Hal Berghel

Identity Theft, Social Security Numbers, and the Web

Privacy is lost in the proliferation of technology's omnipresent accessibility.

When one changes employers, as I have recently, the different institutional and cultural attitudes become obvious. For example, consider salary-benefit packages. From my perspective, as an academic for the past 20-plus years, employers seem to consistently bear about the same institutional cost for benefits—about 25% to 30% of one's salary. This is not to say that everything is equal; different employers emphasize different benefits options—a great group health plan may come at the expense of greater pension contributions, and so forth. But in my world, employer commitment to employee benefits appears to be a constant.

What does this have to do with identity theft, social security numbers, and the Web? Well, one of the institutional differences I noticed with my current move was the widespread use of SSNs as primary keys within university administration, municipal and state government, and a good percentage of utility and communication companies. In my effort to explain to sundry administrative folks just how dangerous the practice of using SSNs as primary keys and authenticators in their databases is, how it exposes the employees and citizens to unnecessary risk. I composed what became the first draft of this column. The use of SSNs for purposes other than that for which it was intended is an exceedingly bad idea. This point has been made many times. Add the Web, and we have the makings of a disaster that makes the recent Y2K computer problem pale in comparison.

MARTIN MAYO

Social Security Numbers

The Social Security Act that defined the U.S. government's attempt to establish an old-age pension system was enacted in August 1935, as one of President Roosevelt's many depression-era relief, reform, and recovery programs. Originally intended for retirement alone, the Act has been periodically amended to include survivor-benefits coverage and disability payments. A by-product of this legislation was the decision to assign every citizen who qualified for social security benefits and/or contributed a social security tax the unique record identifier which has come to be known as the social security number. The intention was that the SSN would be used as a primary identifier only within the Social Security administration.

Then things began to unravel.

The first loose thread appeared in 1943 when the Roosevelt administration (Executive Order 9397) authorized SSNs as primary keys for other government databases. Although this practice ended in 1975 because of a change in policy brought about by The Privacy Act of 1974 (www4.law.cornell.edu/uscode/5/552a.html), by then the toothpaste was out of the tube.

The Privacy Act prompted a number of changes. For one, it required some disclosures of the federal agency that requested SSNs. The law mandated that any government agency except the Social Security administration must provide a Privacy Act Disclosure Notice to SSN owners explaining (a) by what authority they are entitled to know an SSN; (b) the intended, primary use of the information; (c) other secondary uses that might be made of the information; and (d) the consequences of refusing to divulge this information.

Second, it relaxed the disclosure restrictions for state and local governments. In this case, (a) and (b) were combined with (c)—the disclosure of whether the request for SSNs is mandatory or voluntary. It is noteworthy (and a major cause of alarm in some circles) that there is currently inadequate legal remedies for violations of the Privacy Act by states and municipalities. It is more noteworthy (and an even larger cause for alarm) that there are no explicit prohibitions or penalties for the use of SSNs in business and commerce.

Finally, the Privacy Act recognized the legitimate use of SSNs as primary keys for all federal agencies who used them as such prior to January 1, 1975, thereby ensuring that the toothpaste would never find its way back into the tube.

So, by 1975 SSNs were in widespread use within the federal government and available for use by state and local governments subject to disclosure constraints under the Privacy Act. The Tax Reform Act of 1976 expressly authorized the use of SSNs by state and local revenue offices, licensing agencies, and so forth. To reuse my tired and worn metaphor, by this time the tube was all but empty. But the big threat to privacy was over a decade away.

The popularity and widespread use of SSNs within governments—whether federal, state, or local—made SSNs a popular choice among business and industry as well. Once the proprietary information of the first giant government entitlement program, SSNs had in just under 40 years started to take on the character of a reliable, persistent, personal, public use identifiers—which is specially ironic given that the original intent was that they were "not to be used for identification." By everyone's agreement, the Social Security administration never intended SSNs to be used by the public or commercially, but that hasn't impeded their evolution. This misuse has caused and is causing many problems, and the worst is yet to come.

Not All Personal Information Is Equal

There are, to be sure, different points of view regarding the unintended use of SSNs. Some would argue that the non-Social Security administration (or at least the non-government) use of SSNs makes it far too easy to infringe on personal privacy. Others would point out that the U.S. Constitution makes no mention of any right to privacy in the first place, and that the use of SSNs for commercial purposes is completely legal so long as it confirms to the relevant statutes, and is completely ethical so long as SSNs are used responsibly. One might argue that if an SSN was obtained legally (say, through lists obtained from licensing bureaus, credit bureaus, or even an occasional warranty response card list), then the responsible reuse by those who purchase these lists is entirely legitimate. The Direct Marketing Association, for example, defines "responsible use" in its codes of conduct, which it demands of its members if they are to be allowed to use the DMA seal of approval.

