consumers. We built a prototype privacy-respecting system for LBS based on WiFi sightings where the service is interupts on a PDA by advertisers. The idea that an advertiser could, say, pop up an advertisement on your PDA based on your location is, in the current spam-infested computing environment, almost a nightmare. However, consumers might want this for the right advertisers. This makes it an interesting case study in privacy enhancing technology. Essentially our system provides protocols for establishing a collection of rights that enables the target of the advertising to control access and protect her privacy to the degree she chooses, while the service providers will have digital licenses that show their rights to perform interupts on the user device for specified purposes and at permitted times, and that they retain the data only in accordance with rules agreed with the subject.

The paper has six sections. In Section 2 we summarize some of the literature related to formal models of privacy and access control and describe our approach within this context. In Section 3 we analyze the idea of using access control matrices as a model of privacy and discuss shortcomings for this purpose of a well-known example of an access control matrix system. In Section 4 we introduce a formal access control system that focuses on privacy. In Section 5 we carry out our case study for the use of PDRM to develop a privacy-protecting architecture for an LBS system for advertising on PDAs based on WiFi sightings. We then provide a brief conclusion.

2 Related Work

Early approaches for modelling protection systems include those by Graham and Denning [8], Lampson [10], and Harrison, Ruzzo, and Ullman [9]. A recent area of interest is trust management, which concerns checking authorization of unknown users [3] and there are attempts to connect these approaches [11]. DRM is a related area that focuses on managing access to disseminated digital content like music, movies, and text. The Open Digital Rights Language (ODRL) (`odrl.net`) and the eXtensible rights Markup Language (XrML) (`www.xrml.org`) typify work in this area. Usage CONtrol (UCON) [12] strives to unify the areas of access control, trust management and digital rights management.

This paper makes a similar attempt to unify these diverse areas, but we focus on the expression of privacy rights as the driving application and take what seems most needed from access control, trust management, and DRM. We aim to create a system that could, for instance, formalize standards for protecting the privacy of individually-identifiable health information [6]. Our formalisms describe mathematically the kind of transformations and access control decisions that must be made in managing such private patient information. Our architecture has elements in common with the Platform for Privacy Preferences [17], an effort to standardize privacy policies on the web. P3P is a browser-centric standard designed to put web site privacy policies in a machine readable format. A P3P Preference Exchange Langauge (APPEL) (`www.w3.org/TR/2002/WD-P3P-preferences-20020415`) enables users to prespecify their perferences so they can be matched against policies used by web sites. This language has received criticisms from many privacy activists [4, 5, 15] for being unenforceable and vague. Another related effort is the Enterprise Privacy Authorization Language (EPAL) (`www.zurich.ibm.com/security/enterprise-privacy/epal`) which provides an XML-based language for specifying privacy rules. Both P3P and EPAL can be used in connection with our formalism, architecture, and applications. We focused on the use of P3P in the study in this paper. Titkov *et. al.* [16] describe a similar system for privacy-respecting location aware services based on a broker agent architecture, persistent pseudonyms for each user, and P3P. We model the rules for private data transmission and manipulation more formally, introduce the notion of an explicit digital contracts between parties, and introduce the transmission of "fuzzy" location information rather than an all-or-nothing approach.

Our case study focuses on interupt rights based on Location Based Services. The notion of selling interrupt rights for the purpose of controlling unwanted e-mail and telephone calls is studied in [7]. Fahlman's notion of controlling interrupt rights by forcing micropayments on unrecognized parties is interesting, but requires some significant revamping of the phone and email systems. In our design we hope to create a deployable system by relying in part on the effectiveness of audit and non-technical enforcement mechanims like the National Do Not Call Registry (`www.donotcall.gov`) or the legal protections associated with HIPPA.

There have been a number of legal studies related to interupt rights. Warren and Brandeis [18] famously formulate privacy in terms of the "right to be let alone". Their discussion of the right of a person to prevent unauthorized photographs from public circulation has many interesting parallels with modern discussions of location privacy. More recently, in the 108th Congress, HR71 [2], the "Wireless Privacy Protection Act of 2003," sought to require wireless providers to receive explicit approval from users before location information, transaction informatoion, and other kinds of data could be used. The bill also required that the wireless carriers "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the information." With specific regard to wireless messaging, HR122 [1], the "Wireless Telephone Spam Protection Act," also from the 108th Congress, sought to place a ban on unsolicited commercial messages on text or graphic based wireless devices. It is unclear whether either of these bills will ever become law, but the inclination in government towards providing protections for location information and wireless messaging is clear.

The area of location privacy management has begun to develop, but still is lacking consensus, maturity, and theoretical and mathematical analysis.

The geographic location and privacy (geopriv) working group (www.ietf.org/html.charters/geopriv-charter.html) of the Internet Engineering Task Force (IETF) (ietf.org) has made some suggestions for how location information objects should be made and privacy policies formulated. The Geopriv system is based on XML and focuses on access rules and the creation of a trusted location server. Its goal is to allow people to let others track their location through location (data) objects that they publish while maintaining some user controls. Users define rules both on the location server and embedded in the location object that restrict how the data can be redistributed and retained and how accurate the information released to specific recipients is. Geopriv's goal is a set of languages and protocols that allow users to publish their location information on particular servers, have those servers securely distribute location information to authorized individuals, and maintain control over how others use the geolocation data.

The geopriv model is still evolving and most of its documents are works in progress. Its requirements document (already a standards track document in IETF) describes an architecture for running a location information management system. We borrow much of their architecture, but contribute a formal analysis of how information is distributed and collected, offer a richer model of rights and responsibilities, and suggest a manner to negotiate and compose different privacy policies. The access control/permissions model [13] being developed by geopriv is based on rule sets. We offer a contract-based system that is more powerful and flexible with respect to describing usage rights, object transformation policies, and controlling data retention.

Another location privacy system [14] provides a language for writing geolocation privacy preferences as well as an architecture that supports those rules. The focus is on designing a language that can be modelled mathematically and reasoned about formally, rather than one that is ready for immediate implementation. These assumptions result in a system that is less complex and more general than the Geopriv system described above. The language views location objects as having a lattice ordering determined by accuracy and traceability. This lattice structure is a convincing way of viewing the accuracy of location objects and identity, but stops there. We provide methods to express purpose, retention, usage, creation, and transfer rules. We borrow from this work the idea of object accuracy ordering when modelling the transformations that are done on objects before they are transferred between parties.

3 Background

The concept of an access control matrix is one of the oldest formalisms for describing access rights. The basic idea is to create a matrix indexed by principals $\mathcal{P}$ and objects $\mathcal{O}$. This is a function $R : \mathcal{P} \times \mathcal{O} \to \Sigma$ where Σ is a space of rights. For instance, we might have $\Sigma = \{r, rw, rwx\}$ for read-only, read/write, and read/write/execute rights. The matrix R provides an elegant abstraction: it describes the boundaries of a principal's ability to act on an object without the details about other constraints on this interaction. That is, it can indicate that principal p can execute object x without describing whether the actions of p will, in fact, execute x. This form of access control matrix is too simple for some purposes. In particular, it does not describe relationships between principals, such as whether one principal created another (if principals are like processes) or gave it access to the system (if principals represent users). It also does not by itself describe the events that cause its entries to change, such as the idea that a principal transfers a right on an object to another principal.

