Society Cannot Function Without Privacy

In most civilized societies, the privacy and confidentiality of many individual activities has long had the benefit of legal protection—often to the annoyance of law enforcement officials. Such activities include consultations with an attorney, most (but not all) confessions to a priest, and some (but definitely not all) secrets shared with mental-health professionals. Whispering sweet nothings into someone's ear enjoys de facto privacy; why should the same sentiments conveyed over a telephone call or Internet connection not receive the same?

MICHAEL CALOYANNIDES
Mitretek

Many in the law enforcement business pontificate that the only reason someone would want to keep information and activities private is that such data would be incriminating. Yet this is clearly false. Privacy and confidentiality are essential to commerce, for example, and modern economies would collapse without them. Every individual and company must protect the confidentiality of its developments from competitors (hence the legally protected notion of *proprietary* information). Moreover, civilized individuals rightly want to keep many activities, such as visiting the restroom or engaging in conjugal relations, to themselves. The same is true of facts like whether we dye our hair or have funny moles on our behinds, or which prescription medications we take. All individuals form hierarchies of privacy: some things are shared only with family, others with close friends, still others with medical doctors, and some subset of the rest (if any) with total strangers. None of these conventions has anything to do with wrongdoing.

Personal boundaries

We do not paste our correspondence, tax returns, or personal diaries on our windows for the benefit of passers-by and police, and we do not publicize our social security or credit card numbers. We must protect ourselves from any loss that prudent precautions could have prevented. This means not only protecting our property, such as houses, cars, jewelry, cash, or other valuables, but also protecting information whose compromise can result in such obvious illegal acts as credit card fraud and the increasingly popular identity theft. Otherwise, as individuals, we risk being denied insurance coverage for losses or even being unable to qualify for loans because of damaged credit reports. It follows that we have the legal and civic obligation to protect not only our "things" but also information about us and our families. Indeed, protecting our information is what privacy is all about, and it is part and parcel of living in civilized society.

Far from "hiding crimes," proactive protection of confidential information is not only a very prudent effort to prevent crimes, but actually required in many situations. In the US, for example, failure by healthcare providers, insurers, or clearinghouses to protect data pertaining to medical privacy exposes them to criminal penalties that include up to 10 years' jail time.

Ironically, industrialized countries are far more vulnerable than less-developed countries to criminality and national security threats that result from data warehousing.

Regardless of what we purchase and where, we expect full anonymity and privacy when we pay with cash—much to the consternation of stores that try to extort us with higher prices unless we surrender this time-honored anonymity by using their various "loyalty" or "frequent buyer" cards. It is perfectly legal (and perhaps advisable) for an unmarried teacher to go to a store in a nearby town to buy birth control (with cash), for example, or for the local pastor to do the same to buy a book extolling the virtues of another religion. Similarly, we can look at a newspaper without anyone else knowing which of the many articles we are reading in it. Yet many in government and law enforcement worldwide have embarked on a holy war to convince us that these privacy rights we have enjoyed throughout our lives must end the moment we involve our personal computers in the process. Why? The simple answer is that Internet-based purchases and browsing can be (and are) tracked, whereas cash purchases and selective reading of the daily newspaper cannot (at least not without physical surveillance or a vast network of informants).

Individuals' computer hard disks and the records of their Internet-based activities are being subpoenaed as "evidence" with a frequency that is accelerating to epidemic proportions—not only in criminal investigations but even in plain old civil cases. In so-called cyber-SLAPP civil suits, for example, litigants (usually large corporations seeking to intimidate anonymous critics) can file cases to subpoena individuals' computers on the basis that they "might" contain relevant evidence. A judge does not review such civil subpoenas unless the defendants challenge them in court, which rarely happens given the short timeframe for compliance. Moreover, defendants often do not even know that their Internet records have been subpoenaed.[1] (See www.cyberslapp.org for more.) An entire cottage industry in computer forensics has emerged to service the insatiable appetite of law enforcers and civilian litigants to find others' thoughts that were mistakenly entrusted to personal computers.

Practically all nations are now monitoring their respective citizens' individual Internet usage, including

- what they write in email and to whom (the equivalent of opening the envelopes of conventional private mail),
- what sites they browse on the Web (the equivalent of looking over our shoulders at the bookstore), and often
- what they type on their "personal" computers—even if it is never sent over the Internet (the equivalent of standing behind us all the time, taking notes on our every act).

Unlike law enforcement investigations (as opposed to secret police monitoring), which are launched only after crimes have been committed, wholesale monitoring of Internet usage is done before any illegal act occurs.

Rational options

In 1791, British social reformer Jeremy Bentham published a design for the Panopticon—a jail built in a semicircular pattern with an "inspection lodge" at the center and cells around the perimeter. Guards could always see the prisoners, but the inmates could not tell when they were being watched. "There was nowhere to hide, nowhere to be private. Not knowing whether or not they were watched, but obliged to assume that they were, obedience was the prisoner's only rational option."[2]

It seems we now we have a global Panopticon that intimidates people into behavior approved by the state. Creativity, which by definition challenges the status quo, therefore becomes impossible if we use the Internet—unless we are willing and able to deploy techniques (such as those described later) that negate interception. We cannot have free speech without freedom to speak anonymously because locally unpopular opinions can expose the speaker to physical harm, or even death, as when Galileo told the Pope the earth is not the center of the universe. Likewise, we cannot have freedom of information without anonymous access to information.

What justifies the massive electronic intrusiveness we now see? Governments justify it in the name of protecting us from terrorism and crime—as if these did not exist before computers and the Internet came about. In truth, however, they do it simply because technology makes it so easy to maintain control today. And it will be even easier tomorrow.

