AUTHENTICATION AND ACCESS: The challenge of providing access to the right individual

I. OVERVIEW

Once a decision has been made that the individual should be provided access to information about them maintained by a business, the question is how to ensure that only the individual, and no one else, can gain access. Authentication devices provide a means of limiting access to authorized individuals – in this case the subject of the information. The Committee worked to identify the authentication options that would best ensure access to information is provided only to the individual to whom the information pertains.

During its meetings the Committee concluded that where information is tied to a specific identifier – for example a name, address, or unique identifier – access could be provided. Thus, the discussion of access covers both information tied to a specific individual's name and address and information tied to a unique identifier that has been assigned to the individual or his or her browser. However, as discussed below the second case raises additional authentication concerns that must be acknowledged and addressed.

Authentication can be accomplished through:

- something the user knows (like a password),
- something the user has (like an electronically readable badge), or
- something a user is (such as a biometrics identifier like a retina, handprint, or thumbprint).

Often authentication tools are used in combination - an ATM card requires a PIN (password) and is also used as an identifying physical and electronic token. It must be recognized that different populations have different sensibilities regarding acceptable techniques for identification, authentication, and authorization.

It is important to note that identification is different than authentication, which is in turn different than authorization. In many instances an individual's activities and access can be defined by non-identity based authentication.

Three examples reveal the distinctions:

1. My house key is an **authentication** device (something I have) that **allows** me to enter my house. If it is stolen it will allow the thief to enter my house, but her access will be un-**authorized** It does not provide any indication of my **identity**.

2. My work photo identification badge is a smart card. It provides information about my **identity** (a picture, name, title) that the desk uses to **authenticate**

that I am who I say I am. I use it to enter various floors in my building. By swiping it through a reader the card controls who enters what areas. In this case it is used to **authenticate** my ability to enter spaces – my **authorization**. While there is a record of the use of the card, there is no way to know for sure whether I or someone else, used it. In this instance the card does not authenticate my identity, rather it authenticates the cardholder's **authorization**.

3. A concert ticket is also an authentication device. It authorizes its holder to enter the concert. However, it neither verifies the holder's identity, nor verifies whether the holder purchased the ticket.

Authentication, identification and authorization are equally important in considering the measures a business employs to control internal and external access to and use of data. Therefore the issues discussed herein are relevant to the efforts of the security working group and should be considered as an integral component of any security plan. Authentication assists an organization in maintaining data integrity by controlling and providing a record of system activities, limiting outside access, and limiting the scope of access provided to authorized users.

II. IMPORTANT CONSIDERATIONS

A. Account v. Non-account

Authentication varies depending upon the context of the relationship, in particular it varies when: 1) an individual has a pre-existing account with which data is associated; and, 2) an individual has no pre-existing account but nonetheless data associated with his or her activities has been collected in non-aggregate form. The distinction of importance is whether the collected data is tied to a specific known individual, or the collected data is associated with a browser, unique identifier, or other proxy for identification. In the second scenario questions of providing access become complicated by questions of how to appropriately identify the subject of the data.

The collection of data about a computer or browser may lead to information about several individuals being compiled into a single profile, further complicating questions of authentication and appropriate access. However, it would be a paradox to allow others access to this data while limiting the record subjects access. Businesses can limit the complexity of the access issue by not collected or retaining profiles of information about non-account holders, or by retaining and using such information exclusively in the aggregate or by insuring non-account holders are anonymous. The assumption being that: account-holders are identified and by definition non-account holders are not.

B. Considerations of Access, Correction, Amendment

The level of authentication required to safeguard personal information may vary depending upon whether access permits the record subject to view information or allows the information to be corrected or amended as well. While providing access to the wrong individual violates the record subjects privacy – and may lead to additional harm ranging from embarrassment to loss of employment – allowing personal information to be corrected or amended by the wrong individual can result in other forms of harm. Where correction or amendment is provided, an audit trail should be maintained to aid in identifying potential problems.

The inappropriate correction or amendment of information could lead to faulty decision making by those who rely on the record. In circumstances where the record is relied upon for important substantive decisions, such as financial and health, inappropriate changes can have devastating consequences. For example, some criminals were gaining access to individual's credit card accounts by changing the individual's mailing address. The crook would fill out a change of address card with the post office diverting the individual's mail to another location. With access to the individual's bank statements and credit card bills the crook had ample information to impersonate the victim. The Postal Service has recently initiated changes to make this more difficult.[1]

Therefore, in considering what form of authentication a business should employ the level of authorization conveyed by authentication must be considered.

C. Sensitivity

The Committee discussed the notion that security and perhaps authentication needs would vary depending upon the sensitivity of the data the business maintains. Particularly in the difficult area of non-account information, the Committee felt that the risks of inappropriate access to sensitive information had to be discussed prior to establishing access procedures. There are important privacy interests on both sides that must be respected.

In addition, the definition of access – does it include correction and deletion rights – creates questions of sensitivity. Where access also connotes the right to amend or correct the information it maybe important to heighten or readjust the authentication requirements.

