15. Scenario II: Universal National Identifier

Allan Friedman

Introduction

Fears of terror, the promise of efficiency, and the potential for commercial gain make the prospect of using a single identifier look very attractive. Some believe that every individual in the United States should have a single, unique identifier that is bound to their person by the strength of law, a carefully constructed infrastructure and a robust biometric. The adoption of the Real ID Act and the requirements for RFID in passports indicate a perception of policymakers that identities are too fluid and uncertain.

While expensive and difficult to implement, a universal identifier makes control of personal information much easier, both for governments wishing to provide services and protect citizens, and potentially the individuals themselves trying to control their personal information. But, others note (source) the implementation of a single, unique identifier also can generate dangers for a democratic society including blows to privacy, the erosion of civil liberties, and the strengthening of a central government.

The State of Identity

In the Age of Information, it makes sense to have identifiers that come closer to meeting the needs and potentials of information technology. Thus, each individual is assigned a unique, universal identification number. This aspect, while not trivial, represents only one small part of the identifier challenge; a large infrastructure is necessary to bind the individual to that identifier. This is done in three levels, with increasing security and trust in that binding at each level. This UID serves as a key to access both public and private databases, as well as being the base for security and privacy policies in those databases.

A UID number should not be a secret, any more than a name is a secret. This was one of the great failures of the Social Security number as an identifier: it was widely employed as both an identifier and a verification mechanism. It is unlikely that a stranger will know another's name, and less

likely that the stranger will know her UID number. Yet having knowledge of that number should not give the stranger any more power than having a name (and in some cases, less power). The number space should be large enough to avoid redundancy, and ideally leave space for an error bit or other administrative information, yet be small enough to allow an individual to remember the number, if he or she has been prompted for it repeatedly. Alternatively, alphabetic characters could be used to increase the space with fewer digits. This number could be used as a stand-alone for transactions that do not require any large amount of trust. A call to a technical support center, for example, just needs a key to a database so that the technician can pull up the right software specifications that an individual purchased.

Most transactions, however, require confidence in the participants. Rather than simply knowing what can essentially be treated as public knowledge, a basic level of trust could be conferred on having something. In this case, a smart card is the most likely choice, since it can hold protected information and can be signed by trusted institutions or government agencies for an added degree of security. A swipe of the card could produce an ID number, providing a basic level of verification. More importantly, a swipe could securely reveal to a concerned merchant or government official whether or not an ID holder is a member of a group. Is a consumer in the over-21 group or a traveler in the wanted-for-questioning group? A card reader can send an encrypted query to a trusted database and gain the necessary knowledge, and only the necessary knowledge. This builds a series of protections. A merchant must have appropriate permission to query the database, and each query can be tracked. The cardholder can be more confident that only the necessary information about her is drawn from remote databases, and little personal information actually has to be kept on the card itself.

To fully protect the link between identifier and individual, however, a biometric is necessary. Situations arise where a transaction party may wish to be certain that the person in possession of an ID card is actually the person identified by the card in previous transactions. Essentially, this question is seeking to determine whether the user of the card is the same person who has used the card all of the previous times. This can be asserted recursively with a biometric enrollment on issuance of the card; occasional matching of the cardholder with the biometric on file will help verify that the original individual-identifier link is still valid. This assumes that a biometric will be stable throughout the course of a lifetime; the UID drafters ultimately chose iris recognition. Biometrics are secured only occasionally, and in accordance with the risks of a mismatched identity and the necessary expenses. Obviously, the harm caused by a minor obtaining cigarettes are not on the same order of magnitude as the harm caused by a house purchased in some one else's name. It may be far too inefficient to check the biometric of every flier all the time. Since immigration and customs already performs a