

What September 11th May Mean to Netizens (3 pages)

The tragic events of September 11 should not serve as a catalyst for the infringement of fundamental freedoms on the Net.

By Richard Forno

Column appearing in Securityfocus on Sep 18 2001.

Article Copyright © 2001 by Securityfocus. All Rights Reserved.

[NOTE: In accordance with 17 USC 107, this material is distributed without profit or payment to those who have expressed a prior interest in receiving this information for non-profit research and educational purposes only.](#)

Last week's tragic events in New York and Washington captured the world's attention. The visions of destruction in Manhattan and at the Pentagon will likely never be erased from the American psyche. Yet we are all too aware that this was not some surreal dream, but a sad reality that must be addressed quickly and effectively.

Even prior to these events, I've said time and again that the United States must not respond to any emergency or issue without knowing all the facts. We must not be unduly swayed by emotion, sensationalism or fear mongering. Any response must be made in a way that does not diminish the freedoms enjoyed by Americans or dramatically change the way in which Americans live their daily lives. To do so would mean that the sponsors of last week's attacks have won.

Almost immediately following the two incidents in New York and Washington, lawmakers and law enforcement were scrambling to respond to these attacks and to prevent future ones. Unfortunately, many of the measures put forth run contrary to the American ideals of privacy and personal freedom – particularly those that involve technology and communications. Unfortunately, being presented in the aftermath of national tragedy, many of these proposals stand a good chance of being approved. Lawmakers understandably want to appear responsive to the safety and security of the American people. But while this motivation is noble and laudable, it is crucial that the long-term freedom of Americans not be jeopardized in the name of short-term uncertainty and emotional closure.

Already we are seeing the intrusion of security on liberty. A recent Wired article reports that federal law enforcement agencies are already looking to increase Internet surveillance activities after last week's deadly attacks. The FBI is approaching ISPs and web providers looking to deploy its controversial DCS1000 software, formerly known as Carnivore, to monitor communications that may be linked to the attacks. Reportedly, most companies that have been approached are supportive of the FBI's request.

If these events had not occurred, it's doubtful that Carnivore's use would be so warmly welcomed. Over the past year, DCS1000 has been the center of heated controversy due to concerns about the ability of a single law enforcement tool to blur the legally-defined lines that separate law enforcement's abilities to monitor and intercept ostensibly private communications. (Mark Rasche's recent SecurityFocus column, my white paper entitled Who's Afraid of Carnivore? Not Me!" are excellent references to learn more about Carnivore's controversial functionality and effectiveness.) Congressional action – led by Rep. Dick Armey – in investigating Carnivore's potential for privacy invasions was welcome by the Internet community last year; however, in light of the recent attacks, it stands to reason that on-line privacy may be sacrificed in the name of counter-terrorism preparedness.

Those responsible for the attacks might well have used strong encryption and data-hiding (e.g. steganography) techniques to protect their communications. In recent years, the Congressional testimonies of federal law enforcement officials have made it clear that such technologies should be viewed as a national security threat. We have been down this road before. In the mid-1990s, the creator of Pretty Good Privacy (PGP) – now the defacto standard for e-mail encryption - was arrested in the United States for allowing strong encryption software to be distributed around the world. The Department of Justice sought to classify strong privacy-enhancing cryptography like PGP as a military-grade munitions akin to stealth technology and biological agents.

Ultimately, the government realized that technology and the networked nature of the world, coupled with the human capacity to communicate and express ideas and information, made it impossible to restrict the further public distribution and understanding of strong encryption for the masses. As a result, the Justice Department realized that, given the speed and dynamic nature of the Internet, continuing to prosecute the PGP matter would be an exercise in futility. Unfortunately, in light of recent terrorist events, this futile endeavor will most likely be undertaken again. Sadly, it will achieve the same outcome as the PGP case.

It's a good bet that we will soon see law enforcement around the world lobbying for more widespread use of keystroke monitoring, stronger anti-encryption laws, key escrow, and other pie-in-the-sky attempts to control the spread of data protection methods on the Internet, all in the name of investigating and preventing on-line terrorist communications.

Already we see the results of public surveys containing questions designed to "lead" the respondent to answer a certain way. These surveys are put forth as evidence of public support for a given government course of action. For example, one of the questions on the the September 13 Princeton Survey Research Associates public poll reads: "Should encryption laws be reduced to aid CIA/FBI surveillance?" This assumes that the intelligence community did not know about

the events beforehand because strong encryption played a part in maintaining the terrorist's secrecy. This implies to the respondent that such technologies are a bad thing. However, it's a good bet that survey respondents have little if any understanding that stronger anti-cryptography laws will not matter to people who intend to break much more important laws like, say, murder. Such leading questions are intentionally designed to generate artificial public support for a given issue, such as increased surveillance powers.

Regardless of whether or not attempts to suppress these technologies are unconstitutional or anti-democratic, there is no reason to believe that they will help prevent future terrorist activities. Those with even a moderate level of expertise can bypass Carnivore and other data-sniffing technologies easily without using any form of encryption. As we saw during the PGP fiasco, and in the ongoing loony-land debates over the full-disclosure of security vulnerabilities, ideas and analysis are difficult to censor in an ever-shrinking world.

Deploying Carnivore, restricting strong data protection mechanisms and privacy-enhancing technologies will not discourage criminals in the cyber world any more than gun control laws do in the real world. In both cases, if criminals want to use prohibited technologies, they will, regardless of the law. Implementing such privacy-invading restrictions are simply feel-good, short-term public demonstrations of the government taking action against terrorism. In reality, such actions serve only to limit the fundamental rights of law-abiding citizens - placing their actions under the arbitrary microscope of law enforcement while criminals continue to ignore operate outside the law.

When developing our response to these tragic events, we must make decisions based on fact and truth, not fear-mongering or psychological blackmail. After all, as American founding father Ben Franklin once noted, if we surrender our liberty in the name of security, we shall have neither. I implore national policymakers to refrain from making knee-jerk reactions that will muddy the waters of civil liberty and hinder the development of effective, rational technology and law enforcement policies.

Out of every tragedy is born the seeds of change, may it be a change for the better.

###

Richard Forno is Chief Technology Officer of Shadowlogic, LLC in Dulles, VA. He is the coauthor of Incident Response (O'Reilly) and The Art of Information Warfare (Universal). He helped establish the first incident response team for the U.S. House of Representatives, and is the former Chief Security Officer at Network Solutions. He holds degrees from Valley Forge Military College, The American University, and is the youngest graduate on record from the United States Naval War College.