Risk Assignment in Identity Infrastructures: We're From The Government, and We're Here To Help Someone Pretend To Be You

Adam Shostack
adam@homeport.org

June 19, 2003

Abstract

Much discussion of privacy invasion starts with either an economic or weather analysis. That is, someone is motivated to invade privacy, or it's just happening. In this essay, we advance the idea (pointed out to me by Adam Back) that a great many privacy invasions happen because there is a (largely compulsory) infrastructure, which enables other privacy invasions. We show that this infrastructure has poor risk assignment properties that inhibit the creation of solutions to identity theft and other privacy problems.

1 Identity Infrastructure

In much of the US, it is practically impossible to live without a car, and thus a driver's license. The DMV, in accordance with US law, makes the fruits of its labor freely available. It is unclear how much it costs to perform the identity verification functions of the DMV.

Similarly, social security numbers are now assigned at birth, and it is quite difficult to prevent a hospital from assigning one. The tax cost of not having a social security number for a child can be enormous, and so most everyone has one.

When starting a new job, the applicant needs to fill out an "I-9" form for immigration. Failure to complete this form can expose an employer to a $10,000 fine. Thus, a social security number and two forms of ID are needed to start a new job. To open a new bank account, know-thy-customer regulations require ID and SSN.

Thus there is an identity infrastructure, created by the government, which it is very difficult to opt-out of while participating in modern society, changing jobs, using a bank, or traveling. While theoretically there is no official compulsion to do any of these, there is a very practical need to do all of them, thus requiring that everyone have government issued photo ID.

1.1 Free Riding

It is very inexpensive to demand or use someone's social security number for all sorts of identification uses. It is so inexpensive, in fact, that the privacy-aware engineer is often looked at askance for pointing out that it makes a poor identifier. Similarly, requests for ID are so routine that few people bother to ask why, and we are compelled to show an ID each time we enter an office building, for "security" purposes.

2 Privacy Problem

The overuse of the social security number is widely acknowledged as a privacy issue today. Widespread checking of identity papers is not yet seen that way, but may be in the future. (As any 19 year old knows, getting fake ID is easy, and it doesn't need to be good, because a bar wants to serve customers. The move towards making bars liable for drunk drivers who drank there is an attempt to align liability with responsibility.)

Many of today's privacy issues, such as the widespread use of social security numbers, the internal passport regime in effect at US airlines, identity theft, etc, are a direct result of how inexpensive they are. There is no cost to asking for, or demanding, either.

I can't reasonably say at a skyscraper security desk that I don't have ID, because the government has issued everyone ID. When those IDs are run through a verifier, tracking everywhere you go at a central source, you won't be able to object. I can't tell an employer that I don't have these documents, because everyone does. Thus, the cost of privacy invasion is low; it is reasonable to require SSNs and IDs, because all your customers or employees will have them. There is no data protection law in the US that justifies a refusal.

These are privacy issues in the senses of anonymity; it infringes the right to be left alone, and it reduces informational self-determination. In addition, there are issues that may better be termed security issues, insofar as identity theft is now leading to false arrests, the loss of people's homes (an ID thief takes a second mortgage, drains the cash, and leaves the homeowner holding the debt.)

This lack of cost is a result of the government's provision of an ID infrastructure, and the ease of free riding on it.

By making these costs more explicit, we may be able to address them, or otherwise engineer privacy gains.

3 Risk Transference

The risks we discuss here are to the person, their dignity, their time, their financial security, and their liberty. There are not usually risks to those relying on the data. Thus, much like bars are happy to take fake ID, because the risk to them is small, and the reward is immediate, many organizations are willing to work from SSNs and drivers licenses because the cost is low, and the risk to them is small or nonexistent.

When a bank accepts two forms of ID at its office, rather than meeting twice in the home to be mortgaged, it is making a rational cost/benefit tradeoff. The pain, like the pain of British ATM customers, is not the bank's problem. [1] Similarly, when a credit card company offers credit through the mail, it has engaged in a cost/benefit analysis, and decided that checking ID for its new customers is too high a barrier, and is willing to accept and manage the risk of customer defaults. The pain to consumers of ID theft is ignored, or it is suggested that customers check their credit reports yearly. The absurdity of this as advice is obvious to most security experts. It is as if you checked your burglar alarm once per year. Much better to lock the doors. I don't wish to minimize the value created in the US economy by easy and fast credit. I am here focusing here on its costs, which are less well understood.

