Politics : Law

Congress Mulls Stiff Crypto Laws

Declan McCullagh 09.13.01

WASHINGTON -- The encryption wars have begun.

For nearly a decade, privacy mavens have been worrying that a terrorist attack could prompt Congress to ban communications-scrambling products that frustrate both police wiretaps and U.S. intelligence agencies.

Tuesday's catastrophe, which shed more blood on American soil than any event since the Civil War, appears to have started that process.

Some politicians and defense hawks are warning that extremists such as Osama bin Laden, who U.S. officials say is a crypto-aficionado and the top suspect in Tuesday's attacks, enjoy unfettered access to privacy-protecting software and hardware that render their communications unintelligible to eavesdroppers.

In a floor speech on Thursday, Sen. Judd Gregg (R-New Hampshire) called for a global prohibition on encryption products without backdoors for government surveillance.

"This is something that we need international cooperation on and we need to have movement on in order to get the information that allows us to anticipate and prevent what occurred in New York and in Washington," Gregg said, according to a copy of his remarks that an aide provided.

President Clinton appointed an ambassador-rank official, David Aaron, to try this approach, but eventually the administration abandoned the project.

Gregg said encryption makers "have as much at risk as we have at risk as a nation, and they should understand that as a matter of citizenship, they have an obligation" to include decryption methods for government agents. Gregg, who previously headed the appropriations subcommittee overseeing the Justice Department, said that such access would only take place with "court oversight."

Gregg, the GOP's chief deputy whip, predicted that without such a requirement, "the quantum leap that has occurred in the capacity to encrypt information" will frustrate the U.S. government's efforts to preserve the safety of Americans.

Gregg's speech comes at a time when privacy and national security, long at odds, had reached an uneasy detente. In response to business pressure and the reality of encryption embedded into everything from Linux to new Internet protocols, the Clinton administration dramatically relaxed -- but did not remove -- regulations intended to limit its use and dissemination.

Janet Reno, Clinton's attorney general, said in September 1999 that the new regulations struck a reasonable balance between privacy and security. "When stopping a terrorist attack or seeking to recover a kidnapped child, encountering encryption may mean the difference between success and catastrophic failures," Reno said at a White House briefing. "At the same time, encryption is critically important for protecting our privacy and our security."

Now the balance has abruptly shifted -- and new laws that were unthinkable just three days ago are, suddenly, entirely plausible. As a measure of how suddenly the political winds have shifted from business to national security, consider this: Gregg recently has won 100 percent ratings from the National Federation of Independent Business and the U.S. Chamber of Commerce.

An Associated Press dispatch on Thursday, written by Dafna Linzer, reports: "These days, terrorists can download sophisticated encryption software on the Internet for free, making it increasingly difficult to tap into their communications."

The *Los Angeles Times*, in an article by Charles Piller and Karen Kaplan, predicted "calls for new restrictions on software encryption."

Frank Gaffney, head of the Center for Security Policy, a hawkish think tank that has won accolades from all recent Republican presidents, says that this week's terrorist attacks demonstrate the government must be able to penetrate communications it intercepts.

"I'm certainly of the view that we need to let the U.S. government have access to encrypted material under appropriate circumstances and regulations," says Gaffney, an assistant secretary of defense under President Reagan.

Gaffney said that he's unsure, however, if a global encryption-restriction regime is wise: "I'm not sure if I'm in favor of trying to foster an international regime whereby hostile goverments, or for that matter governments that may not be hostile at the moment but may be hostile in the future, can take advantage of backdoors."

Instead of privacy being in the minds of legislators, as it was until Tuesday, domestic security concerns have become paramount.

The four hijacked airplanes and the disasters they created have abruptly returned the debate on Capitol Hill to where it was years ago, when FBI Director Louis Freeh spent much of his time telling anyone who would listen that terrorists were using encryption -- and Congress should approve

restrictions on domestic use.
"We are very concerned, as this committee is, about the encryption situation, particularly as it relates to fighting crime and fighting terrorism," Freeh told the Senate Judiciary committee in September 1998. "Not just bin Laden, but many other people who work against us in the area of terrorism, are becoming sophisticated enough to equip themselves with encryption devices."
He added: "We believe that an unrestricted proliferation of products without any kind of court access and law enforcement access, will harm us, and make the fight against terrorism much more difficult."
In response to the FBI director's entreaties, a House committee in 1997 approved a bill that would have banned the manufacture, distribution, or import of any encryption product that did not include a backdoor for the federal government. The full House never voted on that measure.
Another Clinton administration initiative was the Clipper Chip, a cryptographic device that included both a data-scrambling algorithm and a method for certain goverment officials to decode intercepted, Clipper-encoded communications. After a public outcry, the federal government eventually abandoned its plans to try to convince American businesses to build Clipper-enabled products.
Gregg, in his speech Thursday, said that the kind of court oversight Clipper was intended to have would let "our people have the technical capability to get the keys to the basic encryption activity."
It's far too early to know how serious foes of encryption are, what kind of a hearing business and privacy lobbyists will receive on Capitol Hill, and whether Democratic and Republican leaders will encourage or discourage Gregg's approach. But some of encryption's brightest lights are already worrying about the effect of Draconian new laws and regulations.
In a post to a cryptography mailing list that he moderates, Perry Metzger wrote: "Cryptography must remain freely available to all."
"In coming months, politicians will flail about looking for freedoms to eliminate to 'curb the terrorist threat.' They will see an opportunity to grandstand and enhance their careers, an opportunity to show they are 'tough on terrorists,'" wrote Metzger, president of Wasabi Systems of New York City. "We must remember throughout that you cannot preserve freedom by eliminating it."
During the early and mid 1990s, when e-mail was a rarity and good encryption programs even more scarce, it was easy for encryption's proponents to argue that terrorists and other malcontents were not cloaking their communications. Now, with readily available applications like hushmail.com and PGP, crypto buffs are left with one less argument than before.
Matt Blaze, the AT&T Research scientist who was a chief critic of Clipper, said in an essay this week that: "I believed then, and continue to believe now, that the benefits to our security and freedom of widely available cryptography far, far outweigh the inevitable damage that comes from its use by criminals and terrorists."
Wrote Blaze: "I believed, and continue to believe, that the arguments against widely available cryptography, while certainly advanced by people of good will, did not hold up against the cold light of reason and were inconsistent with the most basic American values."
In an open letter this week, cypherpunk co-founder Eric Hughes offered a public plea not to restrict privacy or anonymity -- such as that offered by anonymous remailers -- in an attempt to preserve national security.
"We will find that there are internal champions of liberty that have without conspiracy or knowledge furthered the plans of our opponents, who have taken advantage of the liberties that America offers all who enter her shores," Hughes predicted.

See Also:
Pentagon Hides Behind Onion Wraps
Searching for Life Amid Rubble
Web Vents Open on U.S. Muslims
Hide Out Under a Security Blanket

Related Topics:
Politics , Security