NY case underscores Wi-Fi privacy dangers

April 24 2011, By CAROLYN THOMPSON , Associated Press

In this April 21, 2011 photo, Wi-Fi logos are shown on a computer screen search engine in Buffalo, N.Y. The poll conducted for the Wi-Fi Alliance, the industry group that promotes wireless technology standards, found that 32 percent of respondents acknowledged trying to access a Wi-Fi network that wasn't theirs. An estimated 201 million households worldwide use Wi-Fi networks, according to the alliance. The same study, conducted by Wakefield Research, found that 40 percent said they would be more likely to trust someone with their house key than with their Wi-Fi network password. (AP Photo/David Duprey)

Lying on his family room floor with assault weapons trained on him, shouts of "pedophile!" and "pornographer!" stinging like his fresh cuts and bruises, the Buffalo homeowner didn't need long to figure out the reason for the early morning wake-up call from a swarm of federal agents.

That new wireless router. He'd gotten fed up trying to set a password. Someone must have used his Internet connection, he thought.

"We know who you are! You downloaded thousands of images at 11:30 last night," the man's lawyer, Barry Covert, recounted the agents saying.

They referred to a screen name, "Doldrum."

"No, I didn't," he insisted. "Somebody else could have but I didn't do anything like that."

"You're a creep ... just admit it," they said.

Law enforcement officials say the case is a cautionary tale. Their advice: Password-protect your wireless router.

Plenty of others would agree. The Sarasota, Fla. man, for example, who got a similar visit from the FBI last year after someone on a boat docked in a marina outside his building used a potato chip can as an antenna to boost his wireless signal and download an astounding 10 million images of child porn, or the North Syracuse, N.Y., man who in December 2009 opened his door to police who'd been following an electronic trail of illegal videos and images. The man's neighbor pleaded guilty April 12.

For two hours that March morning in Buffalo, agents tapped away at the homeowner's desktop computer, eventually taking it with them, along with his and his wife's iPads and iPhones.

Within three days, investigators determined the homeowner had been telling the truth: If someone was downloading child pornography through his wireless signal, it wasn't him. About a week later, agents arrested a 25-year-old neighbor and charged him with distribution of child pornography. The case is pending in federal court.

It's unknown how often unsecured routers have brought legal trouble for subscribers. Besides the criminal investigations, the Internet is full of anecdotal accounts of people who've had to fight accusations of illegally downloading music or movies.

Whether you're guilty or not, "you look like the suspect," said Orin Kerr, a professor at George Washington University Law School, who said that's just one of many reasons to secure home routers.

Experts say the more savvy hackers can go beyond just connecting to the Internet on the host's dime and monitor Internet activity and steal passwords or other sensitive information.

A study released in February provides a sense of how often computer users rely on the generosity - or technological shortcomings - of their neighbors to gain Internet access.

The poll conducted for the Wi-Fi Alliance, the industry group that promotes wireless technology standards, found that among 1,054 Americans age 18 and older, 32 percent acknowledged trying to access a Wi-Fi network that wasn't theirs. An estimated 201 million households worldwide use Wi-Fi networks, according to the alliance.

The same study, conducted by Wakefield Research, found that 40 percent said they would be more likely to trust someone with their house key than with their Wi-Fi network password.

For some, though, leaving their wireless router open to outside use is a philosophical decision, a way of returning the favor for the times they've hopped on to someone else's network to check e-mail or download directions while away from home .

"I think it's convenient and polite to have an open Wi-Fi network," said Rebecca Jeschke, whose home signal is accessible to anyone within range.

"Public Wi-Fi is for the common good and I'm happy to participate in that - and lots of people are," said Jeschke, a spokeswoman for the

Electronic Frontier Foundation, a San Francisco-based nonprofit that takes on cyberspace civil liberties issues.

Experts say wireless routers come with encryption software, but setting it up means a trip to the manual.

The government's Computer Emergency Readiness Team recommends home users make their networks invisible to others by disabling the identifier broadcasting function that allows wireless access points to announce their presence. It also advises users to replace any default network names or passwords, since those are widely known, and to keep an eye on the manufacturer's website for security patches or updates.

People who keep an open wireless router won't necessarily know when someone else is piggybacking on the signal, which usually reaches 300-400 feet, though a slower connection may be a clue.

For the Buffalo homeowner, who didn't want to be identified, the tip-off wasn't nearly as subtle.

It was 6:20 a.m. March 7 when he and his wife were awakened by the sound of someone breaking down their rear door. He threw a robe on and walked to the top of the stairs, looking down to see seven armed people with jackets bearing the initials I-C-E, which he didn't immediately know stood for Immigration and Customs Enforcement.

"They are screaming at him, 'Get down! Get down on the ground!' He's saying, 'Who are you? Who are you?'" Covert said.

"One of the agents runs up and basically throws him down the stairs, and he's got the cuts and bruises to show for it," said Covert, who said the homeowner plans no lawsuit. When he was allowed to get up, agents escorted him and watched as he used the bathroom and dressed.

The homeowner later got an apology from U.S. Attorney William Hochul and Immigration and Customs Enforcement Special Agent in Charge Lev Kubiak.

But this wasn't a case of officers rushing into the wrong house. Court filings show exactly what led them there and why.

On Feb. 11, an investigator with the Department of Homeland Security, which oversees cybersecurity enforcement, signed in to a peer-to-peer file sharing program from his office. After connecting with someone by the name of "Doldrum," the agent browsed through his shared files for videos and images and found images and videos depicting children engaged in sexual acts.

The agent identified the IP address, or unique identification number, of the router, then got the service provider to identify the subscriber.

Investigators could have taken an extra step before going inside the house and used a laptop or other device outside the home to see whether there was an unsecured signal. That alone wouldn't have exonerated the homeowner, but it would have raised the possibility that someone else was responsible for the downloads.

After a search of his devices proved the homeowner's innocence, investigators went back to the peer-to-peer software and looked at logs that showed what other IP addresses Doldrum had connected from. Two were associated with the State University of New York at Buffalo and accessed using a secure token that UB said was assigned to a student living in an apartment adjacent to the homeowner. Agents arrested John Luchetti March 17. He has pleaded not guilty to distribution of child pornography.

Luchetti is not charged with using his neighbor's Wi-Fi without

permission. Whether it was illegal is up for debate.

"The question," said Kerr, "is whether it's unauthorized access and so you have to say, 'Is an open wireless point implicitly authorizing users or not?'

"We don't know," Kerr said. "The law prohibits unauthorized access and it's just not clear what's authorized with an open unsecured wireless."

In Germany, the country's top criminal court ruled last year that Internet users must secure their wireless connections to prevent others from illegally downloading data. The court said Internet users could be fined up to $126 if a third party takes advantage of their unprotected line, though it stopped short of holding the users responsible for illegal content downloaded by the third party.

The ruling came after a musician sued an Internet user whose wireless connection was used to download a song, which was then offered on an online file sharing network. The user was on vacation when the song was downloaded.