Is there a way to maintain the privacy of cash and casual browsing from yesteryear even when using computers today? Indeed there is, but it takes some extra effort.

Computer forensics cannot find what does not exist in the first place. Instead of using a computer's hard disk, we can use only floppy disks: we can boot from a floppy with DOS, write whatever we want using a DOS text editor, encrypt it, and save the encrypted file on a pristine new floppy disk. The moment the computer is turned off, all remnants of what we did with it will disappear into thin air. Of course, this works only with files that are smaller than the capacity of the media in use.

To be truly safe, we must also check the keyboard cable for any keystroke recorder masquerading as an adapter. Opting for a laptop adds a level of certainty because it makes it harder for someone to hide a keystroke recorder in it. Furthermore, the laptop's lower power consumption suggests that it should generate much fewer unintended, interceptible emanations than a desktop computer.

To browse the Web anonymously, we must begin with the question, "Anonymity from whom?" From our ISP? From the remote Web site we're visiting? From overzealous local security services? Each of these privacy threats requires a different solution, and I will explore these subjects in my next few columns.

Computer forensics cannot find what does not exist in the first place.

Lest someone parrot the law enforcement propaganda that a desire for private Web browsing implies wrongdoing, consider the following situations where it is, in fact, essential:

- An individual accessing medical information about a dreaded disease, but fearing to go on record in so doing and risking future insurance coverage.
- A desperate teenager accessing an

online suicide-prevention support group looking for help.
- An educator in a setting with a small-town mentality accessing information about religions, concepts, or social trends that the local community does not like.

In short, there are numerous everyday situations in which anonymous browsing serves essential societal functions.

Propaganda and power

When Guttenberg invented the movable-type press, royalty and people of influence felt threatened that, horror of horrors, common mortals could document and easily share their ideas. The effect was an involuntary transfer of power from the state to the people.

The Internet phenomenon is of equal, if not greater, social significance: anyone can now proclaim anything they like and reach an instant worldwide audience without prior approval or peer review. This is pure anathema to most, if not all, regimes. The concurrent availability of unbreakable encryption is the final straw. Not only can common people now reach worldwide audiences, but they can communicate and store information in a manner that the state cannot read—or even detect, in some cases. It is no surprise that regimes have gone into high alert over cyber activities, but they risk vast economic loss by opting out of the Internet. Instead, governments are spending fortunes (of their citizens' tax money) to monitor Internet traffic.

Regimes and their security services have elevated to an art form the requisite propaganda to make this intrusiveness palatable—even desirable to some populations—by appealing to basic human fears:

- *Protection from crime.* Arguing that terrorists and criminals use the Internet (along with everybody else), governments attempt to monitor and even control Web usage by implying that this will enhance citizens' safety.
- *National defense.* Citing the threat posed by foreign terrorists and spies, regimes attempt to ban encryption and other Internet technologies that protect users' anonymity (proxies, remailers, and so on). Never mind the fact that spies and terrorists have been around since before the times of Moses.
- *Morality.* Claiming that the Internet is corrupting citizens' morals with propaganda or endangering children, some countries' officials and even some Internet service providers in otherwise enlightened nations seek to limit access by all to sites that provide information they want to block. I recall with weary amusement the ISP who had censored the word "breast," thereby preventing subscribers from accessing information about breast cancer or chicken recipes. As a parent of two infants, I can attest that protecting the children is certainly my highest priority. However, I would argue that it is a parental obligation, prerogative, and right, which should not be abdicated in favor of governmental censorship.

The creeping growth of privacy violations reminds me of the frog syndrome: if you put a frog in water and raise the temperature suddenly, the frog will jump out to save its life. If you raise the water temperature ever so slowly, the frog will stay there and die.

The main difference between totalitarian and representative regimes is the extent of the freedom their citizens enjoy, but freedom is not free, and democracy cannot be measured merely by whether we can vote for our leaders. Pre-World-War-II Germany had a democratically elected government, but we all know what ensued.

It is, unfortunately, quite easy to sell an oppressive platform of "law and order" to many people by conjuring up images of unshaved savages roaming free and looting our neighborhoods. Every reasonable person wants to feel secure, but it is far easier for law enforcement to treat us all as criminals and take everybody's privacy away than to actually identify the perpetrators of a given crime.

In response to my last column, one reader wrote to me saying he couldn't do anything about the issues I raised because he was "only an information technology engineer." But I say we are much more than that. We are the magicians that make this awesome new power—information technology—possible. We are like the scientists and engineers of years past who gave us electricity, airplanes, nuclear energy, and other technologies that governments have since put to use—often, but not always for good.

Information technology's power is perhaps more potent than nuclear bombs. We must stand and have our say in how it is used. It is all too easy to accept the demagoguery of those who thrive on controlling others under the banner of law and order, and to surrender all freedoms as the price of living in peace. It is also an inexcusable admission of the human spirit's defeat. □

References

1. B. Sullivan, "Advocacy Groups Claim Free Speech Imperiled," *Computerworld*, 12 July 2002; www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,72692,00.html.
2. J. Bentham, *Collected Works*, vol. 2, John Bowring, ed., Edinburgh, 1843.

Michael Caloyannides *is a senior fellow at Mitretek Systems. His research interests include information security, radio frequency telecommunications, and covert communications. Caloyannides is author of* Computer Forensics and Privacy *(Artech House, 2001) and* Desktop Witness *(Wiley & Sons, 2002). Contact him at micky@ieee.org.*