

Resolution in FBI-Apple case prolongs larger legal battle

By Brandon Bailey, AP

SAN FRANCISCO — The FBI's victory in breaking into a San Bernardino killer's iPhone without Apple's help merely prolongs a battle over how far the government can go to examine private messages, photos and other files.

"There's a clash of values and interests that I think will continue," said Ed Black, head of Computer and Communications Industry Association, a trade group whose members include Google, Facebook and Microsoft.

Federal prosecutors have appealed a court ruling that said Apple doesn't have to help them extract data from another iPhone in a New York drug case. Speaking in general, the Justice Department said it will continue seeking digital evidence, "either with cooperation from relevant parties or through the court system when cooperation fails."

After finding its own way to access files on the San Bernardino iPhone, the Justice Department said it no longer needs a court order to force Apple to remove safeguards against guessing that iPhone's passcode. That means Magistrate Sheri Pym won't be ruling on whether a centuries-old law, known as the All Writs Act, provided legal authority for compelling Apple's assistance.

Some in the tech industry worry that authorities will now try to pursue a smaller company — one without the financial and legal resources that Apple had — to win a favorable legal precedent that authorities could then use to pressure other firms — including heavyweights like Apple.

"When you're a company of five people, you don't have a

general counsel's office. You have a card table that everyone sits and codes at," said Morgan Reed, executive director of a tech industry group known as ACT, which represents software application developers.

Although the Justice Department repeatedly insisted that its request for Apple's help applied only to the San Bernardino iPhone, Apple said having to rewrite its iPhone software would make all phones less secure and open the door to more demands from government authorities, both in the United States and other countries.

Tech companies say they turn over the customer data they have, when faced with a legal court order. But many companies are increasingly using encryption and other safeguards that put at least some customer data out of their reach. Companies say they're determined to protect customers' privacy against unwarranted intrusion.

On the flip side, today's popular smartphones contain a wealth of information about their users – who they talk to, where they travel, what they view online – which authorities can use to prosecute suspects, unravel plots and identify accomplices.

"Every case is now a cyber investigation," said Ed McAndrew, a former federal cybercrimes prosecutor now in private practice. "You're going to have electronic devices and technology and online storage in virtually every case."

State and federal authorities in several jurisdictions have confirmed they would like to get access to encrypted smartphones seized in a variety of criminal investigations. In at least a dozen pending cases, the government has cited the same All Writs Act as legal authority to compel Apple's cooperation.

The FBI might be able to apply the same forensic technique it used with the San Bernardino iPhone, but it's not clear if that will work with newer iPhones that have added security

features, said Jonathan Zdziarski, an independent computer forensics expert. The San Bernardino iPhone was a 5C model, which largely had 2012 hardware, although it had a recent version of the iPhone software.

Late Wednesday, the FBI agreed to help an Arkansas prosecutor unlock an iPhone and iPod belonging to two teenagers accused of killing a couple. What is unclear is whether the FBI – which already had the ability to get data from some phones – is using the same techniques as in San Bernardino.

Meanwhile, the government's authority under the All Writs Act remains in dispute. Any decision in the pending New York case will likely be appealed again, said Fred Cate, a law professor and fellow at the Indiana University Center for Applied Cybersecurity Research. "There's no question that will be up in the air until the Supreme Court rules on it," he added.

In the San Bernardino case, most of Apple's biggest competitors – including Google, Facebook and Microsoft – filed court briefs on Apple's behalf. Representatives from those companies didn't respond to requests for comment this week. But Black, the trade group head, said companies recognize the importance access to information is to law enforcement and national security.

But he said many in the tech industry believe authorities went too far by trying to force Apple to write software that would override the security features of its own products.

Members of Congress have discussed legislation on both ends of the spectrum – either to require tech companies' cooperation or to limit law enforcement authority to compel companies' help. The latest case could spur Congress to act, though Black and others don't believe that likely given legislative gridlock on other issues.

That means these battles are likely to recur in court instead.

In a statement this week, the Justice Department said, "It remains a priority for the government to ensure that law enforcement can obtain crucial digital information to protect national security and public safety."

Apple responded by saying it will assist law enforcement in at least some ways as it has in the past. But the company added, "we will continue to increase the security of our products as the threats and attacks on our data become more frequent and more sophisticated."