3.1 Graham/Denning Model

An early example of an extended access control matrix model that incorporates some of the key concepts related to events and constraints is the Graham/Denning model [8]. In this model, the access control matrix is a partial function $R : \mathcal{P} \times (\mathcal{P} + \mathcal{O}) \rightarrow \mathsf{pwr}(\varSigma)$ where pwr denotes the powerset operation. The space $\varSigma$ is defined over a primitive set of access rights $\varSigma_0$ augmented with a few additional expressions. If $\sigma \in \varSigma_0$, then $\sigma*$ is a right to transfer σ as well as perform it. Distinguished rights include the idea that a principal is the owner of an object or that one principal has control over another. These rights govern a sequence of allowed events that describe the ability of principals to manipulate the rights on principals and objects. Events may be disallowed if the appropriate rights are not present. The following sequence of events illustrate the Graham/Denning model. We assume an initial principal p that creates other principals, which, in turn can create their own descendants.

1. p **creates** q; q **creates** r; q **creates** x. These events create two principals and an object. $R(p, q)$ and $R(q, r)$ are set to $\{$control$\}$ and $R(q, x)$ is set to $\{$owner$\}$.
2. q **grants** $\sigma*$ **to** q **on** x. This creates a transferable right for q on x which is entered into $R(q, x)$. This is allowed because q owns x.
3. q **transfers** σ **to** r **on** x. This transfers the right σ to r for the object x setting the value of $R(r, x)$ to be σ. This is allowed because q has the right $\sigma*$ which allows it to transfer σ.
4. q **creates** s. Now $R(q, s)$ is $\{$control$\}$. Table 1 describes the state of the access control matrix R after this step.

Table 1. Sample Access Control Matrix

	p	q	r	s	x
p		control			
q			control	control	owner, $\sigma*$
r					σ
s					

5. r **transfers** σ **to** s **on** x. This is disallowed because the right of r is not transferable.
6. p **deletes** σ **of** r **on** x. This is disallowed because because p does not own x or control r.
7. p **deletes** r. This is disallowed because p does not control r.
8. p **deletes** q. This removes q from the access control matrix. It is allowed because p controls q.

A model of this kind improves on the basic access control matrix by adding relationships between principals and the effect that this has on the delegation of rights. It provides a useful basis for thinking about the management of access rights and the enforcement of these rights using an reference monitor. This provides a useful model of multi-user time-sharing systems.

3.2 LBS Scenarios

To analyze the suitability of an access control system like access control matrices as a model of privacy let us review it for use in an application space with rich privacy issues. For this paper we have chosen to focus on privacy associated with geo-location and LBS. Let us now turn to a collection of examples that illustrate the challenge. We identify three general classes of principals. First, there are the principals on which geo-location data is collected. Although these will typically be computers the data often gains its relevance because of its association with a human principal. Such prinicpals have interests in the privacy of the information that is collected. Let us refer to such principals as *subjects*. A second class of principals collects information about *sightings*, that is, they obtain information that a subject was at a location at a given time. Let us call these principals *holders* of geo-location data. A third collection of principals exploit location information to provide services. These principals can be called *providers*, but they may also play a role as *subscribers* to the data of the holders. They may provide a service to the subject, the holder, or some other party. Here is a collection of examples of these kinds of parties.

Subjects Individuals concerned about privacy: Alice, Bob, Claire, Dan, *etc.* The devices that generate their location data: Alice's cell phone, Bob's GSM-equipped car, Claire's laptop making WiFi Internet connections, Dan's active badge, *etc.*

Holders Principals willing and able to collect location information on entities with tracking capacity through sightings.

- *CellTrek* is a cellular provider that collects sightings using cellular triangulation based on the handsets of its subscribers.
- *Autorealm* is a telematics system for automobiles that tracks automobiles using GPS.
- *Canada On Line (COL)* is an ISP that tracks the locations of Internet connections made by its users based on information such as WiFi sightings.

– *Spartan Chemicals* is a complex of chemical plants where user movements are tracked in their facilities through the use of RFID tags.

Subscribers Providers of location based services based on collections of sighting information.

– *Friendsintown.com* correlates sightings using a kind of buddy system. These correlations are used to inform buddies if they are in the general vicinity of one another to facilitate a friendly get-together. For instance, Alice and Claire may be old college friends who travel frequently on business and like to get together for dinner if they are in the same city. Bob and Dan are computer science researchers working on similar problems and like to get together ahead of meetings if they are at the meeting site early.
– *Market Models* supplements geo-location information with demographic information from subscribers to produce statistical GIS information. For example, Market Models might have a profile of the incomes of individuals in Penn Station at noon. Market Models may have a model of how far from home a driver is when he passes a given restaurant on an interstate highway.
– *What's Here!* provides information to a PDA about the place where the PDA is currently located. What's Here provides a continuously updated map with a 'You Are Here' pointer on it. What's Here also uses context to determine likely interests of the holder. For instance, when a tracked subject enters the Penn Computer Science building, it provides a listing of the public seminars being held that day.
– *Travel Archive* keeps long-term records of travel for archival purposes such as long-term data mining or entertainment. For instance, SalesRUs uses travel archive to provide general information about its travel trends over time such as the average length and time of trips by its employees. Claire uses Travel Archive to keep long-term records of her travels so she can review family trips over the years (Did we visit Mother for Christmas in the year when Father died? Where was I when the Berlin Wall fell?).

3.3 Privacy in LBS

Let us now consider the privacy issues entailed in our complex of subjects, holders, and subscribers. It must first be noted that the distinctions are not at all rigid. For instance, a subject could hold location information about himself, holders may provide services themselves or subscribe to other holders, and subscribers like Travel Archive are clearly holders in their own right. However, a dominating feature of the scenarios is the fact that location information is typically data *about* a subject and this subject may well consider its use to affect her privacy. Arrangements to manage this privacy may take a variety of forms.

Several of basic LBS scenarios involve operations similar to the ones in the Graham/Denning model. For instance a principal may set a right on a location object so that another principal can read it. This looks like a typical operation on a time-share OS where an owner sets a permission on a file so another user can read it. However, it is an operation only indirectly involved in a typical scenarios for privacy management in these LBS systems. A more fundamental issue is the form and meaning of the contract between principals p and q that says q has the right to carry out sightings of p and report this data to a third principal r.

