PAM FORUM

The IMPORTANCE of PRIVACY in NEW TECHNOLOGIES

Abstract

As technology takes bold leaps in creating new applications, it can clash with the user's perception of his right to privacy. For example, the deployment of location-based services, like those used to report wireless 911 calls, now gives telecommunications providers the ability to pinpoint an individual's location with a high degree of accuracy. For privacy groups and consumer advocates, fearing that this technology might be used for commercial purposes to market to consumers or by governments to track the public's whereabouts, this new technology is cause for some concern. For this reason, privacy has emerged as an important issue for governments and diverse organizations such as Federal Express and Procter & Gamble.

This paper addresses how communications service providers can ensure the privacy of their subscribers. It outlines five privacy requirements (notice, choice, access, onward transfer and security) as seen by three regulatory bodies charged with ensuring public privacy (U.S. Federal Trade Commission, European Union and Organization for Economic Cooperation and Development). The report also addresses how each privacy requirement can be managed through the use of the Presence and Availability Management (PAM) specification. Examples of how these issues related to everyday life are given to aid the reader in understanding this complex issue.

The Presence and Availability Management (PAM) Forum is an independent, nonprofit consortium dedicated to giving users of diverse communications and messaging services greater control over where, when, how and by whom they are contacted. Communications systems using presence and availability management include data and voice services over wired and wireless networks.

Privacy Assurance: A Must For Presence & Availability Management - Version 1.0. March 2002.

Contributors *include Shane Furlong, Evolving Systems; Craig Medin, TeleCommunication Systems, Inc; Mario Tapia, TeleCommunication Systems, Inc.; Barbara Boyle*

Editing Team *includes Barbara Boyle; Technical Marketing, Inc. staff; APCO Worldwide, Inc. staff.*

Introduction

Privacy has become a popular topic of discussion among many specification and standard bodies in both the telecommunications and Internet realms. Recent studies have shown an overwhelming concern from consumers for privacy [1] and this concern has escalated a need for legislation. In this report we will discuss how the PAM specification helps service providers meet both the regulatory and consumer demands for privacy protection. We will also outline the business reasons for providing services that protect consumer privacy and demonstrate how privacy protection actually helps service providers increase subscriber loyalty and differentiate themselves from their competitors.

PRIVACY FOR TODAY'S WORLD

The Wayne family has just subscribed to a new service from their Internet service provider. Their Internet service provider has partnered with their wireless provider to allow services to interoperate seamlessly among their PC, their home phone and their mobile phones.

Frank Wayne is a techie at heart and was talked into the new service by his son Jason, 13. Katie Wayne isn't that interested in the service but feels the kids Jason and Jessica, 16, will use them.

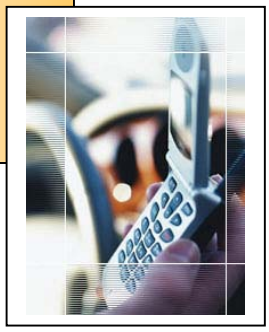
Their service provider has agreed to protect the Wayne's privacy and personal information. The Waynes answered a series of questions about when their personal information, such as presence or location information could be released. There are many times the Waynes are unaware that their service provider is protecting them and their privacy.

PAM Solves Regulatory Requirements

In the analysis of the PAM Forum, the requirements from the United States (U.S.), European Union (EU) and the Organization for Economic Cooperation and Development (OECD) have five areas of broad agreement. (For more information on these requirements see Appendix A) These are in the areas of notice, choice, access, onward transfer and security. In all five areas, the PAM specification can be used to control access to the presence and availability information of a subscriber.

NOTICE

What Frank likes the most about his new mobile phone flight status feature is that it lets him know if a flight is delayed or the gate has changed, no matter what city he is in.



Notice

Notice is given to a subscriber when another user or an application requests access to the subscriber's personal information. For example, when an application requests availability or presence data of the user, a PAM compliant server will send a message to the user before honoring that request, using the PAM specification's Availability Management interface. This feature can be offered to subscribers who require high levels of privacy. Notice can also be sent to a subscriber through the Identity Management interface when an application requests the addition of the subscriber's identity to a group in order to validate that the subscriber has opted in to the service.

Because Frank has agreed to receive these alerts when he signed up with his service provider, he doesn't see that the airline asks for Frank's location and presence information before sending the alerts. The airline gives notice to the service provider that the information is coming and Frank doesn't need to give an OK every time because of his agreement with the service provider.

