Privacy in the Identity Management Landscape in the United States:

Issues Raised by Using Employer-Issued Credentials for Personal Transactions

Shauna Russell, Anna Slomovic, Peter Alterman

Background

Two trends are expanding in cyberspace currently: the use of online identity credentials issued by one source for authentication and authorization to access resources elsewhere, and the expansion of pernicious theft of personal information (PI)[1] and its subsequent misuse for fraud and theft. This problem occurs all too frequently to users of health care portals and leading e-commerce sites, where more significant personal data are exposed, such as medical conditions, insurance claim numbers, credit card information and bank account passwords. The convenience factor experienced by end users everywhere is a testament the successful transition society has made to the Internet age. While acknowledging the vast benefit of the Internet, governments and law enforcement at all levels have yet to find effective ways to stem the tide of theft and fraud, and particularly, the theft of PI.

It is axiomatic that over the past thirty years, governments and businesses in all sectors have gone electronic; that is, most business processes that were once paper-based and people-based are now done by and on interconnected computer systems of various sorts linked wirelessly with personal devices carried by roughly 90% of the American people. One consequence of this is that employees regularly receive online identity credentials from their employers and the credentialing process generally includes identity-proofing processes that collect and store significant amounts of PI about the employee, some of which is related directly to identity assertion and some of which is extended attribute data. These more-trustworthy credentials, issued on the basis of more reliable identity-proofing and possibly use of tokens that resist attacks more effectively, are then used to access the employer's online systems and associated systems operated by other related businesses.

Many online consumer applications, such as banking and healthcare discussed above, could be more secure if they were accessed with more secure and trustworthy credentials. One potential source of such credentials is a credential issued by employers for business purposes. While having an identity credential usable many places on the Internet is convenient, use of a business-related online identity credential in personal applications poses special threats to privacy. The personal application may receive data about the employee that it would otherwise not receive. Additionally, if the non-job related online application validates the employee's credential against the employer's system (e.g., Active Directory or Public Key Infrastructure), then the employer acquires information about where the employee is using

[1] This paper uses the term personal information throughout but we note that, in the United States, the term "personally identifiable information" is used to describe information that might be covered by the various privacy laws. PI is a broader category of information that may or may not be covered by privacy laws.

those credentials in his or her personal life. This creates a substantial challenge to the employee's privacy protections.

There are two sources of protection for PI in the US. The first is protection provided by the privacy laws. US privacy regulation is sectoral, so different parts of the economy are subject to different privacy laws. Healthcare and banking have significant privacy regulations for consumer data, although these regulations do not cover the data of employees in their professional capacities. In other sectors, however, privacy protection requirements can vary from none to some protection. The second source of privacy protection comes from agreements made between two or more parties such as between a credential issuer and the online application that consumes the credential in the course of business. These are contractual arrangements that reflect voluntary agreements between parties and may include clauses that govern the rights of various parties in the areas of data collection, use and disclosure.

The growth of online transactions has created demand for systems to perform Identity Management functions for both internal company systems and for their customer-facing systems. Sometimes these functions are performed in-house and sometimes they are performed by a growing number of external identity credential providers. By a series of agreements, groups of these identity credential providers and relying parties implement rules for issuing, managing and consuming the information about the subscriber that may include rules for protecting user privacy. These rules are the basis for asserting and relying on end-user identities and attributes. Where such rule sets (call them Trust Frameworks) are limited to specific market sectors or communities of interest, they may not need to consider whether their rule sets operate across market sectors. Instead, the intended use of identity and attribute information is defined by the needs of the community involved.

Recently, there has been some desire to expand the Trust Framework concept by opening systems targeted to specific communities of interest to more parties, creating a more all-inclusive set of rules[2] for managing identities and credentials that allow interoperability among disparate communities of interest and across multiple sectors. The difficulty with establishing a truly open rule set is how to address the different and sometimes conflicting legal and policy requirements within each market sector and among market sectors so that interoperability might be achieved. Such open rule sets underscore the challenges to individuals' personal privacy on the Internet.

A host of as-yet unresolved privacy challenges are inherent in the emergence of broadly interoperable identity and attribute assertions and their consumption on the Internet. This paper aims to highlight the privacy issues that arise when the electronic identity an employer gives an employee is used to authenticate to online applications for personal purposes, rather than for business purposes. We aim to draw broader conclusions from this example.