We classify the primary operations and relations of a privacy system as follows:

Transfer What is the right of a principal p to transfer an object x to a principal q where x is about a subject r? This depends on rights of both p and q relative to r and features of x. For example, Autorealm may have the right to obtain very accurate information about the position and direction of Bob, but when this information is reported, with Bob's permission, to friendsintown.com, it should be reported with only metro-area accuracy. COL is only permitted to retain and transfer location information about Alice within a few minutes of its creation, but, once this information has been transfered to Travel Archive, it is retained as long as Alice continues her subscription with Travel Archive and can be transfered to Alice at any time during that subscription. Spartan Chemicals may be concerned about a security breach and transfers location information about Dan's active badge to the FBI, which does not offer Dan a subscription to see this data. Market Models is unable to obtain Dan's information from Spartan Chemicals, but Dan was happy to provide similar information through CellTrek in exchange for a reduction in his cellular bill. However, CellTrek cannot reveal his name in the location information it transfers to Market Models.

Action What is the right of a principal p to carry out an action that affects the privacy of a principal q? This depends on the policy of p. For instance, friendsintown.com has a right to send email to Alice and Claire telling them someone on their buddy list is in town. Alice and Claire gave friendsintown.com this right. Spartan Chemicals has a right to question Bob about his reasons for being in a given location reported by his active badge. His employment contract gave this right to them.

Creation Which principals p are allowed to create objects x whose subject is q? The right to create objects may be held by the subject only. For instance, Bob's telematic auto system may store location information in Bob's car, but Bob may choose to transfer this to Autorealm for various purposes. In other cases, the holder creates the object and it may not be directly available to the subject, as in the case of Spartan Chemicals. The right to create objects may exist for only a limited period of time. For instance, Claire might offer this to COL for a trial period of one month in order to explore the value of the service offered by What's Here!

Right Establishment How are rights established for a principal p? For instance, Spartan Chemical may have an understanding with Dan that his location information may be passed to law enforcement officials as part of an ongoing investigation at the plant. The right of Spartan Chemicals to set a right for the FBI may derive from the rights they established with Dan.

> The right of Market Models to convey information derived from objects of Claire may derive from their rights as negotiated with COL, which, in turn, are related to the rights they established with Claire.

3.4 Limitations of Graham/Denning

Let us now consider some of the limitations of the Graham/Denning model with respect to the kinds of needs one infers from the requirements for privacy in LBS systems. Applying the model encounters the following limitations:

1. There is no explicit representation of the idea that an object is private data about a given subject.
2. There is only a limited analysis of the rights that exist between principals (as opposed to the rights between principals and objects).
3. There is no explicit representation of the way in which the objects are transfered (distributed) between the principals.
4. The concept of delegation is too limited.
5. There is no explicit representation for the idea that information transfers and actions are collaborations between principals.
6. There is no concept of the transfer of an object after a privacy-enforcing transformation.

Some of these can be addressed by an encoding, while others require an extension. Our system, which is described in the next section, deals with these limitations by focusing on a general view of abstract rights between subjects and the four operations and relations described above.

4 Privacy Systems

Assume we are given the following three spaces: *objects* $x, y, z \in \mathcal{O}$, *principals* $p, q, r \in \mathcal{P}$, and *actions* $a, b, c \in \mathcal{A}$. Let us model time as non-negative real numbers $t \in \Re$. Each object is assumed to have an associated *subject* $\mathsf{subj}(x) \in \mathcal{P}$, and an associated *creation time* $\mathsf{ct}(x) \in \Re$. We also assume that there is a distinguished *null object* $\bot_{\mathcal{O}} \in \mathcal{O}$ and a distinguished *null principal* $\bot_{\mathcal{P}} \in \mathcal{P}$ where $\mathsf{subj}(\bot_{\mathcal{O}}) = \bot_{\mathcal{P}}$ and $\mathsf{ct}(\bot_{\mathcal{O}}) = 0$.

Definition 1. *A privacy system is a tuple*

$$\langle \Sigma, T, U, V, W \rangle$$

where

- Σ *is a set of rights and* $\bot_{\Sigma} \in \Sigma$ *is a distinguished null right,*
- $T : \Sigma \times \Sigma \times \mathcal{O} \times \Re \to \mathcal{O}$ *is a publish/subscribe rights function,*
- $U \subseteq \Sigma \times A \times \Re$ *is an action rights relation, and*
- $V \subseteq \Sigma \times \mathcal{O} \times \Re$ *is a creation rights relation.*
- $W \subseteq \Sigma \times \Sigma \times \Sigma \times \mathcal{P} \times \Re$ *is a right establishment relation.* □

The intuitive explanation of the functions and relations in a privacy system $\langle \Sigma, T, U, V, W \rangle$ is as follows:

- $T(\sigma, \sigma', x, t)$ is a transformation of the object x that is determined by the policy σ of its publisher, the policy σ' of its subscriber, and the time t at which the subscriber receives the object. In some cases the value of the function will be a modified version of x that removes pre-specified types of sensitive information. If the policies of the publishing and subscribing parties accomodate full transfer, then the object x will be the value of this function, but in cases where the transfer is entirely disallowed, the value may be $\bot_{\mathcal{O}}$.
- $U(\sigma, a, t)$ indicates whether the right σ allows the action a at the time t. An action is usually based on a particular principal or object but the effect of an action is not described by the system.
- $V(\sigma, x, t)$ indicates whether σ allows the object x to be created at time t. The source of the object x is not described by the system. Typically it is obtained from an observation made by the creator.
- $W(\sigma_1, \sigma_2, \sigma_3, p, t)$ indicates whether a principal with the right σ_1 can, at time t, endow the right σ_2 to a principal with right σ_3 with respect to the objects of subject p. This will typically depend on the rights that the party endowing the rights has on the objects of p.

An informal example may be helpful before proceeding with further formalisms. Suppose Σ is a set of rights that indicate the right of a physician to collect and share the medical records of a patient. The relation W will indicate that a patient can endow upon a physician the right to collect and share data about the patient. The relation V will describe the right of a physician to create objects with the patient as their subject, by running tests for instance. The relation U will indicate that a physician may act in a certain way upon the medical information of a patient, by enacting a treatment, for instance. The effect of the treatment and whether the treatment is justified by the patient data are viewed as external to the privacy system.[1] The function T will indicate the right of the physician to share information with others. For instance, the physician may be able to share information about the patient with his partners without changing the object. The physician may be able to supply the object for research if it is transformed to protect the privacy of the patient. This may be done by changing the subject of the object to the null subject or by some more sophisticated technique.

The functions and relations in a privacy system are very general and cover quite a range of possibilities. For example, it is straight-forward to model the idea that a patient has a right that allows her to revoke the right of the doctor to create or distribute objects about her after a given time. To understand how

[1] The physician may have a right to prescribe a drug, but choose not to do this because of its potential side effects. The basis for this decision is not modeled by the system. On the other hand, the system may model the idea that the physician does not have a right to impound the automobile of the patient, regardless of the results of his tests. Another party, such as a bank, may have rights to this action.

we model actions of this kind, we need to introduce the concept of an event sequence.