Jessica loves to get the notice via instant messaging that someone wants to add her to a buddy list. As a popular teenager, she likes to see who wants her as a buddy and make sure that she's not on any of the nerdy kids' lists or that no one adds her to his list without her consent.

CHOICE

Another feature Frank likes while he travels is the ads sent to his phone. He can search for a restaurant on his phone and see an ad that promotes the evening special. This handy feature has kept him from getting a bad meal while on the road.

Katie, on the other hand, has chosen to turn this feature off in their local calling area. Since she has lived here all her life, she finds it annoying to get these ads to her phone. She has also chosen to restrict ads to Jason's computer log-on.

Choice

Choice, also known as consent, implies that a subscriber can decide whether or not to use a service. A PAM compliant server allows a subscriber to give his consent proactively rather than by opting out. Choice can be incorporated to manage different events using the Event Management interface and in particular contexts, such as the location or the time of day, with the Availability Management interface.

ACCESS

Mr. and Mrs. Wayne go regularly to the service provider's web site to change the options and personal preferences on their new service. Frank finds it much easier to change his mobile phone options at the PC than to try to manipulate the small menus on his phone. Katie uses the PC based access to change information on the fly, like call forwarding their home phone to their mobiles each time they leave the house.

Access

Access refers to the ability to view and alter subscriber preferences. For example, if a subscriber wants to change the number of applications that can view his presence and availability information, he can access these recorded preferences and make changes. A PAM compliant server allows a subscriber access to his privacy preferences using the Agent and Presence Management interface.

Onward Transfer

Onward transfer of data describes data that flows out of a PAM compliant server to another network. Once this data is outside the PAM compliant server, the subscriber no longer controls its use. However, the PAM specification mandates a field within the information profiles provided to specify an expectation of the degree of privacy under which the information is provided. This field can state privacy conditions such as "Not for further distribution", "One time use only", etc.

The enforcement of these restrictions is beyond the scope of the PAM specification but a service provider could insist that applications over its network follow the directions contained within these privacy codes, and bar access to the information by applications that do not follow these rules.

ONWARD TRANSFER

With Frank's nationwide travel, he has agreed that other providers may contact him in various locations. That way, his stock quotes, favorite sports scores and daily news are transferred to another provider when he is roaming with his mobile phone. The service providers need to share some of Frank's information in order to assure that the services get to Frank's phone everyday.

Katie has restricted this feature on Jessica's mobile phone. Jessica can only receive a very limited amount of features within her calling area. This restriction came after Jessica's all night instant messaging session with several teens in Finland.

Security

Security via authentication is a component of privacy that the PAM specification supports if it is in the implementation. However, the PAM specification does not *mandate* the use of authentication. As long as the authenticated credentials supplied by the client (or gateway) are acceptable for validation and the client (or the gateway) itself is authenticated by the implementation, the authentication of end users can occur anywhere outside the PAM implementation.

The following security issues were considered to be outside the scope of PAM:

- Authentication of the identity of the end-users or entities. This authentication may be provided by a third-party authentication service or it may occur through an authentication service written over the PAM platform. The only requirement is that the type of credentials supplied by the authentication service be acceptable to the PAM platform implementation being accessed.

- Encryption of the flow of information between a PAM platform implementation and clients of this implementation is dependent on the method of access to the interface which is outside the scope of the PAM specification and hence to be determined by the implementation.

- Data Integrity, although maintaining data integrity is PAM implementation specific. PAM advocates that personal data should be relevant to the purposes for which they are to be used and to the extent necessary for these

SECURITY

Each member of the Wayne family has a pin number that they enter to sign on to their PC's, mobile phones and PDA's. This provides a security check and limits the features of each user on the same phone or PC. When Jason is on the mobile phone, it is for safety only. His mom wants to know where he is. So, no ads for R rated movies or videos are sent to the phone. Jessica's pin restricts the hours that she can use the instant messager instead of doing her homework.

While some of these features are working in products today, some are in the labs and others are still in the imagination of the developer. As presence and availability become both a blessing and curse with new technology, the need to control these two aspects of human existence will become more important. That is why the PAM Forum was founded, to squarely face the good and bad aspects of the new technology and give users a method of controlling information about themselves and their families.

purposes, should be accurate, complete and kept up-to-date.