[2] For the purposes of this paper, federated rules are a set of rules agreed by multiple parties that can operate across market sectors and among a number of communities of interest and that are adopted by the participants in multiple market sectors and communities of interest.

Business Persona and Personal Persona, an Example of Cross-sector Use of Credentials

A Persona is a collection of PI and other attributes that defines individual identity. Most people have more than one such Persona because different attributes are relevant in different areas of their lives. In many cases, different Personas are not connected to each other in a way that is visible externally, which is not necessarily a bad thing. Privacy issues can arise when a Persona from one context is used in a different context.

Collection, storage, and use of identity and PI have always been essential in the employer-employee relationship. The relationship starts at the pre-employment stage with submission of an employment application or resume, verification of education and experience, checking of references, ensuring appropriate certifications and licenses are valid, performing appropriate background checks, drug testing, verifying identity documents, and using collected information to demonstrate compliance with law and regulation. Identity information and other PI is vital to the employment relationship itself where human resources information about an employee continues to be collected, stored, and used. The information is required for a myriad of purposes, such as identity verification, suitability determinations, employee evaluations, provision of benefits, productivity and performance statistics, privilege issuances and physical and logical access determinations. It frequently provides the basis for determining accountability within an organization. For the duration of the employment period it provides the basis for a Business Persona of an employee who is engaging in business transactions for the benefit of the employer. PI continues to be important post-employment for pension and benefit determinations, recordkeeping requirements, and historical purposes.

The Business Persona of an employee includes not only identity information, but also attributes such as business affiliation and business role, evidence of authority to commit the employer to an agreement or contract, citizenship information or other PI that may be required to support a set of business transactions that the individual may be authorized to perform on behalf of the employer. Business-to-Business relationships frequently require trust which is based on confidence in the identity and authority of the individuals seeking to do business on behalf of an organization. Employers can issue identity credentials for their employees or they can hire firms that specialize in Identity Management to provide credentials.

Several Trust Models exist in the business landscape to facilitate secure business transactions. Rules for the models exist today and are frequently called Trust Frameworks. The Trust Frameworks operating around the employer-employee relationship tend to be employer-centric and focused on the Business-to-Business transactions that occur daily. Employee privacy expectations within these Frameworks are based on employer obligations under various state and federal labor and employment laws, such as anti-discrimination laws and health and welfare laws.

A Personal Persona is a collection of PI and attributes that defines an individual in a particular personal context. In many cases, individuals have multiple Personal Personas, such as “student” and “patient” that are relevant in different online contexts (signing up for classes online and signing up for an appointment with a doctor). Creation of each of these Personas requires an identity management system to collect and verify PI, including identity information and attributes relevant to that Persona. As

a result, each Persona can result in a separate store of PI and a separate credential. Depending on the security needs of the relying party (RP), the credential may involve collection and verification of a significant amount of PI.

If strong identity credentials issued for an employee's Business Persona could be used for personal transactions, it might limit the number of systems in which PI is stored, simplify the user experience, and provide cost savings for users and online services by relying on the identity verification processes that employers already perform as part of the employment relationship. While this may reduce some risks to the individual by reducing the number of personal data stores that could be breached, it inadvertently increases risk in other ways. If an individual uses an employer-issued credential for a personal transaction in which the issuing system is asked to validate the credential, then the employer could receive information that allows it to follow that transaction. Also, Business Persona information stored on the credential or provided in response to a credential validation request may become available to the online business, with unassessed consequences. Clearly, there are the privacy related implications that need to be addressed.

Privacy Issues in the Use of Business Credentials for Personal Purposes

There are three sets of privacy issues to be considered when thinking about the use of employer-issued credentials for personal purposes.

Ability of employers to track personal activities performed outside work

People often use credentials in "federated" mode without realizing that this is what they are doing. Any time a driver's license or a passport is used to board an aircraft or a school ID is used to obtain a library card, the credential issued by one party is being relied on by an unrelated party for its own purposes. This is what we usually mean by "federated identity." However, documents used in this way are usually not verified with the issuer. In other words, the DMV that issued a driver's license does not know where or when holders of the license fly. Instead, validity of the credential is verified through security features on the credential itself.