The concepts of publishing, subscribing, creating, establishing policies, and acting upon objects are modeled using a labeled transition relation over an assignment of objects and policies to principals. A *state* is a pair $S = \langle H, R \rangle$ consisting of a *holder state* $H : \mathcal{P} \rightarrow \mathsf{pwr}(\mathcal{O})$ and a rights matrix $R : \mathcal{P} \times \mathcal{P} \rightarrow \Sigma$. For each principal p, the set $H(p)$ represents the objects that p has obtained by direct observation or by subscription. The right $R(p, q)$ is the right of p with respect to the privacy of q. Four kinds of events are related to changes in this state.

1. A *set policy event* is a tuple of the form

$$p \textbf{ sets } \sigma \textbf{ on } q \textbf{ for } r \textbf{ at } t$$

where p, q, r are principals, σ is a policy, and t is a time.

2. A *creation event* is a tuple of the form

$$p \textbf{ creates } x \textbf{ at } t$$

where p is a principal, x is an object, and t is a time.

3. A *publish/subscribe* event is a tuple of the form

$$p \textbf{ gets } x \textbf{ from } q \textbf{ at } t$$

where p is a principal called the *publisher*, x is an object, q is a principal called the *subscriber*, and t is a time.

4. An *action event* is a tuple of the form

$$p \textbf{ does } a \textbf{ on } q \textbf{ at } t$$

where p is a principal, a is an action, q is a principal and t is a time.

We denote events and the space of events with the notation $e, f \in \mathcal{E}$. In each of the cases for an event e the value t in the tuple is called the *time of* e.

Definition 2. *Let R be a rights matrix over privacy system $\langle \Sigma, T, U, V, W \rangle$. Suppose e is an event and $S = \langle H, R \rangle$ and $S' = \langle R', H' \rangle$ are states. Then we write $S \xrightarrow{e} S'$ if one of the following four cases holds*

*1. $e = p$ **sets** σ **on** q **for** r **at** t. The matrix R' is the same as R except $R'(q, r) = \sigma$. If $p \neq r$ then we must have*

$$W(R(p, r), \sigma, R(q, r), r, t).$$

We say that p, q are the actors in the event and r is its subject.

*2. $e = p$ **creates** x **at** t. The function H' is the same as H on principals other than p, but $H'(p) = H(p) \cup \{x\}$. In this case $\mathsf{ct}(x) = t$. It must be the case that*

$$V(R(p, q), x, t)$$

where $q = \mathsf{subj}(x)$. We say that p is the actor in the event and q is its subject.

3. $e = p$ ***does*** a ***on*** q ***at*** t*. We must have*

$$U(R(p, q), a, t).$$

We say that p *is the actor in the event and* q *is its subject.*

4. $e = p$ ***gets*** x ***from*** q ***at*** t*. We must have* $x \in H(p)$*. The function* H' *is the same as* H *on principals other than* q*, but* $H'(q) = H(q) \cup \{y\}$ *where*

$$y = T(R(p, \mathsf{subj}(x)), R(q, \mathsf{subj}(x)), x, t).$$

We say that p, q *are the actors in the event and* $\mathsf{subj}(x)$ *is its subject.*

A sequence of the form

$$S_0 \xrightarrow{e_1} S_1 \xrightarrow{e_2} \cdots \xrightarrow{e_n} S_n$$

is a valid event sequence if each of the indicated relations holds and, for each $i < n$*, the time of* e_i *is strictly less than that of* e_{i+1}*. In general we will assume that such sequences begin with a value* $\perp_{\text{state}}$ *representing a state in which* $R(p, q) = \perp_\Sigma$ *and* $H(p) = \{\perp_\mathcal{O}\}$ *for each* p, q*.* □

To save the need for writing subscripts, we generally drop the subscripts on $\perp_\mathcal{O}$, $\perp_\mathcal{P}$, and so on when this does not cause confusion.

The intuition behind actors and subjects is that the actors are the parties to a transaction that concerns private information about the subject of the transaction. The actors initiate events through joint agreement subject to the privacy rules they have with respect to the subject of the event.

Note the condition in the set policy event that allows the event p **sets** σ **on** q **for** p **at** t for any values of p, σ, q, t. This means that p is *always* able to negotiate rights on his data with other parties. This provides a somewhat liberal view of private information compared to current practice. By dropping this condition we generalize the system to accomodate the idea that parties must obtain rights to the objects of a subject by other means, as defined by W. This makes the examples below more difficult to describe (since they must describe this mechanism), so, for simplicity, we have restricted our attention to the basic case in which rights originate only from the subjects and can be changed by them at any time. The relation W determines all of the potential propogation of these rights and the operator T determines all ways in which data is transfered based on these rights. This raises issues with at least one of the examples in the previous section. For instance, a holder may not wish to change its right concerning transfering objects to their subject, as was the case with Dan and the FBI. However, if Dan and the FBI mutually agree, the data can be transfered to Dan regardless of any rights that may pertain to Spartan Chemicals.

In general we will be concerned about the question of whether a principal p can obtain (transformations of) objects with subject q *under the assumption* that p cannot create these objects directly but must obtain them by subscribing to a principal that is able to obtain them directly or by another subscription.

Similarly, we will want to ask whether a principal p can perform an action a with respect to subject q. This will be tantamount to asking whether this object can be obtained by p (possibly under the assumption that it cannot be created directly by p) and whether the action is allowed by the action rights of p at the time p wishes to perform the action.

Example 1. (Direct Permissions) Let $\mathcal{P}, \mathcal{A}, \mathcal{O}$ be any sets. The privacy system of *Direct Permissions (DP)* takes $\Sigma = \{\mathsf{dir}, \bot\}$. The value $\bot$ represents no permissions and the value dir represents direct permission. The operator and relations are defined as follows.

1. Define $T(\sigma, \mathsf{dir}, x, t) = x$. For all other arguments the value of T is $\bot$. That is, an object can be passed from one party to another only if the recipient has direct permission.
2. $U(\sigma, a, t)$ iff $\sigma = \mathsf{dir}$. That is, permission to perform action a is given to a principal only if it has direct permission from the subject of the action.
3. $V(\sigma, x, t)$ iff $\sigma = \mathsf{dir}$. That is, objects can only be created by principals with direct permission
4. $W = \emptyset$. That is, subjects must directly grant rights over their objects and actions. □

Proposition 1. *In a DP privacy system only principals with direct permission from* p *can create or obtain objects of* p *or perform an action* a *on* p. □

To illustrate direct permissions, let $\mathcal{P} = \{p_1, p_2, q_1, q_2\}$ consist of a pair of homes p_1, p_2 and offices q_1, q_2. Let $\mathcal{O}$ consist of a collection of telephone numbers, and let $\mathcal{A} = \{a\}$ represent the act of an office calling a home using the home telephone number object. Here is an example of an allowed sequence of events: (1) p_1 and p_2 set their own rights to dir; (2) p_1 and p_2 create telephone objects x_1 and x_2 respectively; (3) p_1 sets the right of q_1 to its objects and actions to dir; (4) p_1 and p_2 transfer their telephone objects to q_1 and q_2 respectively; (5) q_1 telephones p_1. In the second step p_1 and p_2 establish rights to create and call themselves using their telephone objects so $R(p_1, p_1) = R(p_2, p_2) = \mathsf{dir}$. In the fourth step q_1 comes to have $H(q_1) = \{x_1\}$, that is, the telephone object of p_1 is held by q_1. However, q_2 does not have permission to hold the telephone number of p_2 so the transfer of this number to q_2 only causes q_2 to obtain the null object $H(q_2) = \{\bot\}$. A nuance is worth noting: nothing in the privacy system says that q_1 needs the telephone object x_1 in order to call p_1. This is a domain-specific criterion.