- Enforcement is outside the scope of PAM but its implementation must conform to local law.

Business Drivers for Privacy Protection

A recent Driscoll-Wolfe study showed that, while open to location based services (LBS), consumers are wary of privacy issues and want the ability to control access to their geographic location data [2]. Consumers want control over who receives their location data and they want to have the ability to turn the application *on* when they want to use it and *off* when they don't. The PAM specification offers a way to do just that.

Studies discussing the power of marketing using wireless data all stress the importance of building in consumer control over private information. These reports show that service providers that offer subscribers the ability to control access to their communication and availability status will be rewarded with increased subscriber loyalty and increased demand for new services. By providing privacy controls, service providers are not only complying with privacy regulations, they are also differentiating themselves against their competitors

Once a subscriber has establish availability profiles with an operator he will also be more reluctant to change service providers and have to recreate that data somewhere else. An operator that gives subscribers the ability to develop detailed profiles of their availability for communications can expect to be rewarded with increased subscriber loyalty and decreased churn.

A policy of strict privacy control, coupled with the building of customer preferences for privacy, will allow an operator or service provider to establish a "sticky" relationship with subscribers. A perception that a service provider is acting as a responsible steward of personal information will make consumers appreciate and value the relationship more than they currently do, and this should translate into increased customer satisfaction and lower churn.

The PAM Forum is the First Industry Organization to Propose a Privacy Solution

Many communications industry organizations are working to develop privacy requirements and policies, but none have developed a solution. The PAM Forum is the only organization to develop and propose a privacy solution for sharing personal information across multiple services and networks, while allowing the subscriber to maintain control over the use of personal data.

Below is a list of selected privacy initiatives in the communications space:

- 3rd Generation Partnership Project (3GPP) has recently started work on a Technical Report to identify and describe the service requirements for enhanced user privacy in location-based services (LBS). The presence service for 3GPP has not addressed a privacy solution. (www.3gpp.org)

- Location Interoperability Forum (LIF) is drafting its Privacy Guidelines that address conceptual privacy architecture, privacy laws, usage of location information, and use cases for location services. (www.locationforum.org)

- The Wireless Location Industry Association (WLIA) has released its adopted privacy policy. The WLIA advocates the use of Fair Information Practice Principles set forth by the U.S. FTC. (www.wlia.org)

- Liberty Alliance is a new organization and has not yet issued requirements or solutions to the public. The role of the Liberty Alliance Project is to support the development, deployment and evolution of an open, interoperable standard for network identity. It will require collaboration on standards so that privacy, security, and trust are maintained. (www.projectliberty.org)

Privacy Work in the PAM Forum

The PAM Forum is an independent, nonprofit consortium dedicated to giving users of diverse communications and messaging services greater control over where, when, how and by whom they are contacted. The members of the PAM Forum are committed to keeping the specifications relevant to the commercial application of presence technology and addressing privacy concerns.

Membership in the PAM Forum is open to any company interested in the evolution, promotion and/or adoption of the PAM specification as an industry standard. Any company interested in furthering the aims of the PAM Forum and interested in privacy issues should visit www.pamforum.org and join today.

Appendix A: Regulatory Environment

For most countries around the globe, local law mandates a business' responsibility for customer data privacy protection. Below we review the basic elements of privacy in both the U.S. and European Union, and internationally with the Economic Organization for Co-operation and Development (OECD).

United States, Federal Trade Commission (FTC)

Fair information practice principles were first articulated in a comprehensive manner in the United States Department of Health, Education and Welfare's seminal 1973 report [3]. In May 2000, the U.S. FTC reinforced these set of privacy principles in a report to the U.S. Congress. These principles require the following Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security, and Enforcement/Redress [4], [5].

- Notice/Awareness: Must be clear and conspicuous, provide what information is collected, provide how it is collected, and provide how it will be used, whether disclosed, whether other entities are collecting information through the site.
- Choice/Consent: Provide opt-in or opt-out regimes.
- Access/Participation: Provide reasonable opportunity to review and correct inaccuracies.
- Integrity/Security: Provide reasonable steps to protect information collected.
- Enforcement/Redress: Can be self-regulation, private remedies, or Governmental enforcement.

