eWEEK® Enterprise IT Technology News, Opinion and Reviews

When Hackers and Law Enforcement Team Up We May Be the Losers

By **Larry Seltzer** | Posted 2003-08-09

The case of James "Whitey" Bulger should have been a lesson to the FBI, or perhaps to us all. Now high on the governments Ten Most Wanted list, Bulger used to be a secret buddy of the G, helping them to prosecute the Italian mafia while protecting his own ongoing criminal activities. The FBI allegedly tipped Whitey off to stings and cut deals to keep him out of big trouble.

Now the FBI is moving into the modern technology era and taking their information from anonymous Internet hackers. A recent Court of Appeals decision upheld the use of evidence obtained by a 3rd-party hacker who was encouraged, indirectly perhaps, by the FBI in a criminal case.

Heres the issue: An anonymous hacker, known in the decision only as Unknownuser, hacked into the computer of the appellant, obtained evidence of child pornography, and finked on the appellant to the FBI. The District Court convicted the appellant, locked him up and threw away the key.

But theres a twist in the case. This wasnt Unknownusers first such effort assisting the prosecution, and prior to this appellants case, the FBI was in contact with Unknownuser. They thanked him for the earlier help and assured him—explicitly and implicitly—that he was not the target of any actions by them. They did not advise him to end his illegal hacking activities.

For those of you who dont watch enough Law & Order, under the Fourth Amendment to the U.S. Constitution we are protected against unreasonable searches and seizures. Under the "exclusionary rule," evidence collected by the state in violation of this amendment is inadmissible in court. But a body of law exists that says that evidence collected by private individuals, legally or otherwise, may be admissible, assuming the individual was not acting as an agent of the government. See the above decision for far more detail on all this.

When faced with this evidence of FBI encouragement of Unknownuser, the District Court reversed its original

decision and ruled that Unknownuser was an agent of the government and that the evidence was inadmissible. Then the Circuit Court reversed the decision, saying that the government knew nothing of Unknownusers specific actions in advance and was not actively involved in his private searches. But even the famously conservative Fourth Circuit Court called this a borderline case and said the FBI skated close to the edge.

I asked defense attorney Joshua Dratel about the legal issues.

"Unfortunately, the Fourth Circuit has adopted a technical and semantic interpretation of government participation," Dratel said. "The effect will be to encourage cyber-vigilantism, and promote—in advance—the trading of information by criminals to excuse their own illegal conduct."

This case leaves me speechless at the possibilities for abuse by both the government and criminals. Never mind that it puts the FBI in the position of tacitly encouraging hacking and invasions of computer privacy. As Dratel said, it gives criminals reason to believe that their activities will be tolerated as long as they throw enough information the governments way.

And it could go further; I see nothing in the decision that would prevent Unknownuser from first attempting to blackmail the user he was attacking before passing the information on to the FBI, and no reason to believe that the FBI would care.

Even worse, as Dratel warns, "There also exists the problem of the integrity of the information seized—did the vigilante plant the information there in the first place? We would not tolerate a policy that encouraged and rewarded burglars who happened to find incriminating evidence in the houses they broke into, and we should no more countenance it in cyberspace, where the accountability of the anonymous "Unknownuser" is diminished even further."

More specifically, with the Trojan horse program used by Unknownuser on the appellants computer (Subseven), Unknownuser could have planted all the evidence himself, if he were talented enough, there would be no way to tell the difference. Unknownuser appears, based on the text of the decision, to have acted as an anti-child pornography crusader. But motives, as Whitey Bulger will tell you if you could find him, dont have anything to do with the law here.

In a sense, theres nothing hacking-specific about this issue, still, like so much in the application of law to technology, an existing problem becomes worse. The ease with which a capable user may become and remain anonymous on the Internet means that the way is open for freelance individuals to go out hacking en-masse, searching for evidence of crime in the pursuit of justice or money or whatever. Silly me, I thought it was the job of the FBI to protect us from such people.

Security Supersite Editor Larry Seltzer has worked in and written about the computer industry since 1983.

More from Larry Seltzer