Example 2. (Direct Time-Limited Permissions) Let $\mathcal{P}, \mathcal{A}, \mathcal{O}$ be any sets. The privacy system of *Direct Time-Limited Permissions (DTLP)* takes $\Sigma = \{\bot\} + (\{\mathsf{dir}\} \times \Re)$. The value $\bot$ represents no permissions and the value (dir, t) represents direct permission until time t. The operator and relations are defined as follows. We write $\mathsf{dir}(t)$ for (dir, t).

1. Define $T(\sigma, \mathsf{dir}(t'), x, t) = x$ provided $t' \geq t$. For all other arguments the value of T is $\bot$.

2. $U(\sigma, a, t)$ iff $\sigma = \mathsf{dir}(t')$ where $t' \geq t$.
3. $V(\sigma, x, t)$ iff $\sigma = \mathsf{dir}(t')$ where $t' \geq t$.
4. $W = \emptyset$. □

Example 3. (Sharing With Partners) Let $\mathcal{P}, \mathcal{A}, \mathcal{O}$ be any sets and let $\mathsf{partner} \subseteq \mathcal{P} \times \mathcal{P}$ be a symmetric relation between principals. The privacy system of *Sharing With Partners (SWP)* takes

$$\Sigma = \{\bot\} + (\mathsf{dir} \times \mathcal{P}) + (\mathsf{indir} \times \mathsf{pwr}(\mathcal{P})).$$

It is defined in terms of the $\mathsf{partner}$ relation and a restricted set of actions $\mathcal{A}_{\mathsf{indir}} \subseteq \mathcal{A}$. The value (dir, p) represents direct permission to p from the subject and the value (indir, L) represents indirect permission from principals in L. The operator and relations for the privacy system are defined as follows. We write $\mathsf{dir}(p)$ and $\mathsf{indir}(L)$ rather than (dir, p) and (indir, L) repectively.

1. Define $T(\sigma, \mathsf{dir}(p), x, t) = x$ and, if $p \in L$, define $T(\mathsf{dir}(p), \mathsf{indir}(L), x, t) = x$. For all other arguments, the value of T is $\bot$. That is, an object can be passed from one party to another if the the recipient has a permission of 1 or has been given a permission by a partner.
2. $U(\mathsf{dir}(p), a, t)$ holds for any p, a, t and $U(\mathsf{indir}(L), a, t)$ holds if L is non-empty and $a \in \mathcal{A}_{\mathsf{indir}}$. That is, permission to perform action a is given if the permission is direct or a is a restricted action and the permission is indirect.
3. $V(\sigma, x, t)$ iff $\sigma = \mathsf{dir}(p)$ for some p. That is, objects can only be created when the permission is direct.
4. $W(\mathsf{dir}(p), \mathsf{indir}(\{q\}), \sigma, r, t)$ holds if $\mathsf{partner}(p, q)$. If $L' = L \cup \{p\}$ and $\mathsf{partner}(p, q)$, then

$$W(\mathsf{dir}(p), \mathsf{indir}(L'), \mathsf{indir}(L), q, t).$$

   That is, parties with a direct permission can set an indirect permission for their partners. □

To illustrate the SWP, consider financial institutions such as credit card companies that collect records on their customers and releases genearal information and addresses to partner companies with the permission of customers. The customer has also given permission for such institutions to empower its partners with the ability to approach her by direct mail with product and service offerings. In an example series of events, a subject p provides a direct right $\mathsf{dir}(q)$ to an institution q who collects objects of p. Based on these objects, q decides to delegate a right concering p to a partner r who receives objects x of p that lead it to send direct mail advertising to r. A *dis*-allowed sequence might begin with p giving a direct right to q and q attempting to provide an indirect right to one of its (non-partner) competitors. Another disallowed sequence would entail a principal with an indirect right attempting to confer this right on another principal.

Proposition 2. *In an SWP privacy system, only a principals with direct permission from a principal p can perform an action a that is not in $\mathcal{A}_{\mathsf{indir}}$.* □

5 LBS Case Study

The AdLoc location privacy and interruption rights management system mediates the rights of others to interrupt users with advertisements or coupons based on their location.

The system is comprised of a moblie client application, Geographical Location Service (GLS), Geographic Information service (GIS), and an advertising service application. We now describe the system and give an example.

5.1 PDA Application

The AdLoc test bed uses a Compaq iPaq running Microsoft PocketPC OS. All of the code for the program is written in Microsoft's Visual Studio .NET C# compiled for use on the Compact Framework. We used .NET for the prototype system because of its easy to use interface for XML Web Services. For the connection to the outside, a PCMCIA 802.11 wireless card is used. Due to battery limitations we chose to push location data only at certain intervals.

We chose 802.11 for location tracking since most wireless deivces are not yet GPS enabled. However, our architecture fully supports the devices devices obtaining their location from GPS.

5.2 GLS

The Geographic Location Service (GLS) is an XML Web Service that sits on the default gateway for the wireless network. It is coded in Microsoft .NET C# and its interface is XML. Its relative URL is "/GLS/", a location that could become a well known location for all GLS service instances. The requests that the web service accepts have no inbound arguments. Instead it responds to queries in a uniform manner. Its interface and behavior are described below.

- public string GetLoc() -
  GetLoc() returns the GLS's location in a human readable string. Our implemenation returns the city although one might return street address.
- public string GetGIS() -
  GetGIS() sends back IP addresses of Geographic Information Services (GIS) that can manage and distribute location information. Although most users will already have an existing relationship with one or more GIS, but the GLS provides one for those who don't.

5.3 GIS

The Geographic Information Service (GIS) is another Microsoft .NET C# Web Service entity which sits on an always available server. The code has two web service interfaces, one for clients/users and another for location service providers. It acts as the buffer between the two parties, enforcing rights and managing location data contract fulfillment. The GIS maintains lists of active location generating users as well as approved location service providers, so it acts as a central point of contact for many different classes of users.

