

Privacy, Security, and Anonymity: An Evolving Balance

A noteworthy tenth anniversary will be celebrated this summer. On July 5, 1993, the *New Yorker* published what is still the best-known Internet-related cartoon ever drawn. The artist Peter Steiner depicted two dogs—one seated in a chair, with paw on keyboard, and one on the floor below. The dog at the console summarizes the essence of this still-new technology for his companion: “On the Internet, nobody knows you’re a dog.”

Readers in that pre-Web world could nod and grin and appreciate the profound truth of the canine observation: the Internet was the great “anonymizer.” For the first time in history, humans (and perhaps other species) could casually communicate without the distractions of race, gender, age, size, or physical deformity or impairment. All such extraneous matters disappeared when interactions were reduced to anonymous keystrokes.

Anonymity is a powerful attribute. Fledgling social movements—think of the civil rights and anti-war struggles of the sixties—rely on it. (Imagine if all the people attending a protest rally or meeting were required to identify themselves at the door.) Anonymity also finds a natural and important home in higher education, where the right to read anonymously, though hardly ever explicitly articulated, is, on reflection, universally assumed and ab-

solutely required. As noted in the American Library Association’s “Principles for the Networked World”: “The rights of anonymity and privacy while people retrieve and communicate information must be protected as an essential element of intellectual freedom.”¹ In addition to teachers and researchers, college and university campuses are home to another group for whom anonymity is vital: students. Students spend a large part of their undergraduate years in a quest to discover who they are, to “find themselves.” Whether this is a search for sexual identity or social structure, for many adolescents, the search can take place comfortably only when it is free from prying eyes. Finding yourself is a lot easier when you don’t have an audience watching you look.

In 1986, Cornell University created the first online counseling service, “Dear Uncle Ezra” (<http://ezra.cornell.edu>), allowing anonymous questions to be sent to an equally anonymous trained counselor, who replied via public postings. “Ezra” is still going strong in its sixteenth year, and letter after letter affirm that the questions asked, the problems raised, and the fears exposed would not have been expressed if a signature had been required.

It is hard to overstate the importance of anonymity in our daily lives, but like the fish who don’t perceive the ocean they live in, we seldom take note of that part of our environment. The subliminal reality can be seen in the Hollywood cliché, “Your papers, please!” We instantly know that the society depicted is a totalitarian one, and our instinct is not

without justification. A defining element of the police state is its obsession with maintaining dossiers on all of its citizens. As eloquently summarized by Canada’s privacy commissioner, George Radwanski, “The right not to be known against our will—indeed, the right to be anonymous except when we choose to identify ourselves—is at the very core of human dignity, autonomy, and freedom.”²

Unfortunately, like nearly every other powerful force in our world, anonymity has its dark side. For the typical Internet user, the first negative inking probably arrived along with

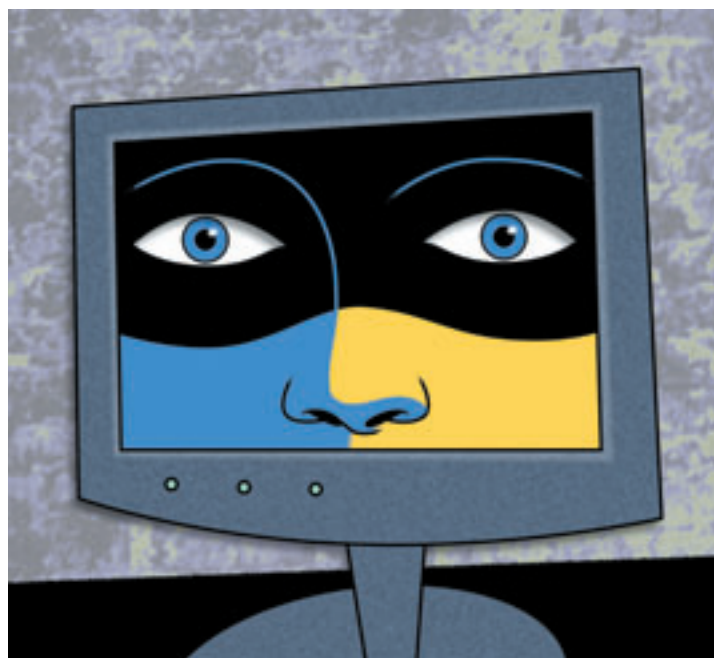


Illustration by Steve McCracken, © 2003

the first piece of spam. Who sent that bizarre message offering millions of dollars for help with a Nigerian bank account or spewing overblown hype about the wonders of this or that drug or treatment? Of course, if it's impossible to tell the dogs from the humans on the Internet, it's even harder to tell the honest correspondents from the scam artists and hucksters. News reports described children lured to tragic encounters by chat-room perverts masquerading as potential friends. Lonely adults also fell prey to those tricks, and everyone knew someone who knew someone with a personal story to tell. Next arrived the viruses and the denial-of-service attacks, launched by anonymous vandals against a confused Internet citizenry who were slowly learning that cyberspace has its own criminal element.

