recently had occasion to take my son to his first chess tournament. We were asked to bring chess clocks, so I dutifully searched through the house to locate my old chess gear from my own tournament-playing days. I was rather dumbfounded when I pulled out my old chess clock and found my last name and my US social security number (SSN) prominently displayed on top of it.

Engraving my SSN was meant as an identification tool, in case the clock was lost or stolen, and I believe my father used it on numerous pieces of personal property. This was, of course, long before the days of identity theft, and I guess it made sense at the time. These days, I've lost count of how many times I've been warned that some institution with which I was once involved had detected the theft of personally identifiable information, such as SSNs.

Of course, countermeasures do exist, such as fraud alerts with credit-reporting agencies. These tend to expire unless you arrange with yet another agency to renew them periodically, something I've done. The intent is to raise the bar and require me to authorize the release of credit information, but it's hard to tell if it ever works. One company advertises that it will protect your credit and, to prove it, announced its CEO's SSN right over the radio. Perhaps there's hope.

**Mistaken Privilege**

By now, a few of you are probably wondering what this has to do with the Internet, so let's look at some IC-related anecdotes.

In the past, companies frequently used SSNs for identification. To take attendance at mandatory meetings, one employer I once worked for passed around a paper on which we each put our name and SSN. Organizations have also used them for medical plans, pharmaceutical benefits, and so on. A few years ago, the US government cracked down on this practice due to privacy concerns, and in general few companies or organizations use SSNs as an identifier anymore.

My previous employer at some point established a single sign-on mechanism for accessing most of its intranet sites. It set up a separate “human resources ID” that let it better control access to the most sensitive personal information in the HR system. When I joined IBM, I found that there, the same intranet sign-on controls access to HR as well as all other sites. The company policy is that we should use this password via HTTP authentication (meaning that the password itself isn't transmitted to the Web server), but, in fact, a huge number of intranet sites require me to enter such credentials in a Web form. An unscrupulous programmer could, I imagine, record this information and then access HR and other sensitive systems. Such accesses would be logged, but how long would it take to notice them? If a rogue trader could lose billions of euros without being detected for months, I don't have high hopes for this sort of protection.

**Internet Presence**

I recently tried to locate someone on the Internet whom I hadn't contacted in some time. I thought he worked at company X, but a simple search showed that in the recent past, he was at company Y. However, although my searches found references to him appearing on panels and giving invited talks, they didn't give me an actual homepage with personal contact information. The same is true of other computer professionals I've tried to locate: they might have a Web presence from student days, but to all
Not-so-Secret Identities

intents and purposes they’ve disappeared. Why?

One possibility is the burden of maintaining such information. Someone might feel it’s better to have no Web presence than to have a dated one. Or maybe such people procrastinate and simply never create the presence in the first place because they don’t want to do it until they can invest the effort to do it well, in which case, simply listing contact information isn’t sufficient.

Another possibility, and one that I subscribe to, is that these people are consciously hiding. Moving to a new job and a new email address is an opportunity to escape from all the spam sent to your old address; the moment you expose the new address online, you’ll get deluged all over again. People might feel that those who need to reach them will know how to do so. In fact, I asked a mutual friend about the whereabouts of the person at company Y, and he said that he too had been trying to locate him without success, despite them being very close in the past.

Of course, spam isn’t the only risk you take having a visible Internet presence. Roughly a decade ago, I received mail from a complete stranger named “Chris” saying something like, “Your daughter is cute. Do you have more pictures of her?” I panicked, thinking how weird this was. I immediately password-protected the area of my Web site that had things like family pictures (and I know many others do this as well), and I asked Chris what brought him to me. He said, “I typed find pictures of kids into a search engine.” I might believe that search engines today would tie those together and produce my daughter, but I had a lot of trouble believing it back then. When I didn’t send additional pictures, Chris sent another note saying “Since you won’t send me another picture, I’ll send you one of me.” It was a picture of a girl a few years older than my daughter, holding a stuffed rabbit similar to the one in the picture Chris had commented on; “Chris” was apparently a young girl, not the older male pedophile I had feared. But on the Internet, no one knows you’re a dog, and no one can be sure you’re a girl with a rabbit. I’m inclined to go with my first reaction here.
True Names

Of course, one way to find people on the Internet these days is through social searches (see the special issue of *IC* from November/December 2007). You can feed a name into a “generic” site such as Facebook or MySpace, a professionally oriented site such as LinkedIn, a specialized people-finder such as Spock, and so on. I tried looking for the mysteriously absent company Y person this way — to no avail — but searches on such sites can be risky due to mistaken identity. In my case, I have what might well be a globally unique name because my last name is spelled in an unusual fashion. People who look for me and spell my name correctly will find me, but many people in multiple companies are named “Fred Douglas” and have received my emails, been invited to meetings in my place, and so on.

When people do have the same name, disambiguation is a pain. A recent *Communications of the ACM* article on document identifiers discussed the problems of people with names in common or that are misspelled. Thus, statistics on data such as citation rates can be skewed.

In my case, LinkedIn offered to connect me with former colleagues several months ago by listing their names and titles. I connected to someone with whom I had worked, and he accepted the connection. A few weeks ago, I realized that this person had the same name but a completely different set of experiences from the person I knew. So much for establishing trust.

So how can we combat these issues? Here are a few thoughts about best practices for Internet/intranet identity:

- Companies should move away from the “single sign-on” idea and accept that different types of information require different levels of security. One password doesn’t fit all.
- The notion of unique “document identifiers” doesn’t go far enough. We need unique “person identifiers” that aren’t sensitive but can be used to disambiguate people. Then we need a way to record those identifiers to associate them with the right people. Some systems, such as LinkedIn, are starting to serve in this capacity, in the sense that once I’ve connected to someone, I should be able to find them regardless of how their email address and other contact information change in the future.
- Finally, if you want to fall off the grid, at least leave a few breadcrumbs for your old friends.

P.S. Does anyone have an engraving tool I can borrow? There’s a chess clock I have to anonymize.

Acknowledgments

The opinions expressed in this column are my personal opinions. I speak neither for my employer nor for *IEEE Internet Computing* in this regard, and any errors or omissions are my own.

Reference