Even though a particular GIS may have data from users in far flung locations, it may be useful to have certain GISes focus on particular geographic or logical areas. In that situation, a location service provider may discover a targeted audience by just focussing its attention on a particular GIS's user list. For example, a particular airport may maintain a GIS for all travellers waiting inside of it. In that case, an airline wishing to send flight information to waiting passengers might query the local GIS to discover which of its customers are nearby. In this particular case, it would be logical for the GLS on the airport's wireless network to provide the IP address of the airport's GIS as described above.

Since the GIS manages private information, all interactions with it require authentication and all private data is sent over encrypted channels. The facilities of .NET's Web Services tools are used to extensively in managing the X.509 certificates, encryption, and digital signatures required for the secure operation of the GIS. Specifically, all users sign their location object submissions and encrypt them using public key cryptography. Similarly, location service providers identify themselves with X.509 certificates and encrypt their communications with the server with public key cryptography.

Since the GIS manages private user data, it must be careful about who it allows to view its user list. Since GIS presence itself may indicate particular geographic proximity and may reveal information about user habits, only trusted service providers may interact with it. In order for a service provider to gain access to the server it must submit a digitally signed version of its privacy policy. The policy format is described below. If the submitted policy is in accordance with the minimum privacy standards for the GIS, the service provider is allowed access to the user list. This privacy policy is in addition to the digital contract checking that must be done before actions can be done by the service provider.

As part of its role as the buffer between users and service providers, the GIS acts as the facilitator of interrupts on the users. When a service provider has identified a user that it has an interrupt right on, it may send an interrupt message to the GIS to be delivered to the user device. When the user device connects to send new location objects to the GIS, it also accepts new approved strings to be displayed to the user. In our system, the PDA application contains a function to display a notification window on the PDA when new messages are received. When the user clicks on the window the new message(s) are displayed. The GIS is used as a buffer to reduce the potential problem of wireless spam. The PDA initiates all connections with the GIS and has an agreement with the GIS to manage communication rights. With just a single point of contact for all messages, users will have an easy time preventing unwanted messages from flooding them.

5.4 Policy Language

We use a policy language that is a blend of the digital rights language XrML and the World Wide Web Consortium's (W3C) Platform for Privacy Preferences

(P3P)[17] notions. XrML is an expressive and easily extensible language for electronic contracts about digital media. P3P is a language with a comprehensive set of privacy rules, regulations, and enforcement options. Merging them together we achieve a language for contracts that can express rights and obligations about privacy requirements. The exact form of the digital contracts is described below.

The P3P language has constructs that express the privacy rights and obligations, similar to the requirements defined above in the formal semantics for our privacy system. The terms that we focus on in the development of our location data subscription system are as follows:

- Purpose - gives terms describing what kind of purposes the collected data can be used for. By declaring the purposes that the data may be used for, users maintain control over how their data is used by both the data collector and anyone who may acquire the data in the future.
- Retention - gives terms for relating how long the recipient may hold the data. The terms are not absolute terms, only relative terms: No-Retention, Stated-Purpose, Legal-Requirement, Business-Practices, Indefinitely
  With respect to the above defined formalisms, the Retention term in P3P models rules for data retention. Different parties in the system may have different rights of retention of the data, so data may pass from a party who has limited retention rights to one who has longer term rights. The particular limits of the retention rights for a particular party is defined by its contract with the user, not necessarily by the party from whom the data were obtained.
- Recipient - lists the parties who the location data can be shared with. The P3P specification has the following general categories to describe recipients: Ours, Delivery, Same, Other-Recipient, Unrelated, Public.
  With the exception of "Ours", all the categories include parties that have the right to autonomously use the data passed to them in unspecified ways. That looseness has been brought up in critiques of P3P, so when designing and implementing a real world privacy system more specific and well defined terms must be defined.

XrML is a digital rights language created to enforce copyrights and usage rights over proprietary digital media. It allows the creation of machine readable contracts that define specific rights to use and transfer media. We define some special use terms and elements for inclusion in the XrML contracts. Our structures identify contractual parties, digital objects, and rights that may be exercised over them. Contracts in the PDRM privacy system contain the following essential parts:

- Identity of the mobile device being tracked
- The user/subject of the location data
- The party receiving rights on the location data
- Validity period of the contract
- P3P privacy policy

- List of acceptable actions
- Digital signature of the user/subject

Since the contract is only signed by the user/subject, it can be viewed as a release by the user. Thus the contracts enforce the notion that users own location objects and maintain control over who can see them and how the data can be used. Interestingly, P3P was designed with the opposite notion - that companies own the data that they collect and make (non-binding and unenforceable) promises to users about how they plan on using them.

The location system we implemented focuses on interrupt rights [7] based on location information. In particular we describe in contract form the right for a service or company to send advertisements or coupons to a mobile user. We define only a limited set of actions for example purposes, but the language could be made as large as desired.

5.5 Advertising Example

We now describe how all the aforementioned pieces interact to provide a location based advertising/coupon service.

When Alice's PDA loads up the AdLoc software, it checks its adapter list to discover the default gateway. It then queries the gateway at the well known URL for a GLS service. The GLS service responds with its location. The PDA can also query for a listing of nearby or associated GISes.

The PDA creates a location object it sends to the GIS. This action is equivalent to a create $(V(\sigma, x, t))$ action as described above. The GIS allows users to create objects about themselves, so the σ policy here is implicit.

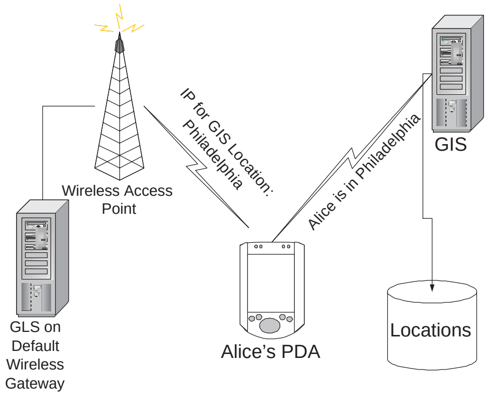


Fig. 1. Registering with the GIS

The GIS retains each of Alice's location objects until a fresher one comes. The AdLoc software on her PDA sends out location objects every few minutes, each new object effectively erasing its predecessors. The GIS erases all location data older than 30 minutes. In summary, its σ can be written abstractly as:

```
<Retain>
    <TimeLimit>
        <M>30</M>
    </TimeLimit>
    <History-Level>1</History-Level>
</Retain>
```

A merchant M-Mart contacts the GIS to discover what PDA users are available. When it queries the GIS, it provides a public key certificate and digitally signs its request. Included in the request is a privacy policy. The GIS checks M-Mart's policy against its default policy to decide to accept or reject the query. If it is accepted, M-Mart's certificate and signed privacy policy are stored in a local database for reference. The GIS sends back a full list of users available, but without their location data, only a pointer to how to contact them by email. At that point M-Mart's σ would look like this:

```
<Access-Level>
    <External-Contact-Info/>
</Access-Level>
```

The transfer of the objects with names and locations removed is a T transformation based on the above definitions.