D. Security of authentication devices

Authentication devices vary and so do the likelihood of unauthorized use, loss, and theft. The Committee discussed the problems with over reliance on passwords – use of one password at multiple places, yellow stickies, common passwords – all of which compromise the integrity of the authentication system. Similarly, in the offline world the reliance on widely available information such as name, address and phone number to authenticate the identity and authorization of an account holder is risky. The use of shared secrets (social security

[1] See The Privacy Rights Clearinghouse http://www.privacyrights.org/AR/id_theft.htm for more information.

numbers) which have been compromised by wide spread use raises additional concerns about the strength of authentication devices. Authenticating identity has become a far more complex endeavor than it once was.

E. Feasibility of authentication devices

The full Committee also discussed the feasibility of authentication devices. The Committee expressed concern that "perfect" authentication tools may be prohibitively expensive or too cumbersome for widespread use. However, the Committee has heard from authentication vendors who that a wide range of authentication solutions are available from a number of security vendors today that solve the password 'problem' described above. These solutions take the form of hardware tokens that are as easy to use as an ATM card or software tokens that can be downloaded easily to a PC, PDA or cell phone. The Committee notes that the questions of liability for misuse and misappropriation of such devices remains.

As discussed in the security section, security is contextual. Authentication is an integral part of system security. Therefore, to establish appropriate authentication businesses must consider the value of the information on their systems to both themselves and the individuals to whom it relates, the cost of particular security measures, the risk of inside abuse and outside intrusion, and the cost of a security failure in terms of both liability and public confidence.

F. Liability

The allocation of liability for inappropriate access and inappropriate use, loss, or theft of authentication devices is an important consideration. While there is not explicit statutory assessment of liability, currently a business could potentially be held liable for allowing the wrong person to access personal information. However, on the other hand if a company allows an unauthorized individual other than the data subject to access personal information it is unclear whether or not the individual would have a remedy under existing law. The lack of certainty regarding liability presents a problem for both individuals and businesses. If liability is strict and put upon businesses they may raise the barrier to access very high, burdening individuals' access rights in an effort to avoid liability. While there are public relation and other market forces to consider, if there is no express liability for inappropriate access businesses may not take appropriate care in establishing robust authentication systems and individuals' privacy may suffer due to inappropriate access. How to strike an appropriate balance that spurs good practices, encourages the deployment of robust authentication devices, and does not overly burden access is the question. This issue is part of the question of how best to facilitate the development of robust and risk-appropriate security and access procedures. As mentioned above, this is an important component of ensuring data integrity and limiting unauthorized access and must be expressly considered and addressed within companies' security plans.

G. Privacy implications of authentication devices

The Committee wishes to emphasize that difference between authentication and Identification. As we seek to provide individuals with access to personal information we must not move toward greater identification of individuals. Maintaining the ability of individuals to be anonymous on the Internet is a critical component of privacy protection. Access systems should not require identification in all instances. Biometrics raise additional privacy concerns that must be explored and addressed. Finally, third party authentication systems raise important privacy concerns (creating additional records of individuals access requests). Inserting a third party into the relationship creates an additional opportunity (at times it may be responsibility) to collect and maintain information about the individual's interactions. What policies govern these entities' use of personal information? On the other hand, third parties – intermediaries -- can also play a role in the protection of identity. Currently several companies have establish themselves as intermediaries whereby they establish themselves as a protector of identity and privacy between the individual and other entities.

III. OPTIONS

This section of the report does not determine whether access to specific information should or should not be provided. It provides guidance on how to ensure access to the appropriate person where access has been determined to be appropriate.

A. Authentication requirements for account affiliated data

Where an account has been established access to the information retained in that account can generally be provided. In general the individual's ability to access information about the account should not be burdened by intrusive requests for information beyond what was required to establish and secure the account. However, it is common practice both offline and online to require some additional piece of information that is thought to be more difficult to compromise.

Where an account has been opened and is activated through a password it would be appropriate to provide access to the data when presented with a person who appears to be the account holder (tested), has the password, and presents some verifiable information about recent account activity. Such an approach would provide a two-token method of authentication, but preserve the privacy offered by the initial account.

I subscribe to an Internet Service Provider providing them my name, address, and billing information. At a later date I request access to data they retain about my usage of the account. What should be used to authenticate that I am the account holder? Should that same authentication grant me complete access to data, or should an additional level of protection be afforded to certain data?

My name, address, and billing information are useful for authentication, however they are also widely available from other sources. Therefore they may not be sufficient to provide access. Many businesses require individuals to use a shared secret (password, mother's maiden name) to access an account. Concerns have been raised that passwords become hard to maintain, and frequently individuals resort to using simple ones or placing them in easily accessed places (the yellow sticky), and that some shared secrets have become so widely used they are no longer secret (social security numbers). The move to dynamic shared secrets (such as Amazon.com's use of two recent purchases (a shared secret)) would be a positive step. It provides a "something you know" token, but allows it to be dynamic (a benefit for security and privacy), and varied between services (because it is service based it is unlikely to be used by multiple systems).

