Like Apple, FBI not willing to play nice

Las Vegas Review-Journal

April 1, 2016 Friday

Section: Pg. A011

Length: 609 words

Byline: PARESH DAVE and DAVID PIERSON LOS ANGELES TIMES

Body

LOS ANGELES — Even when courts compel law enforcement agencies to reveal the ways they hack into technology products, it's criminal suspects — not the makers of hardware or software — who are most likely to learn the details.

As Apple Inc. considers legal tactics that could force the FBI to share how it unlocked an iPhone belonging to one of the San Bernardino, California, shooters, a federal court case in Washington illuminates how the judicial process can leave the tech world in the dark.

The case involves the Tor browser, which is popular among activists, dissidents, journalists — and those who want to mask their identities when surfing online. The FBI hacked the browser as part of a sweeping child pornography investigation that led to 1,300 suspects.

In one of the cases, a judge has ordered that the FBI give defense attorneys details about the software flaw that allowed the FBI to identify suspect Jay Michaud of Vancouver, Washington, whose prosecution has been at the forefront of the investigation. But prosecutors on Tuesday opposed the ruling in a heavily redacted document.

They say the defense already has enough information to analyze the operation. And former federal prosecutors say disclosing the vulnerability takes away the ability to use the technique to nab more offenders.

But technology developers and privacy activists fear that consumers' safety could be put at risk if the Tor issue turns out to be an unpatched bug.

The tension will manifest in "much more litigation to understand the techniques used to capture individuals," said Michael Zweiback, an attorney at Alston & Bird and former chief of the Justice Department's cybercrimes section.

The issue will not go away as the FBI's growing interest in probing the Internet for criminal activity will require using "techniques that are more proactive — that are recognized exploits — to get access to information," Zweiback said.

In the Washington case, federal agents briefly seized control of Playpen, a secretive online forum, accessible through Tor, where more than 214,000 members traded what authorities describe as sexually

explicit photos and videos, including of children. The FBI learned the Internet protocol addresses of Playpen visitors by using a software bug linked to Tor to defeat the browser's security measures.

Public defenders for Michaud, who is charged with possession of child pornography, say they can't fully vet the legality of the FBI's investigation without knowing how the agency hacked Tor. While the government has turned over details about the software that identified his address, it hasn't shared information about how that tracking tool was introduced.

Prosecutors and experts say what matters is that the hack didn't tamper with Michaud's data.

"Getting through the lock doesn't matter, as long as the information on the other side of the door isn't affected," Zweiback said, comparing digital searches with physical ones.

Law enforcement generally seeks to protect its hacking methods as long as possible because the techniques' usefulness shrinks when the public or manufacturers are aware, Zweiback said.

Last month, U.S. District Judge Robert Bryan ruled in favor of Michaud. But prosecutors this week asked Bryan to reconsider, saying that the additional information wouldn't address the defense's concerns. Justice and FBI officials didn't have immediate comment.

Attorneys for Apple say they plan to insist that the government explain how, with the help of an undisclosed outside group, investigators bypassed an iPhone 5c's security — the same device authorities had maintained couldn't be opened without Apple's assistance.

Classification

Language: ENGLISH

Publication-Type: Newspaper

Subject: LAW ENFORCEMENT (90%); INVESTIGATIONS (90%); SPECIAL INVESTIGATIVE FORCES (90%); SEX OFFENSES (89%); CHILD PORNOGRAPHY (88%); PORNOGRAPHY (88%); LAW COURTS & TRIBUNALS (78%); CRIMINAL INVESTIGATIONS (78%); COMPUTER CRIME (78%); LAWYERS (78%); CYBERCRIME (78%); LITIGATION (78%); FEDERAL INVESTIGATIONS (77%); CHILDREN (74%); PUBLIC DEFENDERS (73%); JUDGES (73%)

Company: APPLE INC (85%); ALSTON & BIRD LLP (58%)

Industry: COMPUTER SOFTWARE (89%); INTERNET & WWW (89%); COMPUTER CRIME (78%); LAWYERS (78%); CYBERCRIME (78%); LITIGATION (78%); HIDDEN WEB (78%); SOFTWARE DEFECTS (77%); PUBLIC DEFENDERS (73%); MOBILE & CELLULAR TELEPHONES (72%); NETWORK PROTOCOLS (50%)

Geographic: SAN BERNARDINO, CA, USA (79%); LOS ANGELES, CA, USA (79%); WASHINGTON, USA (79%); CALIFORNIA, USA (79%); UNITED STATES (93%)

Load-Date: April 1, 2016