



NewsFactor Network
Technology's Home Page

@business is the game. Play to win.™

[CLICK TO GET YOUR INFRASTRUCTURE
SOFTWARE SUCCESS KIT NOW >>](#)

WebSphere. software IBM

Battling Terrorism: Trading Digital Privacy for Nothing?

By Robyn Weisman
NewsFactor Network
September 28, 2001

<http://www.newsfactor.com/perl/story/13779.html>



In the wake of the September 11th terrorist attacks on the Pentagon and the World Trade Center, many Americans have expressed support for more intrusive online security and surveillance activities, and a large number seem willing to sacrifice a measure of long-cherished civil liberties.

Comments on Internet message boards support formal surveys. A typical writer said: "I can't imagine anyone having anything to fear [from] having email scanned by a computer program unless they have something to hide."

In the battle against terrorism, many have expressed a readiness to give up some degree of online privacy. But is that really a good idea?

Another agreed, saying: "By all means, read my e-mail and follow my every move on the Net if it means avoiding another catastrophe like the one we're reeling from."

But can laws based on such sentiments, however patriotic and well-intentioned, be effective in identifying and apprehending terrorists? And would such laws erode the basic civil freedoms upon which American society is based?

Please note that this material is copyright protected. It is illegal to display or reproduce this article without permission for any commercial purpose, including use as marketing or public relations literature. To obtain reprints of this article for authorized use, please call a sales representative at +1 (818) 528-1100 or visit <http://www.newsfactor.com/about/reprints.shtml>.

Trading Privacy For Nothing?

On September 13th, the U.S. Senate passed the [Combating Terrorism Act of 2001](#), which includes an amendment allowing for increased monitoring of people's activities in cyberspace, including viewing of citizens' to-from e-mail header data and tracking of visited Web sites.

The government likens the principle involved in gathering this information to federal law enforcement agencies' gathering of phone numbers -- a simple process -- as opposed to the labyrinth of rules and regulations that must be followed when tapping phone conversations.

But Richard Hunter, managing vice president of research firm [Gartner Inc.](#), told NewsFactor Network that citizens agreeing to such measures are "trading their privacy for nothing."

The sort of thinking expressed by both the writers quoted above and by lawmakers is "based on the assumption that increased monitoring and increased technology will do the job," Hunter told NewsFactor. "They're assuming that these sorts

of technology function the way a metal detector on a beach does -- that we'll sweep [the entire telecommunications and Internet systems] and manage to find all the terrorists."

But it's easy for terrorists to evade such measures, now and for the foreseeable future, said Hunter. Only careless terrorists will be caught using such monitoring technologies, and terrorists are rarely careless.

Backwards Evidence Gathering

Hunter expressed skepticism that this sort of evidence-gathering would be an effective way to apprehend terrorists.

"When police investigate a murder, they direct their investigation outward from a small group of potential culprits, versus winnowing [potential suspects] from the entire population," Hunter said.

The methods championed by Attorney General John Ashcroft and Senator Orrin Hatch (R-Utah), in which investigators comb through terabytes of cyber-data in the hopes of finding the terrorist in the haystack, won't produce the desired effects, Hunter said. Moreover, he added, they may well divert attention and resources from approaches that could get better results faster.

"As Americans, we tend to believe that machines and technology do a lot," said Hunter. "But they don't do everything and may be particularly ineffective against certain enemies" like the ones presently threatening the nation's safety.

Private Lives, Public Information

Hunter added that the new powers being authorized by Congress may do little else than turn private lives into public information. And if these powers are being invoked because the country is in a state of emergency, then people need to ask when, exactly, they will be repealed.

"We could be in this state of war for generations," said Hunter, noting that after over 80 years of battling the Irish Republican Army, the British still contend with terrorist bombings.

Said Hunter: "It's disturbing to see such enormous monitoring powers being given to the government, essentially without any limit on when these powers will be revoked. [Such laws] have the potential to put a lot of power into corrupt hands." [END](#)

© Copyright 1998-2002 NewsFactor Network. All rights reserved. This material may not be published, broadcast, rewritten or redistributed in any form without written permission. Please [click here for legal restrictions and terms of use](#) applicable to this site. Use of this site signifies your agreement to the terms of use. If you would like to reprint content from the NewsFactor Network, [click here](#) for pricing information. [Privacy Policy](#).

[NewsFactor Front Page](#) | [E-Commerce Times](#) | [TechNewsWorld](#) | [Linux Insider](#)
[Wireless NewsFactor](#) | [osOpinion](#) | [TechExtreme](#) | [CRM Daily](#) | [FreeNewsFeed](#)