Consider the following quote from the Better Business Bureau on sensitive data: "Not all personal information is equal. Information, like a social security number or mother's maiden name, is far more sensitive than a name and address that can be found in a phone book. A mother's maiden name is often used to confirm identity and is especially sensitive information." (see www.bbbonline.org/consumers/tips.html). The message is emphasized again on the Bureau's Web site under "online shopping": "Be cautious if you're asked to supply personal information, such as your Social Security number or personal bank account information. They should not be required

to make a purchase." (see www.bbbonline.org/consumers/tips.html.) As an anecdote, I recently purchased a car from a dealer who was apoplectic over my refusal to provide my SSN, my home address, and my telephone number for the sales contract. But in the end the dealer wanted the cash more than the information, so the deal was consummated. The plain fact of the matter is that if credit isn't involved, there's never a reason to give out an SSN. And if credit is involved, there shouldn't be—but we're getting sidetracked.

But this column is not about the debate over the legitimate right to obtain information about individuals versus their desire for privacy. It is not about issues of states rights, or primary keys, or whether the commercial use of SSNs is in the public good. This is about the use of SSNs as an instrument of crime—and the use of the Web as an unwitting co-conspirator.

The plain fact of the matter is that if credit isn't involved, there's never a reason to give out an SSN.

Privacy and the Web

Concerns about the impact of digital networks on personal privacy have been raised as long as there have been digital networks. For the past decade, researchers and developers alike have created a formidable array of utilities and tools to protect Internet privacy. These include:

- Web anonymizers (see www.anonymizer.com) that redirect Web accesses so packet headers are sanitized of information identifying the source of the request;
- Remailers (see www.zeroknowledge.com) that redirect email so that the source maintains anonymity;
- Encrypted pseudonym services (see www.zks.org) that generate the pseudonyms on behalf of the client as the messages pass through the server;
- Encrypted authentication environments (www.xs4all.nl/~freeswan/);
- Online Web monitors that report back to the client when information about them is accessed or stored (see www.privacyinc.com); and
- A variety of combinations thereof (www.int.c2.net/).

Offsetting such technology are utilities such as

- Snoopware (see www.hitekinfo.com/) that locates personal data on the Web;
- Stealthware (see www.winwhatwhere.com) that monitors client-side user-behavior;
- Persistent identifiers—in both soft and hard cookies, (for example, Intel's 96-bit Chip ID on Pentium III processors); and
- ID counterfeiters (see www.fakeid.net and www.photoid.com).

All of this takes place in the context of government anti-privacy initiatives such as the Clipper chip and the recent judicial decisions in the Pillsbury Case, determining that employees have no legitimate right to expect privacy from email that passes through an employer's network.

Identity Theft

Identity theft will be the undoing of the blissful ignorance we have maintained with respect to the misuse of SSNs. As any victim can attest, identity theft can destroy personal credit and potentially lead to very expensive litigation that may take years, or perhaps decades, to fully correct. And computer technology is right at the heart of the problem.

Identity theft works in the following way: important information is compiled on someone with good credit. Likely sources include:

- Personal information discarded in trash,
- Intercepted mail,
- Phone books,
- Subscription lists,
- Personal artifacts through theft and robbery,
- Phony telemarketers,
- Credit card carbons,
- Calls to unreputable 800 and 900 telephone numbers,
- Court records,
- Motor vehicle departments, and
- The Web and the Internet.

Of all the pieces of information to be gained, SSNs are the holy grail of identity thieves. With these numbers, one can potentially access all of the databases that use SSNs as primary database keys. Where pre-cyberspace thugs concerned themselves only with the cash and credit cards in a wallet, thereby limiting the "take" to the sum of the cash and that part of the credit limit that could be captured before the cards were cancelled, the bounty of the identity thief is the person's entire credit worthiness—their ability to buy homes, cars, and obtain educational loans. Everything! In urban areas, identity theft rings eagerly pay a premium for stolen wallets that contain SSNs and other identifying data; stolen credit cards can be left for the street urchins.

Of course, this would be a problem even if it were not for the Internet. Personal records in each state and municipal database could be accessed with very little information—an SSN, a mother's maiden name and address are a few examples. But what complicates things is the reckless abandon with which we have allowed

URL Pearls

The first place to start is, of course, with the **Social Security administration** (www.ssa.gov). There's a wealth of useful information on this site. A few historical points of interest might be the explanation of the SSN numbering scheme (www.ssa.gov/history/geocard.html, and the enumeration chronology (www.ssa.gov/history/ssnchron.html). Note that the Social Security administration is aware of the privacy concerns of citizens following from the misuse of SSNs.