Below are current U.S. Government Acts supporting enforcement:

- Children's Online Privacy Protection Act, governing Web sites directed to children or that knowingly collect information from kids under 13.
- Gramm-Leach-Bliley Act, governing financial institutions, went into effect on November 13, 2000 (full compliance expected July 1, 2001).
- FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."

European Union (EU)

In 1995 and 1997, the EU enacted two directives in order to harmonize data protection laws throughout the EU, to ensure citizens' adequate levels of privacy protection and to allow free flow of personal information throughout the member states. In July 2000, an additional proposal was issued to provide further privacy protection in the electronic communications sector.

The Data Protection Directive from 1995 sets the benchmark for the processing of personal information in electronic and manual files and the movement of such data. The Telecommunications Directive from 1997 sets the benchmark for privacy protection in telephone, digital television, mobile networks and other telecommunications systems. It provides additional privacy protection to EU citizens by imposing obligations on carriers and services providers. The directive sets restrictions on access to billing information and marketing activities, and it gives consumers the option to block their phone numbers. Additionally the directive requires carriers and service providers to delete information related to a call once the service is completed.

A new proposal, "The Directive on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector", issued in July 2000 will replace the Telecommunications directive and further strengthen privacy protection in the EU once it is accepted. The proposed directive provides a broader perspective of electronic communications and it will ensure protection of all information transmitted across different electronic communications media, prohibit unsolicited e-mail without opt-in consent, and protect mobile phone users from location tracking and surveillance.

All EU member states are required to enact implementing legislation that follows the EU directives and provide independent bodies (a data protection commissioner or agency) to ensure the enforcement of the rules. The directives impose an obligation on member states to ensure that personal information relating to EU citizens has the same level of protection when the information is exported and processed in countries outside the EU. This requirement has resulted in a growing pressure in many countries outside the EU, including the U.S., to enact stronger privacy protection laws.

Organization for Economic Cooperation and Development (OECD)

Similar to the U.S., the OECD adopted privacy guidelines in 1980 [6]. The OECD Privacy Guidelines establish eight basic principles to govern the handling of personal information. These “Privacy Principles” are:

1. *Collection Limitation: there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where*

appropriate, with the knowledge or consent of the data subject;

2. *Data Quality: personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date;*
3. *Purpose Specification: the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose;*
4. *Use Limitation: personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law;*
5. *Security Safeguards: personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data;*
6. *Openness: there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, the main purposes of their use, as well as the identity and usual residence of the data controller;*
7. *Individual Participation: an individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him: within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and, in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified completed or amended;*
8. *Accountability: a data controller should be accountable for complying with measures which give effect to the principles stated above.*

Resources:

General

- Privacy Exchange (www.privacyexchange.org)

United States (U.S.)

- FTC Privacy Initiatives (www.ftc.gov/privacy)
- Government for Consumers (www.consumer.gov)
- Final Report of the FTC Advisory Committee on Online Access and Security (www.ftc.gov/acoas/papers/finalreport.htm)

European Union (EU)

- European Union Data Protection Directive (http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html)
- Internal Market Directorate General (Data Protection) (http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm)
- U.S. Department of Commerce, International Trade Administration, regarding relationships with EU (www.export.gov/safeharbor/)

OECD

- OECD Privacy (http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm)
- Global summary of Government Privacy Requirements by Country (www.olis.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)12-final)

References:

1. Lorrie Faith Cranor, et al., Beyond Concern: Understanding Net Users™ Attitudes about Online Privacy at 5 (1999) [hereafter" AT&T Study"] (Available at www.research.att.com/projects/privacystudy).

2. Driscoll-Wolfe Marketing & Research Consulting. Wireless Location-Based Services Study: Consumer Opinions on Privacy (July 2001).

3. Fair information practice principles were first articulated in a comprehensive manner in the United States Department of Health, Education and Welfare's seminal 1973 report entitled *Records, Computers and the Rights of Citizens* (1973) [hereinafter "HEW Report"].

4. Prepared Statement of the Federal Trade Commission on *Privacy Online: Fair Information Practices In the Electronic Marketplace*, (May 2000). (Available at www.ftc.gov/os/2000/05/testimonyprivacy.htm).

5. Privacy Online: A Report to Congress Federal Trade Commission, (June 1998), (available at www.ftc.gov/reports/privacy3).

6. OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (1980) [hereinafter "OECD Guidelines"].

www.pamforum.org
Questions/comments: info@pamforum.org