

Opinion: What trumps privacy?

Jay Cline

October 30, 2008 ([Computerworld](#))

We all like to think our privacy is absolute. But if your job involves working across borders, you'll want to talk about privacy as a matter of degree rather than as an uncompromising right. Why? Not only do you want to be seen as someone who can get things done globally, but you also may personally want to be part of advancing social objectives that are arguably as important as privacy.

Have you ever had to re-architect your global rollout of [PeopleSoft](#) or Lawson because of [European Union](#) privacy concerns? Or adjust how your company offers technical support to medical products sold in Europe? Have you ever been part of acquiring a failing European company where the privacy of employee data was a final sticking point? If you've seen projects with obvious social benefit get held up by seemingly minor data-related questions, then you might have been running up against this notion of "nothing trumps privacy."

It's a popular idea. The half-billion people of Europe do view privacy as a human right. And they're not the only ones. As one of the first acts of the [UN](#), Eleanor Roosevelt and the U.S. delegation in 1948 lobbied for the global adoption of the [Universal Declaration of Human Rights](#)(UNDHR), whose Article 12 states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."

With Europe and the UN using absolute-sounding language to describe a right to privacy, it's no wonder we have all of these delayed and downsized corporate projects. People are legitimately concerned about our sometimes reckless march into the Information Age, and they want to put some brakes on it.

But does privacy trump all foes? I can think of at least six other equally important social objectives that regularly put limits on privacy:

1. **Personal health.** We all want to stay healthy — even when we lose the ability to communicate and give consent. Emergency-room personnel need access to all available information about unconscious patients — about their pacemakers, their medical histories and their bio readings — in order to give effective care. Caregivers for children and the elderly also need to disclose their medical information to coordinate care, without always first obtaining consent. These instances of information sharing compromise privacy, strictly speaking.
2. **Public health.** We also want to avoid catching infectious diseases, and we want drugs and medical devices to be safe. To achieve these objectives, however, information about people infected with fatal, contagious diseases must be shared with a central clearinghouse such as the [Centers for Disease Control](#). Actions may also need to be taken to notify others potentially at risk of infection. Similarly, when drugs and medical devices cause harm to someone, these "adverse events" get reported to the companies and to the [Food and Drug Administration](#) for the purpose of improving the products and alerting the public. Allowing for degrees of privacy protection within these processes may be a life-and-death matter for at-risk people.
3. **Parental rights.** The UNDHR, in the very statement proposing the right to privacy, extends that scope to include the family and the home. Article 16 further states, "The family is the natural and fundamental group unit of society and is entitled to protection by society and the State." To this end, parents arguably have a right to know about the medical treatment given children living under their roof, what their children have told doctors and school nurses, and to make decisions about their children's medical treatment. When children go missing, parents also regularly share their child's photo and description with authorities for the purpose of local and national broadcast. A strict understanding of the child's privacy, however, would curtail these rights of parents within their homes and families.
4. **Personal property.** Article 17 of the UNDHR states, "Everyone has the right to own property alone as well as in association with others." To that end, people have a right to buy land, buildings and computer equipment to run a business. Part of maintaining ownership of this property — especially data — is to monitor employee use of that property. Absolute privacy rights, however, would prevent employee monitoring and increase the opportunity for violations of property rights.

5. **Law enforcement.** Article 3 of the UNDHR states, "Everyone has the right to life, liberty and security of person." Ensuring these rights requires enforcement of laws. Tracking down suspects necessarily involves collecting data about people who don't end up being the criminal, in ways that are impossible to provide notice and consent. We tolerate these compromises of privacy because we don't want criminals to remain at large.
6. **National security.** The UN has from its beginning recognized that nations have the right to defend themselves against foreign aggression. When the aggressors come across your borders and interact with your citizens, tracking them necessarily involves capturing information about your citizens at the same time. As great a risk to liberty as it is to allow government surveillance of public spaces and private communications, an even greater risk to liberty could be having no effective defense in an age of terror.

These six spheres of exceptions to a so-called right to privacy are so large in total that I think we'll never, at least in America, rank privacy alongside the bedrock inalienable rights of free speech, freedom of the press and freedom of assembly. There are too many necessary compromises to call privacy a foundational or primary human right.

So don't believe all the press about privacy. Without question, it's one of the most important social objectives of the Information Age. But you can protect privacy in matters of degrees without harming people, their liberty or their dignity — and accomplish other vital humanitarian goals in the process.

Jay Cline is a former chief privacy officer at a Fortune 500 company and is now president of [Minnesota Privacy Consultants](#). You can reach him at cwprivacy@computerworld.com.