• The **Better Business Bureau** has a number of useful sites. The main site for the parent organization is www.bbb.org. Another BBB site which is oriented toward online commerce is at is www.bbbonline.org. This site contains consumer tips and advice for online shopping. A third site is the Better Business Bureau Consumer Assistance Center (www.bbb.org/library/ outsideResources/index.html).

• The **Electronic Privacy Information Center** (EPIC), is a de facto clearing house for privacy-related documents and activities (see www.epic.org)

• The **Computer Professionals for Social Responsibility** site (www.cpsr.org), and derivative documents found therein (e.g., www.cpsr.org/cpsr/privacy/ssn/ssn.faq.html), provide the reader with an excellent, current overview of the important issues. The writings by Chris Hibbert are especially useful in terms of the history of SSN misuse, including useful links to the Federal Privacy Act of 1974. Hibbert's short essay, "History and Significance of the Social Security Number," is a must-read.

• **The Direct Marketing Association** (www.the-dma.org) includes the Mail Preference Service (MPS) page that enables you to request removal of your name and address from DMA member mailing lists, and the Telephone Preference System (TPS) page which does the same for telephony. But don't look for online convenience here. The extent of the automation of the removal process is access to DMA's online form which you have to print out from your browser, manually fill in, and send via snail mail. Whether this inconvenience is a result of their need for an original signature or to create additional transaction friction to discourage name withdrawl, is an open question. It should be mentioned that name withdrawl from the DMA email mailing list can be done via email, but the removal of a name from the DMA member lists requires hardcopy. Also, widespread and unnecessary use of frames without any navigational aids makes travel through the site confusing and awkward.

• Illustrative privacy policy statements such as that from **Michael Dell** (www.dell.com/us/en/gen/misc/policy_003_policy.htm), the Direct Marketing Association (www.thedma.org), and the ACM www.acm.org/serving/acm-privacy.html), provide an idea of how different organizations are reacting to privacy concerns.

• An excellent source of information on Identity Theft is **Travis Perry's FutureCrime Prevention Association** (www.futurecrime.

the collection and dissemination of highly personal and confidential information on the Web. In the absence of prohibitive legislation and substantial penalties for noncompliance, cyberspace is becoming a paradigm of untrustworthy systems.

Our two themes, the history of misuse (or at least unintended use) of SSNs on the one hand, and the evolution of privacy concerns with respect to the Internet and Web on the other, intersect at identity theft. This may prove to be one of the most negative consequences of the Web. Identity theft and sundry-related computer crimes ported over to the Internet may become an unparalleled, destabilizing force for 21st century society to deal with. And yet it never had to happen. If only the Social Security administration had held on to its proprietary identifiers, and the Web had evolved with provisions for regulating the posting of identifying data, this problem could have been avoided. By Travis Perry's estimate, there are 500,000 cases of identity theft each year. By law enforcement accounts, identity theft is the fastest growing crime in the U.S.

In the end, society will have been the victim of two well-intentioned concepts, which, just through a few twists of fate, will come together to produce a great deal of harm. One would think that after dealing with the industrial revolution, the space age, radio and television, the computer era, and now digital networks, we would have learned to be more socially responsible with our technology. At this point, the price for even modest security is perpetual vigilance. C

com). For a nominal amount, Perry will supply a booklet and instructions on how to lessen personal vulnerability to identity theft. The site is worth a look.

• **The Ultimate Internet Spy Tool's** (www.hitekinfo.com/snoop/snoop.html) splash page says it all: "Let me show you how to 'tap into' EVERYTHING ON EVERYONE! The complete scoop on your enemies, employees, boss, or anyone else ... and that includes YOURSELF!

Some discussion of privacy issues with regard to email can be found in my column, "Email: The Good, the Bad, and the Ugly," *Communications*, Apr. 1997 (online preprint at www.acm.org/~hlb/col-edit/digital_village/apr-97/dv_4-97.html). A very general discussion of some key terms relating to Web security and privacy issues in our article on the Web in Marv Zelkowitz, Ed., *Advances in Computers*, Vol. 48, pp. 179–217, 1999 (online preprint at www.acm.org/~hlb/publications/web99/web99.html).

Hal Berghel (www.acm.org/hlb) is a professor and chair of the Department of Computer Science at the University of Nevada at Las Vegas.