There are also are company and government-issued electronic credentials or credentials with electronic components that permit the RP to verify credential validity in real time with the issuing party. In this scenario, if an employee-user of an employer-issued identity credential were to present that credential to an online business, the online business (considered a RP in the transaction) would verify the validity of the credential with the employer which issued the credential. Like any other issuer of online credentials, the employer would log the query for record-keeping, legal and security purposes. In accordance with standard security protocols, the log will include entries like date and time of the request and the identity of the requesting RP. It might also include what data was provided in response to the query. This information would be available for regular security monitoring as well as for review as part of investigations, such as security clearance reinvestigations or periodic personnel evaluations. All of this can happen without the employee understanding how this PI has been collected and used, how long it is held by the employer, or whether the information is being accurately maintained.

Logging of identity verification transactions always raises privacy concerns for individuals who use identity credentials, in this case the employee-users. When employer-issued identity credentials are used for personal transactions, the logs can provide employers with information about employees' private lives, such as where and when employees conduct financial transactions, access medical records or medical services, as well as employees' political, religious, or charitable affiliations. There is no specific legal precedent about whether employees can have any expectation of privacy when they use employer-issued credentials. The courts have generally favored employers when they had to rule on cases in which employees used employer networks or employer-issued devices for personal purposes and the employer engaged in monitoring of its networks and devices or gained access to the associated metadata and content.[3]

Logging employee personal transactions also raises concerns for employers. Even if employee use of employer-issued credentials is purely voluntary, and even if employees act with full knowledge of the data collection that results from such use, employers would need to address their potential liability under various employment and other laws. Without existing legal precedent, it is unclear whether an employer has an obligation to examine all information it possesses about its employees in order to assess and monitor whether an employee presents a risk to the organization, other employees, or customers.

On the other hand, employers are limited by various federal and state laws in what data they may collect from and about their employees and the purposes for which they may use such data. For instance, employers have been successfully sued when they have investigated employees' intimate relationships, even though employers may have a legitimate interest in guarding against sexual harassment in the workplace or preferential treatment based on favoritism or granting of sexual favors. Another area that could raise concerns for employers is medical, genetic and substance use information. Several federal laws, including Health Insurance Portability and Accountability Act (HIPAA), Genetic Information Non-Discrimination Act (GINA), and Americans with Disabilities Act (ADA), limit the health-related information that employers may collect and use in the employment context. Some states have broad protections for employees engaging in lawful off-duty conduct, including consumption of legally available products, legal recreational activities, and political activities. It is unclear what rules would apply if an employer gained information about such activities from logs of identity credential verification and then took an adverse action against an employee even for unrelated reasons.

Clearly, there are a number of liability issues that may give employers pause before they allow employees to use employer-issued credentials for personal business transactions. There may be additional liability concerns if the employer has failed to follow its own credential issuance and management procedures and a RP suffers a loss as a result.

Collection and release of attributes along with Identity Information

Attributes such as age, location, and professional status are useful and sometimes required in a wide range of personal online transactions. For example, certain transactions require the user to be at least 21 years old. Some products or services are offered only to certain categories of individuals, such as

[3] See, for example, Kathleen M. McKenna and Anthony J. Oncidi, "Workplace Privacy Law," Proskauer on Privacy, 2006.

those who possess a credit score within a certain band. Still other transactions require a particular business or social affiliation, such as being a member of the military. In some transactions, RPs may also want to obtain and verify certain attributes in order to elevate the level of trust in the presented credential. When an attribute is required as part of an online transaction, it will need to be provided to the RP by the individual, by an identity credential provider, or by another party that has the information.

When a business credential is used for a personal transaction, the credential may not be associated with the appropriate attribute set to support the personal transaction. Conversely, some business attributes may be unnecessary for a RP in a personal transaction and provide more PI than the individual wants to provide.

