virginia edu
The Information Technology Magazine at the University of Virginia

The Information Police

by Chip German
Director, Policy and Strategic Planning
Office of Information Technologies
University of Virginia

A few years ago, an organization trying to weather a public scandal heard a rumor that reporters for the local newspaper had staked out its dumpster, and every time someone delivered new garbage to it, these Pulitzer-hungry writers would pick through the refuse, looking for that one document that would place a smoking gun in the hands of someone richly deserving to be crucified on the next day's front page. The organization quickly installed a $300 paper shredder in each of its offices, along with a new policy that all documents would be shredded before disposal. For about a week, mounds of shredded paper in large plastic bags filled the dumpster and spilled out on the street, but only after temporary help was hired to handle the time-consuming job of feeding the shredders. Then the number of bags started to diminish gradually, as the shredders increasingly fell idle from lack of compliance, and supervisors started letting the temporary staff go. Soon several organization executives were indeed crucified on the front page, not because someone pieced together the smoking-gun document from shreds in the dumpster, but because of an anonymous whistle-blower. Who knows what would have happened if those shredders hadn't been there? The moral: see what happens when you don't spend enough money to protect your information?

Okay, maybe that's not the moral. Maybe the moral is the opposite point. Information security problems can happen no matter how much money you spend. Or another point—the greatest security vulnerability is human. Anyone who's heard the recent news about the FBI man who was a spy for the Soviets and later the Russians understands this point. A significant national security failure is alleged to be the work of a human deeply placed in the security infrastructure, not because of technical failures in that infrastructure. Then there's the notion that's known among the security experts as the social engineer. Although in other contexts this has a different meaning, in systems-security terms, it sometimes refers to a con artist who manages to convince you to simply tell him or her your biggest computing secrets, such as passwords. A criminal doesn't have to possess sophisticated hacking tools and know how to use them if we can be duped into giving up—in human-to-human conversation—the very things needed to break into our accounts. And it doesn't only happen with little old ladies and slick door-to-door operators trolling for easy marks. Now, keeping all of that in mind, the quest for real information security seems futile. So why should we even try?

Don't give up yet—maybe looking at this question from a different angle will prove more fruitful.

Don't hold your breath.

Y2K has come and gone, and everyone who could make any money on that looming-disaster-turned-non-event has gone prospecting for new and fertile territory. Those folks may have found it in information security. And just like Y2K, there's enough truth to the risk they describe to grab our attention and to feed our always-hungry appetite for crisis. After all, this is America—if it ain't crisis, we don't pay attention. If you don't believe it, listen for how the politicians talk about information security. But could it be that the technology prophets working this territory are really trying to sell us expensive, whiz-bang stuff to fix a never-ending progression of obscure security holes when perfect security is a pipe dream? Don't we remember that security in the old paper world wasn't perfect either?

So, when does blind pursuit of complete security block us from reaping important benefits of the Information Age? And, the reverse—after chasing every possible technical solution, only to be thwarted by a human failure, why bother with security at all? The answer, as always, grasshopper, is balance.

Let's examine what these terms "privacy"[1] and "information security" really mean to me.

As an individual, I start from concerns about simple privacy—my information shouldn't be available for inspection by anyone I don't specifically want to see or know it. In its purest form, I'd call this protection from information voyeurs—the satisfaction they seem to get isn't exactly sexual (the usual application of the term "voyeur"), but it does involve greater intimacy with me than I want them to have. An increased-intensity version of this same point is the notion that we don't want other people to link together disparate information about ourselves from various sources. Whose business is it that I like National League baseball, Ravel, blues, ice cream, and short stories?

But voyeurs who are getting their jollies from knowing things about me that I don't want known are a lower concern for me than protection from individual wrongdoers whose ill effects are more direct—people who not only view the information but do something with it that harms me in some way. My usual fear (and probably yours) for this form of violation of my security is that someone is using my confidential information to pretend to be me so he or she can improperly and unfairly cost me money. Or, perhaps they aren't directly costing me money as much as they are pretending to be me to avoid responsibility for some other, often illegal, action (it could involve damaging a computer environment; it could be the current champion of nuisance behavior—spamming—in my name). I also include in this category persons who pretend to be me in order to play a joke on me—rarely do they understand the damage they do in the process.

In another category altogether are organizations that use information about me to my disadvantage (including by damaging my reputation)—i.e., medical information that improperly becomes available to potential insurers who then use it as a basis of discrimination; credit information that is used to deny me the opportunity to conduct some financial transaction; politically sensitive information that is used to damage my credibility as a public official or when campaigning to be one (fear not—as if you need to know—I will not pursue nor will I accept any party's nomination for anything).

---

[1] Definition of privacy from an online source: *privacy—the right to be left alone. Privacy includes both freedom from government interference in private or family matters and confidentiality of such things as personal correspondence, telephone calls, financial information, and medical histories. Courts in recent years have recognized a right to privacy implicit in the United States Constitution and Bill of Rights, but there are concerns that privacy may be eroded by the widespread use of advanced information technologies.*
"Privacy," Microsoft Encarta Online Encyclopedia 2000

Speaking of elections, another of our privacy concerns commonly involves fear of intrusion by government—what should the government (local through federal, the police through the IRS) know about me, and how easy should it be for the government to add information about me to its files?