Case study I open an email account with a free service. Establishing the email account does not require me to disclose personal information. I am assigned an email address and am asked to establish a password to protect my account. If I request access to personal information held by the service, how should they determine whether to **authorize** my access? What level of **authentication** should be required?

Options

a. **Require the same information for access (account name and password).** This approach errs on the side of ease of use for the account holder. But in doing so it relies upon one token (account name) which is frequently shared with others (email address for example) and another token (password) which is (as our discussions indicate) relatively easy to compromise.

b. **Require my account name, my password, and information about recent account activity.** This method adds some protection against unauthorized access. By asking for the account name (something I have), my password (something I know), and recent account activity (something I know that is dynamic, and unlikely to be known or discernible by others) it adds an additional protection.

c. **Require either of the above sets of information and send the requested information to the account.**

d. **Require either of the above sets of information and require that the request for access be made through the account, and send to the account a one-time access code.** This approach would build in an additional precaution against unauthorized use. By requiring the request to come from the account (similar to credit card authorization that must come from the registered phone of the

account holder) and returning a one-time access key to the account the system could further limit unauthorized access. This feature might cause a minor delay, but it does not require the individual to remember additional pieces of information.

B. Authentication requirements for non-account affiliated data:

Consider the situation where an individual has not opened an account with a service, but the service has collected data about the individual (or some proxy for me) and her activities. If this data is found to be within the scope of the access mandate, how should the Web site proceed? How can a service authenticate that the individual is the person to whom the data relates? Should the level of access authorized be lowered due to the complexities of authenticating my connection to the data? Are there other policies that would address the privacy interest and have a lower risk of unintentionally disclosing data to the wrong individual? Does this concern vary from Web site to Web site?

Case study:

A Web site assigns each visitor a unique identifier that is used to track and retain data about the visitor's activities at the site. The Web site does not request or gather information about specific visitor's identities. A visitor requests access to information that the Web site has about her use of the site. How should the Web site proceed?

How can a site authenticate that the person requesting access is the person on whom they have collected a unique identifier based profile? How can Web sites provide access to what they have in a fashion that reflects the potential adverse consequences of disclosing information to someone other than the subject of that information. The consequences of disclosing information about an individual's use of a Web site to another person (family member, co-worker, other) could be quite damaging. Depending upon the type of information or service the Web site provides, inappropriate access to click stream data could be quite harmful.

Options

a. **Require the identifier (presenting the cookie).** This would make it quite easy for the user to access; however if the identifier is tied to an imperfect proxy for the individual (such as a computer) it is possible that other individuals may gain access to the individual's personal information. If a cookie attached to a browser by a specific Web site was used to provide access it could allow all members of a family, or other group, who share a computer to access each others' information. We tolerate this "over disclosure" in certain cases, such as telephone calls where we disclose all calls made from a number back to the individual named on the account

despite the fact that in multi-family homes this discloses other family members' calls. However, in the online environment over disclosure could be more damaging because the information collected about an individual's use of the Web can on its face reveal more about the individual. For these reasons the identifier alone may be insufficient to grant access in many situations. But there may be instances where the identifier alone is sufficient proof of account ownership to grant access. For example, if the Web site is a general interest site that only retains information about how often visitor returns, providing access to someone other than the person who visited may raise little concern. But, if the Web site is focused on a specific disease then providing any information to the wrong person, even information about number of visits, could be quite harmful.

b. **Require the individual to open an account and allow access to data collected from this point forward.** This may or may not limit inappropriate access. For example, if the account is browser based and there are several individuals who use the browser this would allow one individual to access all the data and prevent the others from accessing any.

c. **Require the identifier but limit the scope of access.** This option acknowledges the risk of inappropriate access and to mitigate the harm it may cause limits the information provided. For example, a Web site could provide categories of information it has collected rather than the actual information. In some instances disclosing to the wrong individual the mere fact that a Web site has information tied to a unique identifier could be harmful. For example, if the Web site's subject is sensitive or revealing topic the mere fact that it has any information about tied to the identifier could in the wrong hands cause damage.

d. **Delete the file and commit not to collect additional data.** This option acknowledges the risk of inappropriate access and seeks to provide for the individual's privacy interest in another fashion. While this does not directly serve the individual's access interest, it would protect their general privacy interest by deleting the information. It poses no threat of inappropriate access. However, it could allow some one other than the subject of the data to have the data deleted.

e. **Disassociate the data from the identifier and use it for statistical, aggregate or other non-individually based purposes.** This option acknowledges the risk of inappropriate access, but also recognizes the commercial interest in utilizing the

data in non-identified or anonymous form. While this does not directly serve the individual's access interest, it would protect their general privacy interest by removing information that connects the data to them.

f. **Require no identifier but provide only a general description of the kinds of data collected.** This errs on the side of limiting the impact of inappropriate disclosures and acknowledges that even the fact that a browser has an identifier associated with a specific site or service could in some circumstances be revealing and potentially harmful.