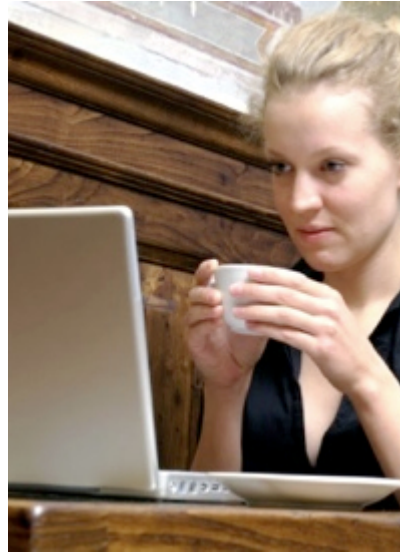




Wiretapping Your Emails

As communications technology has raced ahead of government attempts to tame it, in the name of law enforcement, the Obama administration, the FBI, the Department of Justice, the National Security Agency and other government agencies have been meeting for months to come up with regulations that would allow broadening government powers to intercept, read, and analyze Internet messages, and then prosecute perceived violations of law.

Arguments by proponents of further incursions into citizens privacy initially sound reasonable: new technology, and private citizens use of the Internet for private communications, have exceeded governments ability to keep up, and consequently its ability to monitor, track and follow people is going dark, unless something is done. Specifically, government officials want Congress to require all services that enable communications including encrypted email transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct 'peer to peer' messaging like Skype to be technically capable of complying if served with a wiretap order. That would include allowing the government to intercept and unscramble encrypted messages.



Valerie Caproni, General Counsel for the FBI, says not to worry: Were talking about lawfully authorized intercepts. Were not talking expanding authority. Were talking about our ability to execute our existing authority in order to protect the public safety and national security. She is referring to the 1994 law called the Communications Assistance to Law Enforcement Act (ECPA) which requires communication service providers like the phone companies to be subject to wiretap orders. But services like BlackBerry, offered by Research in Motion (RIM), aren't covered.

The government wants Congress to force those services that encrypt messages to unscramble them if asked to do so. This would include foreign-based providers (like RIM which is based in Canada), and would force peer to peer software providers to build in a back door to allow government to read those communications.

Caproni says that their request is quite modest because the service providers and not the government



Written by [Bob Adelman](#) on September 27, 2010

would hold the key to the back door. But to clarify the governments intent, she added, No one should be promising their customers that they will thumb their nose at a U.S. court order. They can promise strong encryption [but] they just need to figure out how they can provide us [with] plain text.

A coalition of resistance to this government push against privacy has been formed from a disparate group of interest organizations, such as the liberal ACLU and the free market group, the Center for Democracy and Technology (CDT). Called [Digital Due Process](#), they remind supporters on their website that Supreme Court Justice Louis Brandeis referred to privacy as the most comprehensive of rights, and the right most valued by a free people. The coalition's efforts to force Congress to limit the current rules under ECPA are motivated by its concern that the vast amount of personal information generated by today's digital communication services may no longer be adequately protected.

Jack Dempsey, Vice President of CDT, answered a subscribers questions about just how much privacy citizens have under current law:

Q: Under the current ECPA, is there any action one can take to keep Google from handing over the contents of [my] entire Google account (gmail, messaging, calendar, android phone use, etc.) upon request? [In other words] are there steps Google users can take to ensure their privacy?

Dempsey: Under the current ECPA, Google is already prohibited from handing over your data upon request. In the case of disclosure to the government [however], there has to be some process compelling disclosure. Our concern is that the current ECPA allows the government to demand disclosure with a mere subpoena, issued by a prosecutor without a judges approval and without any suspicion that you are engaged in criminal conduct.

Q: If the email on my laptop is protected from government search without a warrant, isn't that same piece of email also protected if it lives in the cloud?

Dempsey: It should be, but unfortunately the law isnt clear, which is why CDT is arguing that Congress needs to act. The Constitution provides the baseline of privacy protection against the government. We believe that, under the Constitution, email stored in the cloud should be protected, just as the things you put into a storage locker are protected In the absence [of a Supreme Court ruling, current] statutes define our privacy rights and, under ECPA, data stored in the cloud is available to the government with [just a] prosecutors subpoena, without court approval. Congress should amend the law to require a warrant issued by a judge and that is what we are advocating.

Q: Wouldnt beefing up the protections in ECPA hurt law enforcements efforts to keep crime under control? Isn't this reform [that your coalition is advocating] really painting law enforcement into a tighter corner?

Dempsey: We are seeking to establish traditional limits, not new limits. True, the traditional rules do *constrain* [emphasis added] the government, but that is the American Way. Back in 1967, when the Supreme Court said for the first time that a warrant was required for wiretapping, it noted: This is no [simple] formality we require today, but a fundamental rule that has long been recognized as basic to the privacy of every home in America.

Joseph Fulda, writing for [The Freeman](#) in 1996, made the point about privacy exquisitely:

If property is libertys other half, privacy is its guardian. The right to privacy is essential to the preservation of freedom for the simplest of reasons. If no one knows what I do, when I do it, and with whom I do it, no one can possibly interfere with it



Written by [Bob Adelman](#) on September 27, 2010

Privacy is the great shield of freedom from interference. Everyone who savors freedom will champion the right to privacy.



Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.

Subscribe