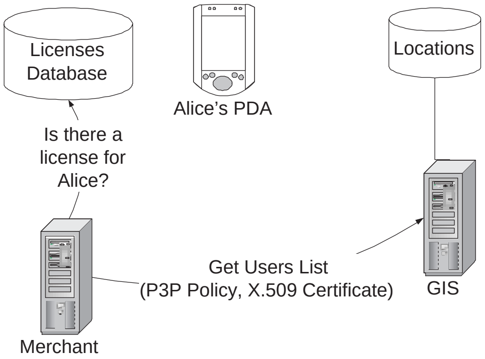
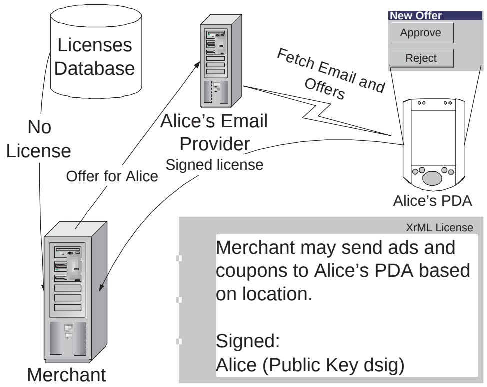

Licenses Database
Alice's PDA
Locations
Is there a license for Alice?
Get Users List (P3P Policy, X.509 Certificate)
GIS
Merchant

Fig. 2. Merchant gathering information from GIS

M-Mart can then contact Alice and ask her for a signed digital contract allowing her to be contacted by PDA to receive coupons. M-Mart then presents that contract to the GIS and asks for more information about Alice's location. After receiving and verifying Alice's signed contract, M-Mart's σ for Alice would look like this:



Merchant may send ads and coupons to Alice's PDA based on location.

Signed:
Alice (Public Key dsig)

Fig. 3. Merchant acquiring license for contact

```
<Access-Level>
    <Name/>
    <Location/>
    <External-Contact-Info/>
</Access-Level>
<Rights>
    <SendCoupon>
</Rights>
```

With the new σ, the GIS will send more specific information about Alice's objects whenever contacted next. Additionally, M-Mart can send digital coupons to Alice through the GIS or its AdLoc messaging proxy whenever Alice is available.

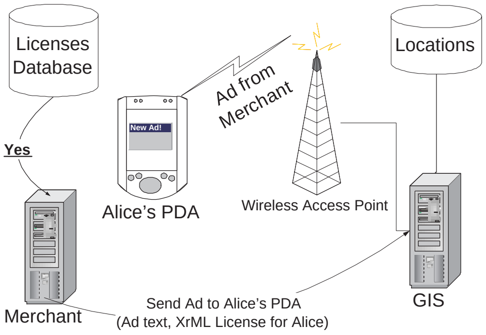


Fig. 4. Merchant sending an ad

6 Conclusions

We have described a formalism called a 'privacy system' that adapts access control matrices to the context of privacy. We have developed an architecture based on DRM that can carry out the negotiations to establish the rights in a privacy system. We have shown how 'Personal DRM' can be used to design a privacy-respecting system for LBS on WiFi sightings, and we have implemented this system for PDAs.

Acknowledgements

This work was supported by NSF grants CCR02-08996 and EIA00-88028, ONR grant N000014-02-1-0715, and ARO grant DAAD-19-01-1-0473 and a gift from Microsoft University Relations.

References

1. HR 122. Wireless telephone spam protection act.
2. HR 71. The wireless privacy protection act.
3. Matt Blaze, J. Feigenbaum, and J. Lacy. Decentralized trust management. In *Proceedings on IEEE Symposium on Security and Privacy*, 1996.
4. Electronic Privacy Information Center and Junkbusters. Pretty poor privacy: An assessment of P3P and internet privacy. 2000. `www.epic.org/reports/prettypoorprivacy.html`.
5. Roger Clarke. Platform for Privacy Preferences: A critique. 1998. `www.anu.edu.au/people/Roger.Clarke/DV/P3PCrit.html`.
6. US Dept of Health and Human Services. Standards for privacy of individually identiable health information. 2002. `www.hhs.gov/ocr/hipaa/nalreg.html`.
7. Scott E. Fahlman. Selling interrupt rights: a way to control unwanted e-mail and telephone calls. *IBM Systems Journal*, 41(4):759–766, 2002.
8. G. S. Graham and P. J. Denning. Protection: Principles and Practices. In *Proceedings of the AFIPS Spring Joint Computer Conference*, pages 417–429, 1972.
9. M.H. Harrison, W.L. Ruzzo, and J.D. Ullman. Protection in operating systems. *Communications of the ACM*, 19(8):461–471, 1976.
10. B. W. Lampson. Protection. In *5th Princeton Symposium on Information Science and Systems*, 1971. Reprinted in ACM Operating Systems Review 8(1):18-24, 1974.
11. Ninghui Li, John C. Mitchell, and William H. Winsborough. Design of a role-based trust management framework. In *Proc. IEEE Symposium on Security and Privacy, Oakland*, May 2002.
12. Jaehong Park and Ravi Sandhu. Towards usage control models: beyond traditional access control. In *Proceedings of the seventh ACM symposium on Access control models and technologies*, pages 57–64. ACM Press, 2002.
13. H. Schulzrinne, J. Morris, H. Tschofenig, J. Cuellar, and J. Polk. Policy rules for disclosure and modification of geographic information - draft-ietf-geopriv-policy-00.txt. Work in progress, 2003.
14. Einar Snekkenes. Concepts for personal location privacy policies. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, pages 48–57. ACM Press, 2001.

15. Robert Thibadeau. A critique of P3P: Privacy on the Web. 2000. `dollar.ecom.cmu.edu/p3pcritique/`.
16. Leonid Titkov, Stephan Poslad, and Juan Jim Tan. Enforcing privacy via brokering within nomadic environment. In *AT2AI-4*, 2004.
17. W3C. The Platform for Privacy Preferences 1.0 (P3P1.0). 2001. `www.w3c.org/P3P`.
18. Samuel D. Warren and Louis D. Brandeis. The right to privacy. IV(5), December 1890.

