Indecent Exposure

The Internet can make some things a little *too* easy to find

by Simson Garfinkel

25 July 1997

I had a girlfriend in college. I was crazy about her, but I was also a jerk. In October 1985, she dumped me and started seeing somebody else. I freaked out and she stopped talking to me. I didn't get over her for years.

The other day I was wondering where she was and what she was doing. So I typed her name into one of those Internet people-finders and there she was, with an email address at some college in Canada. A few more clicks and I learned that she was a graduate student in the physics department - a big departure from her undergraduate studies. A few more clicks and I had her home address and phone number.

For years the digital avant-garde has been telling the world that "information wants to be free." (A search on HotBot turns up almost 2,000 Web pages containing the phrase "information wants to be free," by the way.) Today we are perilously close to realizing that dream. Fueled by dramatically reduced distribution costs and advertiser support, databases that used to cost thousands of dollars per year to rent are now freely available on the Internet. But while modern technology and new business techniques have dropped the cost, they haven't given us tools to deal effectively with the consequences.

Last January, I received a threatening letter from a person about whom I had written a year earlier. "The party is over!" the letter started. "You are libeling me and my company and I am taking appropriate actions unless you cease and desist forthwith."

What these "appropriate actions" might be I had no clue, but the writer made it clear that he would seek to damage my reputation, make me lose my job, portray me as a scoundrel in the eyes of my neighbors, and shake up my marriage.

So how had this man found me, and why had he waited so long to seek me out?

Presumably the same way I had found my ex-girlfriend: He had gone on the Internet and typed in his name and his company's name. And there, between the search results pointing to his Web site and those pointing to the electronic mall in which his company resides, was a link to my February 1996 article about Jeff Slaton, aka "the Spam King," in which I had quoted my now-threatening letter-writer.

The first threatening letter was followed by a second and a third. At that point, I contacted an attorney, who sent some letters of his own. Ultimately, the threatening letter resulted in a bunch of lost time and money spent on legal fees, but nothing changed either on or off the Net. Search engines are good at helping to catalyze this sort of tempest in a teapot; they make it easy for people to find things they find personally upsetting.

I'm not the only journalist who is struggling with this new form of accountability. Over at The National Association of Science Writers, a professional organization to which I belong, participants of the NASW-talk mailing list are struggling with the fact that Internet search engines are now indexing the association's archived mailing lists (like NASW-talk). The archived mailing lists are supposed to be open discussion forums where people interested in science writing can talk about the issues. The problem is that the people being talked about in this not-for-publication forum might do Web searches on their names and find out what is being said about them.

Part of the problem here is the dual nature of archived Web mailing lists: They are both private discussions for their members and lasting publications for others to read. Perhaps this dualistic nature wouldn't matter if it wasn't so bloody easy and cheap for a person to do a Web search and find out if they have been mentioned on any Web page, anywhere in the world. But it is, and in fact it is getting cheaper and easier, rather than more expensive and more difficult, to scan the Web for every mention of your name.

But personal information is just one kind of raw data that's being made available for free in this new information-rich economy. There are now Web pages that can give you free access to once-expensive databases like Medline, issued US patents, and the entire US Code. Meanwhile, more businesses are setting up Web pages containing valuable price and inventory information - just the sort of competitive information that used to cost big bucks through research firms a few years ago. What's missing from much of this free information is analysis that puts it into context. In this new world of free online information, thinking costs extra.

In fact, many businesses have become so blasé about giving away information for free, they've left themselves open to a new kind of corporate espionage: Internet intelligence-gathering.

Last November, I wrote about how the Internet's domain name system (DNS) could be used to snoop on other companies. Using standard utilities that are shipped with most versions of Unix, you can use DNS to obtain a complete list of every networked computer used by a company, and their Internet addresses - just the thing for mapping out your competitor's network. I looked at three companies that were giving away this valuable proprietary information: Sprint, AlterNet, and Hewlett-Packard.

In the eight months since that article was published, Sprint and AlterNet have tightened up the security on their corporate nameservers, but HP's is still wide open. (They have roughly 4,700 Internet-capable hosts behind their corporate firewall.) Meanwhile, UUNET Technologies, AlterNet's parent company, has a corporate network with roughly 3,000 hosts - of which 566 are apparently Macs, three are Radius authentication proxy servers, 13 are mail servers, and 1 is a dual fax and mail server. If an MCI executive called up UUNET and asked them how many Radius mail servers UUNET was running on its internal corporate network, you can be sure they would tell him to take a hike. But out there on the Internet, UUNET is making the same information freely available.

WhatsUp Gold is a powerful network-monitoring tool that runs on any Windows 95 or Windows NT-based computer. The program builds a list of sets of computers on your network, figures out which services they are running, and then checks them every few minutes to see if they are still up. Once it's running, WhatsUp will show how often a particular service is up (or down), how fast the machines respond, and other useful pieces of information like that.

What's neat about WhatsUp is that it doesn't rely on any special network-monitoring protocol. Instead, it just checks standard services: domain name service, file transfer protocol, HTTP, gopher, email, ping, and so on. Why not? After all, it's those services the typical network administrator is interested in watching. But by using these publicly available services, WhatsUp makes it easy to monitor a network belonging to somebody else.

When you install WhatsUp, the program prints this curious warning message:

> Note:
>
> Do NOT monitor host systems, workstations, or other network elements that you do not have control of without the express permission of the owners of those network elements.

In other words, even though WhatsUp makes it easy to do, you shouldn't use the program to play corporate spy.

Other companies with similar products take a more laissez-faire approach. Donald LaMure, sales manager at Castle Rock Computing, says he sees nothing wrong with people using his company's SNMPc Network Manager to eavesdrop on other systems. "In general, we do not feel it is ethically wrong to monitor networks and devices that are out on the Internet. Security should be the responsibility of the company" that is being monitored, he says.

Neither of these approaches make any sense. You might think that monitoring other people's networks without their permission is bad, but you are not going to stop it by telling your customers that the practice is unethical (although you might skirt a lawsuit). Likewise, companies can't take control of their computers and prevent their competitors from monitoring network services that are freely made available to other machines. And to prove the point, I monitored the Web servers at www.microsoft.com. Over two days, it rejected my HTTP requests just 5 percent of the time. Not good.

So what do my ex-girlfriend, the good journalists at The National Association of Science Writers, network providers like Sprint and UUNET, and various people with Web servers on the Internet all have in common? By virtue of taking part in the new electronic economy, they are making information about themselves available - and they have all pretty much lost control of what's done with that information once it gets out.

By lowering the cost of collecting and disseminating information, and by making monitoring easy, the Internet is becoming a culture and an economy that accepts and promotes widespread surveillance. But whereas the technical framework for building our electronic-surveillance economy is being quickly assembled, we have no idea what the social or political costs will ultimately be. Very soon, we may yearn for the day when information wasn't free.

Should network monitoring be regulated? By whom?

Related links:

HotSeat with Simson and two monitoring-software makers

Members discuss selling personal information

Simson advises employees to look busy

synapse