

Archive: [FEATURE]

Mobile Surveillance

By Michael Grebb, Thu Dec 20 00:00:00 GMT 2001

0 comments above threshold (0 hidden)

PRINT

SEND

Newly passed legislation grants the US Government some hefty powers, with broad implications for the mobile industry.

In the wake of the Sept. 11 terrorist attacks, it didn't take much arm twisting for the U.S. Justice Department to receive scores of new powers that presumably would help deter attacks in the future and, in a sadly necessary way, allow authorities to play a little dirtier than they have before.

After a six-week debate on Capitol Hill, U.S. President George W. Bush signed the USA Patriot Act into law on Oct. 26, changing the entire matrix of fighting crime in America, at least temporarily (The new powers will expire in 2005 unless Congress renews them. The Bush Administration had originally requested permanent authority).

The new law grants many new powers, including controversial ones allowing authorities to hold suspected terrorists up to seven days without charging them with a crime and to continue using its "Carnivore" software to intercept email transmissions (although the FBI still must obtain a court order to read actual email content).

For a wireless industry rapidly growing and adding new wireless Web features every day, this new law will forever change the degree to which wireless service providers will have to cooperate with law enforcement authorities. In some ways, they will be forced to balance their need to help authorities with reassuring customers that their privacy remains important and protected. It won't be easy.

Walking a thin line

"We've always swung back and forth on these things," says Bob Rosenberg, a wireless analyst at Insight Research. "Right now, the pendulum is swinging on the side of security. It will swing back when the threat goes away."

Of course, it's impossible to know when that will occur. In the mean time, the wireless industry may in fact be facing increased costs and time-consuming new duties to help authorities track wireless messaging and maintain "roving wiretaps," which under the new law allows authorities to tap an individual rather than just a phone line and to do so with a single court order.

"There will be added costs," Rosenberg says. For example, an ISP with wireless email features would still need to open up a port on their router to track email transmissions from their main hub, adding such functionality to both the wireless and wireline operations.



Score: 0

SITE MAP SEARCH THEFEATURE
MEMBER LOGIN

Username Password

LOGIN Rememb
SIGN UP Member ber

SEARCH THEFEATURE

S

EDITOR 'S CHOICE

Political Texting: SMS an
By Howard Rheingold , Mon A
GMT 2004

MOBLOGGING ON THEFEAT

While software could do much of this automatically, large volumes of requests from the government could require some ISPs to hire new staffers to process the requests and, of course, stop tracking emails when the government is through with a particular investigation. Rosenberg predicts that consumers might have to absorb such costs, at least temporarily, in the form of surcharges on their bills. "But for now, everyone will be happy to pay the 50 cents per month," he says.

The question, of course, is for how long? And furthermore, it's unclear whether the new law will overburden the wireless industry (as well as ISPs and other software vendors whose Web apps run on wireless devices) at a time when the economy is creating vast challenges for the industry at large. All of this exists before a backdrop of potential exhaustion on the part of customers, who may at some point resent the idea that their transmissions could seemingly be intercepted at any moment - with the willing help of their wireless carrier or wireless ISP.

The authorities, however, deny that they will abuse their new powers. In extraordinary times, they argue, authorities must be given unprecedented powers to protect public safety.

Many experts also note that in addition to the new law's built-in 2005 expiration, Congress rarely allows intelligence agencies to operate unimpeded for long-especially after a specific threat has dissipated. But the remnants of powers granted during times like these don't disappear overnight either.

"The FBI keeps getting these privileges taken away because of abuse and then, in a time of crisis, gets them back again," says Richard Isaacs, a security expert with The Lubrinco Group. "Between Carnivore, Echelon [used by the National Security Agency to intercept international wireless transmissions], and assaults on encryption, privacy will take another nosedive. We never fully recover from these incursions, even when the pendulum swings the other way."

Freedom vs. security

Of course, Americans-rattled by constant Anthrax scares and the haunting memories of the twin towers collapsing live on television-seem more willing today to give up some civil liberties in pursuit of greater public safety. In fact, the speed with which the USA Patriot Act moved through Congress after Sept. 11 may be testament to the changing whims of a public desperate for the government to stop future terrorism on U.S. soil.

"People will tolerate a lot of intrusions into their privacy," says Mark Rasch, vice president of cyberlaw at Predictive Systems. "We have created an expectation of what we're expected to tolerate."

Others wonder whether most citizens really have much to worry about anyway, considering that the mere volume of wireless traffic makes the chances of being targeted miniscule-especially when dealing with Internet-based transmissions.

"With the incalculable amount of information that is transmitted over the Internet daily, the odds of wireless tapping are no greater than working from your hard-wired home PC or laptop," says Andy Fox, chairman and co-founder of iConverse, a mobile application technology provider. "Internet users have always been aware of the threat that someone is looking over their digital shoulders so-to-speak. But the odds definitely fall in the user's favor."

Rosenberg agrees that authorities face far greater challenges in tracking wireless data packets that travel over the Internet than in tapping traditional wireless phone calls. "It's considerably more difficult to be able to deal in the Internet space than in the wireless carrier space," he says.

"These transmissions are going to be routed all over the world to cover their tracks. And the kind of computer power required to sift through that would have to be a lot. Carnivore is essentially a vacuum cleaner. The traffic is doubling every year. By the time you have something built, it's obsolete."

Wired vs. wireless

Indeed, the FBI's current Carnivore email tracking system - which can be used for wireless data transmissions as well - can't begin to gather intelligence on any piece of email bouncing around the Internet.

In the future, the FBI is expected to take a more localized approach in which suspect individuals are targeted and their emails monitored closely. The trade-off may be that other suspect transmissions fall through the cracks, but it may be the best the authorities can do until they have more powerful computers capable of processing and analyzing more traffic.

The government will likely have a far easier time tapping traditional wireless phone conversations, especially with its newly expanded "roving wiretap" authority. In addition, the wireless industry already has an apparatus in place to help authorities: Under the existing Communications Assistance for Law Enforcement Act (CALEA), wireless carriers already tap phones for authorities when a court order is issued.

According to the 2000 Wiretap Report, wireless carriers tapped 691 lines compared to only 236 wiretaps for landline carriers, numbers that will presumably multiply in the wake of the new law.

But Tom Wheeler, president of the Cellular Telecommunications and Internet Association (CTIA), says the USA Patriot Act shouldn't overburden wireless carriers even though they perform more court-ordered wiretaps per subscriber line than any other telecom industry segment. "Whatever the Congress has authorized, we will do it," he said at a recent press briefing.

Wheeler noted that the government actually compensates carriers for costs associated with wiretaps, meaning that the new law shouldn't negatively impact the industry. In fact, some feel the wireless industry may even get a boost from consumers' desire to stay connected.

"With recent current events, Americans are finding it necessary to outfit themselves with mobile phones, PDAs, and pagers to keep themselves informed and in-touch," says iConverse's Fox. In this post-Sept. 11 world, keeping in touch with family and friends may indeed have taken on new urgency and meaning-whether or not the government is listening in.

Michael Grebb has previously written for The Industry Standard, Business 2.0, and eCompany. From Washington DC, he covers the impact of mobile technology on modern society.

0 comments above threshold  (0 hidden)