A Example

This is an example license in which The Mobile Ad Company is given the right to send John Doe any ad it wishes to his cell phone (number 215-555-5050) so long as it keeps to the included privacy policy.

```
<?xml version="1.0" encoding="utf-8" ?>
<core:licenseGroup
     xmlns:core="http://www.xrml.org/schema/2001/11/xrml2core"
     xmlns:cx="http://www.xrml.org/schema/2001/11/xrml2cx"
     xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
     xmlns:sx="http://www.xrml.org/schema/2001/11/xrml2sx"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xmlns:priv="http://www.pdrm.org/XrMLPrivacy"
     xmlns:p3p="http://www.w3.org/2002/01/P3Pv1"
     xmlns:xs="http://www.w3.org/2001/XMLSchema"
     xsi:schemaLocation=
     "http://www.xrml.org/schema/2001/11/xrml2cx ../schemas/xrml2cx.xsd">

    <core:license
        licenseId="http://www.pdrm.org/examples/2003/SendAnyAd">
      <core:inventory>
          <!-- Device with ad -->
          <priv:mobile licensePartId="mobiledevice">
         <priv:locator>
           <priv:id>2155555050@MobileISP.com</priv:id>
         </priv:locator>
          </priv:mobile>
      </core:inventory>

      <core:grantGroup>
        <!--The company that is tracking us' specific key.-->
        <core:keyHolder>
          <core:info>
            <dsig:KeyValue>
                <dsig:RSAKeyValue>
                    <dsig:Modulus>...</dsig:Modulus>
                    <dsig:Exponent>...</dsig:Exponent>
                </dsig:RSAKeyValue>
            </dsig:KeyValue>
          </core:info>
        </core:keyHolder>
        <sx:x509SubjectName>CN=The Mobile Ad Company</sx:x509SubjectName>

        <!-- The person allowing the company to track him/her-->
        <core:issuer>
          <sx:commonName>John Doe</sx:commonName>
        </core:issuer>

        <!--The period for which the company may track the user. -->
```

```
<core:validityInterval licensePartId="trackingPeriod">
  <core:notBefore>2004-05-20T19:28:00</notBefore>
  <core:notAfter>2004-07-29T19:28:00</notAfter>
</core:validityInterval>

<!--Grants Company the right to track the user through the
    permission period. -->
<core:grant>
   <priv:PrivacyPolicy>
    <!-- Disclosure-->
    <p3p:ACCESS>
        <p3p:all/>
    </p3p:ACCESS>

    <!-- Disputes -->
    <p3p:DISPUTES-GROUP>
        <p3p:DISPUTES
            resolution-type="service"
            short-description="Customer service will
                               remedy your complaints.">
         <p3p:REMEDIES>
          <p3p:correct/>
         </p3p:REMEDIES>
        </p3p:DISPUTES>
    </p3p:DISPUTES-GROUP>

    <p3p:STATEMENT>
       <p3p:CONSEQUENCE>
        We collect your location information for development
        purposes and for tracking your individual movement habits.
       </p3p:CONSEQUENCE>
       <!-- Why we use it -->
       <p3p:PURPOSE>
         <p3p:develop/>
         <p3p:individual-analysis/>
         <p3p:individual-decision/>
         <p3p:current/>
       </p3p:PURPOSE>

       <!-- Who else can get this data -->
       <p3p:RECIPIENT>
         <p3p:ours/>
       </p3p:RECIPIENT>

       <!-- How long do we hold onto the data for -->
       <p3p:RETENTION>
         <p3p:legal-requirement/>
       </p3p:RETENTION>
    </p3p:STATEMENT>
   </priv:PrivacyPolicy>
```

```
           <!--The mobile device from the inventory-->
           <priv:mobile licensePartIdRef="mobiledevice"/>
           <!--The rights that we are giving-->
           <priv:sendanyad/>
          </core:grant>
      </core:grantGroup>
     </core:license>
</core:licenseGroup>
```

B Example

This is an example license in which the Mobile Tracking Company is given the right to retain John Doe's location data for the length of the contract. In particular, the element `<core:grant>` grants the company the right to track the user through the permission period. No rights are granted otherwise.

```
<?xml version="1.0" encoding="utf-8" ?>
<core:licenseGroup
     xmlns:core="http://www.xrml.org/schema/2001/11/xrml2core"
     xmlns:cx="http://www.xrml.org/schema/2001/11/xrml2cx"
     xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
     xmlns:sx="http://www.xrml.org/schema/2001/11/xrml2sx"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xmlns:priv="http://www.pdrm.org/XrMLPrivacy"
     xmlns:p3p="http://www.w3.org/2002/01/P3Pv1"
     xsi:schemaLocation=
     "http://www.xrml.org/schema/2001/11/xrml2cx ../schemas/xrml2cx.xsd">

    <core:license
        licenseId="http://www.pdrm.org/examples/2003/retentionTracking">
      <core:inventory>
          <!-- This is the location information we want to grant access to -->
          <priv:location licensePartId="locData"/>
      </core:inventory>

      <core:grantGroup>
        <!--The company that is tracking us' specific key.-->
        <core:keyHolder>
          <core:info>
            <dsig:KeyValue>
                <dsig:RSAKeyValue>
                   <dsig:Modulus>...</dsig:Modulus>
                   <dsig:Exponent>AQAQAA==</dsig:Exponent>
                </dsig:RSAKeyValue>
            </dsig:KeyValue>
          </core:info>
        </core:keyHolder>
        <sx:commonName>The Mobile Tracking Company</sx:commonName>
```

```
<!-- The person allowing the company to track him/her-->
<core:issuer>
  <sx:commonName>John Doe</sx:commonName>
</core:issuer>

<!--The period for which the company may track the user. -->
<core:validityInterval licensePartId="trackingPeriod">
  <core:notBefore>2004-05-20T19:28:00</notBefore>
  <core:notAfter>2004-07-29T19:28:00</notAfter>
</core:validityInterval>

<core:grant>
  <priv:PrivacyPolicy>
 <!-- Disclosure-->
 <p3p:ACCESS>
   <p3p:all/>
 </p3p:ACCESS>

 <!-- Disputes -->
 <p3p:DISPUTES-GROUP>
   <p3p:DISPUTES
    resolution-type="court"
    short-description="Take your case to the local court">
     <p3p:REMEDIES>
    <p3p:correct/>
    <p3p:law/>
     </p3p:REMEDIES>
   </p3p:DISPUTES>
 </p3p:DISPUTES-GROUP>

 <p3p:STATEMENT>
   <p3p:CONSEQUENCE>
   We collect your location information for
   development purposes and for tracking your
   individual movement habits.
   </p3p:CONSEQUENCE>
   <!-- Why we use it -->
   <p3p:PURPOSE>
     <p3p:develop/>
     <p3p:individual-analysis/>
     <p3p:individual-decision/>
     <p3p:current/>
   </p3p:PURPOSE>

   <!-- Who else can get this data -->
   <p3p:RECIPIENT>
     <p3p:ours/>
     <p3p:same/>
     <p3p:unrelated/>
```

```
           </p3p:RECIPIENT>

           <!-- How long do we hold onto the data for -->
           <p3p:RETENTION>
             <p3p:indefinitely/>
             <p3p:legal-requirement/>
           </p3p:RETENTION>
         </p3p:STATEMENT>
          </priv:PrivacyPolicy>

          <priv:location licensePartIdRef="locData"/>

        </core:grant>
      </core:grantGroup>
       </core:license>
</core:licenseGroup>
```