I have to pause for a moment here to admit that there is a hint of paranoia in everyone's concerns about online privacy and information security. But I'm an American and as such I'm culturally predisposed to be proud of my paranoia about privacy (although there are some American exceptions—information exhibitionists who seem to enjoy exposing their private lives online). True enough, it may be theoretically easier for someone to find information about me because of the increasing availability of networked computing and the increasing amount of personal information stored in ways that can be touched by that environment. However, the number of persons whose information is kept in such circumstances is growing exponentially, too. The likelihood that someone would want to target me or any other individual who is not making national headlines is fairly remote. It must be our recognition that someone could find information about us that drives our fears. So what is the real risk to any regular individual? Here's where each of us needs to examine relative risks. Remember the old example? It has been said that a higher percentage of the population is afraid of flying than is afraid of traveling in a car, but the chances of death or serious injury are actually greater each time you step into a car. I suspect it may be so with online information. We already know that the risks of bad consequences for handing your credit card to a stranger in a store or a restaurant are greater than giving that credit card information to a reputable online vendor. But most of us accept those risks every day.

We've looked at what information security means to a reasonably representative individual (me), so now let's consider what it means to an organization. Of course, any concerns about information security will shift in meaning and emphasis depending on the nature of the organization. But some of the concepts seem universal.

From an organization's perspective, simple security means that information on customers or clients isn't available for anyone those customers or clients haven't authorized to see it. By safeguarding simple security of information, the organization fulfills the trust of their customers or clients, and that trust is a sensitive and vulnerable thing. If the organization violates that trust in any way, including the failure to take proper steps to protect the information, the customers or clients will withdraw it and discontinue their affiliation with the organization. Business leaders use this rationale to argue that most ideas for new, more stringent regulation by government with respect to privacy and security aren't necessary. It is in each organization's own self interest to ensure that information security is never compromised and that the organization adheres to its published policies and practices with respect to privacy and security.

Paul Misener, vice president for global public policy at Amazon.com, spoke about this on March 1, 2001, at the University of Virginia:

> As you may have heard, privacy bills tend to touch on two or more of the four fair information privacy principles, which are notice, choice, access, and security. Of these, the only obvious candidate for consideration is a requirement that online sites provide users some notice of the site's privacy practices. With such notice, consumers can decide what balance of privacy features they desire, and the Federal Trade Commission already is empowered to force Web sites to live up to their promises. And because the FTC has this authority, private rights of action must not arise from new

> legislation. Federal regulators can handle these issues in a much more rational and uniform way than class action plaintiffs' attorneys.

Perhaps the most worrisome risk in this arena is that commercial organizations that you trust with personal information—information that was given with assurances of the policies with which it will be handled—may go out of business or merge, and their assets may be transferred to another entity that handles personal information in a different way. In the volatile commercial environment of Internet-based companies, this has the potential to affect all of us. But as Misener said, the governmental capacities to deal with this are already in place. Indeed, the FTC has acted forcefully and set important precedents in several instances, most notably in this context in the Toysmart, Online Pharmacies, and ReverseAuction.com cases (see the FTC Web site for details).

Although I agree with Misener's perspective in general on this point, I wonder if one additional issue that should be considered is a requirement for public disclosure of security incidents in which customer or client information was actually compromised. Although some commercial organizations have volunteered such disclosures in the past, they probably had no choice—the news about an incident was going to become public anyway. It isn't hard to imagine that—with the stakes for an organization so high—it might hide such news to avoid a stampede of its customers. And there is another level of disclosure requirement that might be advisable—disclosure by security-services organizations that provide services to, for example, a retail organization that makes the promises about security and privacy to its customers and clients. What real guarantee does the online retailer have that its security contractor will tell it if there has been a security incident that exposed information on the retailer's customers?

But clearly the forces of balance are already at work at the organizational level. I'm inclined to believe that, as Misener said, policy makers, like doctors, should first do no harm:

> All other things being equal, of course we all want more privacy! And, of course, we want better service! And, of course, we want more personalized service. And, of course, we want lower prices! It's simply a matter of balancing these qualities.

As individuals, we probably don't need more information police. Instead, we must find the right balance in our own behaviors. We protect our privacy best when we assume a reasonable degree of personal responsibility for it. We have to realistically evaluate relative risks, and we have to act accordingly. Throughout this issue of ***virginia.edu***, you'll find ideas for safeguarding your information. Some of the most obvious involve simple notions:

- Don't volunteer personal information about yourself when you're not sure how it is going to be used (online or in printed product registration forms that you send back to manufacturers, for example).
- Understand the technology that you use well enough to have reasonable confidence and competence in its and in your capacity to protect your privacy to a reasonable degree.
- Don't frequent neighborhoods in which you're not confident about your safety online or in the real world. In the online world, an important step is to read and make sure you understand the privacy policies of the entity with which you're considering interacting.
- Remember that the biggest risk to your privacy and security is human, not technological. And that human risk may just be you.

virginia.edu, Volume V, Number 1, Spring 2001

Published by the Office of Information Technologies (OIT) and the Department of Information Technology and Communication (ITC) at the University of Virginia