And then came 9/11 and the need to find ways to protect the public against further terrorist attacks. Inevitably, the balance between security and privacy shifted. We now live in a world where airline travel is far more difficult and metal detectors far more widespread. It is a world where the USA-PATRIOT Act makes it easy for law enforcement to find out what books people are reading and what towns they're traveling to, a world where the government plans to combat terrorism by "data-mining" vast stores of information on citizens' activities and looking for "suspicious" patterns. In this world, more and more cities are installing cameras to monitor the public streets, and face-recognition technology is scanning crowds at athletic events. In such a world, the idea of Internet anonymity can easily seem like a naive anachronism, misplaced nostalgia for a warm and cuddly Internet that may never have existed.

It is in this environment that many campuses are considering a requirement that all network access be authenticated—that whenever bits flow, they leave an audit trail that can be traced back to an individual whose identity was originally verified by password or cryptographic key. How else, proponents ask, can we determine who it was that sent the death threat to President George W. Bush from a library workstation? How else can we track down the hackers, the spammers,

the cybervandals who have been taking advantage of unaccountable access to higher education's high-speed digital infrastructure? In this view of the world, computer and network use is not a right but a privilege, one that can and should be duly monitored.

The arguments against universal authentication are equally vehement, starting with the recognized value of anonymity. Further, these arguments go, the Internet is rapidly becoming an indispensable tool for performing the common acts of citizenship: large amounts of government information and databases are available only via the Web. E-mail reaches elected representatives days or weeks faster than paper mail because it doesn't have to be irradiated to kill potential biohazards. Online filing of income tax is moving into preferred status by the IRS. The Internet is the new pathway for voice telephone calls and for an increasing number of newspapers and "broadcast" information sources that have no conventional instantiation. Internet-based political campaigning and fundraising are well established, and online elections are not far away.

The two sides in this debate seem to be irreconcilable. Is there a middle ground? The answer is yes, and here are two examples:

- At the University of Washington in Seattle, clever network designers have created a system whereby anonymous users can surf the entire Internet but can send e-mail only to on-campus addresses. For example, it is possible to send an anonymous message to the president of the university but not to the president of the United States.
- At Indiana University, each network access point may be configured for its own level of anonymous capabilities, chosen by the "owner" of that access point. For example, computers located on staff members' desks might require authentication for network connections, but kiosks in libraries might allow varying degrees of unauthenticated (i.e., anonymous) network activity. Indiana's system can even specify that a particular network port provide anonymous Web surfing but not anonymous e-mail.

The point isn't that either the University of Washington or Indiana University has found the perfect answer to the need for balance between Internet security and Internet privacy. The point is that both institutions are experimenting with the type of solution that society must develop over the next few years for maximizing the benefits of Internet technology while minimizing its more sinister side. Acceptable solutions must fall somewhere in the middle of the spectrum, rather than at its extremes, and will require creativity on the part of both technologists and policy experts.

Nearly 250 years ago, Benjamin Franklin summarized the tension between anonymity and security in less than twenty words: "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." But Ben lived in a world where armies marched in orderly columns and were dispatched and recalled by well-defined nation-states that followed rules and negotiated and signed peace treaties. He had never heard of Osama bin Laden, and he could not have imagined fuel-filled airplanes used as mass-murder weapons by stateless martyrs. Much more recently, in 1963, Supreme Court Justice Arthur Goldberg provided another apt summary that captures the need for the balance we see developing: "While the Constitution protects against invasions of individual rights, it is not a suicide pact."³

Ten years ago, Internet anonymity threatened nothing worse than dogs pretending to be humans. Today, newspaper headlines tell us that we must balance Franklin's idealism with Goldberg's realism. We continue to search for that appropriate balance point.

Notes

1. American Library Association, "Principles for the Networked World," February 2003, <<http://www.ala.org/oitp/principles.pdf>> (accessed March 13, 2003).
2. George Radwanski, "Privacy at a Crossroads" (speech delivered at "The Frontiers of Privacy and Security: New Challenges for a New Century" conference in Victoria, British Columbia, February 13, 2003), <http://www.privcom.gc.ca/speech/2003/02_05_a_030213_e.asp> (accessed March 13, 2003).
3. *Kennedy v. Mendoza-Martinez*, 372 U.S. 144 (1963).

Steve Worona is Director of Policy and Networking Programs at EDUCAUSE.