The people making security and privacy choices are not the ones who are affected by the institutional design effects of those choices. Those who do understand the design of the system are strongly coerced to remain within it. There is a large value to the users of the SSN/drivers license system in ensuring that everyone is part of it, but that neither that value or the costs are charged to them in any way.

4 Solutions

The problem of costs and risks not being properly distributed should now be clear, and the harder task of suggesting what could usefully be done, remains. Part of the problem is that the easy credit infrastructure is quite useful in allowing people to make tradeoffs about when they spend their income, and that helps to propel economic growth. (In particular, being able to plan to use future income to pay for loans allows people to more freely decide when to spend money. Credit's other effects, such as spending at a distance, seem less important for this analysis.) Tinkering with a system that works is always worrisome. However, the system is working for both honest folks and criminals today.

One obvious solution might be forgery-proof ID documents that could be checked. This is a security focused solution that ignores the privacy costs. Worse, an economic analysis shows that it will never work. As the documents become better, the value of the documents increases. As the value of the documents increases, the motivation of criminals to corrupt the creation system increases. A related

[1] Ross Anderson's "Why Cryptosystems Fail" showed that in counties with strong customer rights had less fraud than those countries, like Britian, where consumer rights are weaker, and the cost of fraud and the burden of proof could be assigned to the consumer.

solution is strong biometrics on documents, which, in training people to accept intrusive biometric testing regularly, is very bad for informational self-determination, autonomy and seclusion.

Another possibility is a law forbidding all non-government use of SSNs or driver's licenses. This is an aggressive suggestion, and objections are obvious. At the same time, it forces everyone to be explicit about their costs and benefits. For example, what are bars to do? A second ID card? Perhaps the police could station an officer at each bar. If we're serious about reducing under-age drinking, shouldn't we be willing to pay the cost, rather than imposing it on bars? (Perhaps this could be coupled with increased taxes on bars, so that drinkers pay the costs.) At airports, TSA personnel could either check ID or not. This would, at the very least, clarify John Gilmore's lawsuit.[2] On the other hand, perhaps other security measures are more cost effective, such as strongly reinforced cockpit doors, air marshals, or armed pilots. Most hospitals, banks, and credit agencies would need to re-tool to not use the SSN; however, that is a redistribution of cost, not an imposition. The costs of widespread use of the SSN today are imposed on the public, and under this proposal would be imposed on the institutions that choose to use it.

It is worth noting that in places with data protection laws, strong controls are placed on who may demand, and how they may use, identity documents. documents such as the Dutch passport

It would be difficult to implement such a system in the US, as laws covering what private companies are able to do are constrained by free speech and free contracting laws. One possibility would be to classify the information, and allow each individual an exception allowing them to see all information concerning themselves.

A more modest version of this proposal would be some form of liability for use of government ID that leads to a problem. This is challenging, because finding out where a criminal got their information can be nearly impossible. Fines for losing control of private information could be put into a fund to compensate ID theft victims. This has the advantage of creating an economic incentive to move away from the use of private information.

A more radical version of a liability rule would include personal liability for government decision makers who choose to mandate the collection of personal information. With great power comes great responsibility.

A last idea would be to create costs at the point of collection; a fee would be paid for the collection of the SSN, or the viewing of ID. Such a fee would be paid preferably to the customer directly, or to a victims of ID theft fund. This is an attempt to address the free-rider problem.

5 Conclusions

I have analyzed the growing problem of identity theft is from a risk distribution perspective. I have argued that much of the cost of identity theft is created by free-riding issues and inappropriate distribution of risk, and proposed solutions.

[2] Gilmore vs. Ashcroft, in which John Gilmore is suing to determine if there is a requirement that ID be shown to get on a flight, and challenge that requirement if it exists. See `http://cryptome.org/freetotravel.htm` for details.