A noteworthy tenth anniversary will be celebrated this summer. On July 5, 1995, the New Yorker ran a cover showing all 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 summarized 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 portrayed truth of the cartoon’s 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 the fewest possible keystrokes.

Anonymity is a powerful attribute. Fleeting social encounters (such as those at the civil rights and anti-war struggles of the sixties—rely on it. Imagine if all the people attending a political meeting or gathering were required to identify themselves at the door! Anonymity also lends a natural and important home in higher education, where the right to be anonymous, though hardly ever explicitly articulated, is, on reflection, universally assumed and absolutely 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.” 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 sex, identity, or social identity or social structure, for many adolescents, the search can take place comfortably only when it is free from parental eyes. Finding yourself is a lot easier when you don’t have an audience watching you.

In 1998, Cornell University created the first online counseling service, “Dear Uncle Ezra” (http://ezra.cornell.edu), allowing anyone to seek counseling from 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 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.”

Unfortunately, like nearly every other powerful force in our world, anonymity is moving into the dark side. For the typical Internet user, the first negative inkling probably arrived along with the first piece of spam. Who sent that bizarre message offering millions of dollars for help with a Nigerian bank account or counting spelling Overhyped 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 correspondent from the scam artists and hucksters. News reports described children lured to tragic encounters by chat room perversions 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 air travel is far more difficult and metal detectors far more widespread. It is a world where the USA-PATRIOT Act makes it so easy to issue that warrant to search 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 naively archaic, misplaced nostalgia for a warm and cuddly Internet that may never have existed.

Is it in this environment that many campers are now demanding that 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 access. Indiana University’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 a problem with its high-speed access and balance between Internet security and Internet privacy. The point is that both institutions are experimenting with different types of solution that society must develop over the next few years for maximizing the benefits of new 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 technological language: “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. Franklin’s idealism and Goldberg’s realism. We continue to search for that appropriate balance point.

Notes

By Steve Worona
Policy, Security, and Anonymity: An Evolving Balance

Steve Worona is Director of Policy and Networking Programs of EDUCAUSE.
A noteworthy tenth anniversary will be celebrated this summer. On July 5, 1995, the New Yorker reported, “The Internet has captured the fabulously fast—and 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 proffered tidbit 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 low-level protocols.

Anonymity is a powerful attribute. Fledgling social networks sprouted from the civil rights and anti-war struggles of the sixties—relies on it. Imagine if all the people attending a panel discussion 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 absolutely required. As noted in the American Library Association’s Principles for the Networked World: “The right of anonymity and privacy while people retrieve and communicate information must be protected as an essential element of intellectual freedom.” 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 sex, identity, or social status, or need 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.

In 1989, Cornell University created the first online counseling service, “Dear Uncle Ezra” (http://ezra.cs.cornell.edu), allowing students to communicate with 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 was 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—and, indeed, the right to be anonymous except when we choose to identify ourselves—is at the very core of human dignity, autonomy, and freedom.”

Unfortunately, like nearly every other powerful force in our world, anonymity and privacy were visualized as threats; that is, as agents of evil that needed to be controlled. For the typical Internet user, the first negative inkling probably arrived along with the first piece of spam. Who sent that bizarre message offering millions of dollars for help with a Nigerian bank account or counting spewed 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 correspondent from the scam artists and hucksters. News reports described children lured to tragic encounters by chat room predators 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 easier for government 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 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 campers who provide the “owner” of the 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 access, allowing 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 done something wrong. The point is that both in their experiments with a particular type of solution that society must develop over the next few years for maximizing the benefits of information technology while minimizing its more sinister side. Acceptable solutions must fall somewhere in the middle of the spectrum.

Nearly 250 years ago, Benjamin Franklin summarized the tension between anonymity and security in less technological terms: “They that can give up...the balance we see developing: “While the Constitution protects against invasions of individual rights, it is not a suicide pact.”

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

Notes

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