In order to protect employee privacy and provide only appropriate attributes when business credentials are used for personal purposes, employers will need to provide a transparent mechanism for employees to know what attributes are attached to or associated with the business credential and a way for employees to provide consent for the release of various attribute sets to different RPs. There will also need to be a governance structure that determines whether employers should collect additional attributes on behalf of their employees and, if so, how these additional attributes may be collected, verified, maintained and used. Employers will need to balance the risks associated with collecting and maintaining additional information about their employees with the extent to which such information will make employer-issued credentials more usable to employees and more acceptable to RPs. Employers may view this as an employee benefit, and they would need to evaluate the associated cost and risk to them of providing such a benefit.

Inability of RPs to distinguish a user acting in a business capacity from the same user acting in a personal capacity

Whether transactions are occurring in person or online, there are circumstances in which employees acting in a business capacity may have access to records of many people, but when acting in a personal capacity should have access to only their own records or to records of individuals who have given them explicit authority for access. For example, healthcare professionals can access medical records of many patients in their professional roles. However, when acting in a personal capacity under HIPAA, they may only access their own Protected Health Information (PHI) or the PHI of those for whom they are a Personal Representative. Similarly, mortgage lenders may access credit reports of many loan applicants in their professional capacity, but in their personal capacity may access only their own credit reports. Human Resources employees may have access to 401(K) information for all employees, but should only have access to their own information for personal transactions.

Further potential for confusion is created when data access is delegated from one user to another. In both business roles and personal lives, people delegate responsibilities that include authority to access and use data. For example, the DEA Rule on e-prescribing of controlled substances permits physicians to delegate the preparation of an electronic prescription, as long as the physician subsequently reviews and electronically signs it. In a personal context, it is quite common for spouses to delegate to each other access to financial or health records.

If business credentials are used for personal purposes, RPs will need to determine the role in which the individual is acting--business, personal, or delegated, and if so, in what type of delegated capacity--in order to provide the individual with access to appropriate data or privileges. In many cases, consumer-facing applications are already different from business-to-business applications. If the use of employer-issued credentials for personal transactions is to be successful, RPs that wish to accept such credentials would need to ensure that they have systems and processes in place to properly distinguish personal privileges from professional ones.

Addressing the Challenge Presented by Use of Employee-issued Credentials Outside the Work Context

There is no comprehensive privacy law that governs the Identity Management landscape. This fact makes the use of employer-issued identity credentials in the online marketplace an area where employers and RPs are at risk of not properly managing PI, and one where employees may have privacy expectations that are not based in law or reality. The following suggestions can help mitigate concerns for both employers and employees.

Employers must ensure that PI is collected, stored and used in accordance with the privacy laws and regulations that may be applicable to them. *Without a general privacy law imposing privacy practice requirements in the US, the only option for protecting privacy of employees who use their employer-issued credentials for personal purposes is by agreement between or amongst the parties involved, including agreements to follow Trust Framework rules and publicly available and enforced codes of conduct.*

Today, employers may or may not have policies that govern employees' use of business credentials for personal transactions. Employers that have no such policy may be at risk for collecting and storing information about employees that they did not intend to collect and do not know they possess. Those with policies that restrict or prohibit such uses may not know that credentials are being used in spite of policy, and may face difficult choices and legal challenges if they take adverse action against employees that have violated policy. In both cases, transaction information may be automatically recorded without the employer being aware of it and may surface only after a violation of the employer's policies has occurred. On the other hand, there may be circumstances where employers may want to encourage use of employer-issued credentials for personal transactions, such as access to employer-based but privately managed 401K accounts or employee perks such as discounts for baseball and theater tickets that are offered to employees through the employer. *In order to ensure that employer-issued credentials are used appropriately, employers should create reasonable and easy-to-understand permissible use policies for their employees. They also need to have systems in place to distinguish permissible transactions from those that are prohibited under their policies.*

In order to move forward in the absence of new law, we need a set of rules that include technical and security controls on the issuance and use of credentials, procedural and policy controls over issuance and use of credentials, and a framework that establishes privacy protections for the use of employer-based credentials when such use is permitted. This framework would need to bind all the parties to the intended transactions – employers, employee-users, credential providers and RPs. *In the end, reality*

will meet expectation only if individuals understand the privacy implications of use of the credentials issued by their employers and employers and RPs comply with legal or contractual requirements that ensure privacy protections for all users.

General Reference: Daniel J. Solove & Paul M. Schwartz, *Privacy Law Fundamentals 2013* (2013).