APPLE vs. THE FBI

The battle between the tech giant and the government agency over the right to search an iPhone may have an enormous impact on our lives

BY BRYAN BROWN

ONE OF THE BIGGEST LEGAL RIGHTS DISPUTES of our time is brewing over something that is a key part of our lives: a smartphone. In February, the tech company Apple defied a federal court order requiring it to help the Federal Bureau of Investigation (FBI) unlock an iPhone 5c. By resisting the judge's order, Apple has set the stage for a legal showdown. That could help define a constitutional right to privacy for Americans in the digital age.

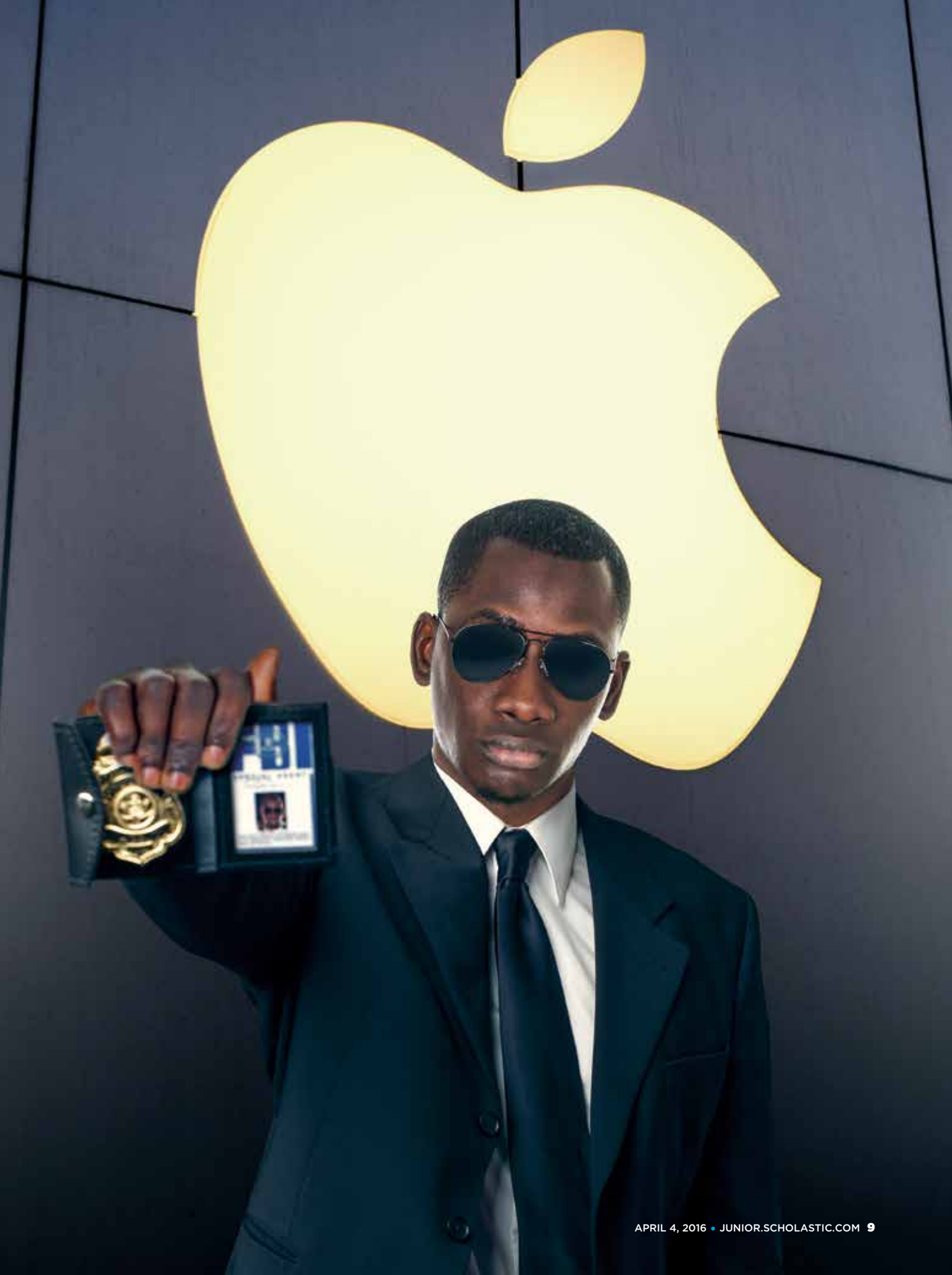
The device in question is not just *any* iPhone. It was used by Syed Rizwan Farook, one of the two shooters who died after killing 14 people last December in San Bernardino, California. The FBI believes that the phone might reveal whether Farook was in touch with anyone before the massacre. The FBI thinks it could even help prevent future attacks.

But the device is locked with a passcode that the agency does not have. Technicians can guess at the code. But iPhones are designed so that after 10 incorrect password attempts, all data will be automatically erased.

The FBI wants Apple to create special software that would disable the auto-erase function. That would allow a computer to try to crack the phone by entering thousands of possible passcodes until it found the right one. Apple has refused to create such software.

The standoff represents a critical moment in an ongoing debate between the tech world and the government. Tech companies manage massive amounts of user data, from photos and text messages to Social Security and credit card numbers. Authorities say that this information is →

ILLUSTRATION: JUSTIN METZ; SHUTTERSTOCK (FBI AGENT); AGE FOTOSTOCK (BADGE)



crucial to solving crimes and stopping terrorists. But Apple protests that user data must remain private to protect citizens from cyber crime and government surveillance.

"The government is asking Apple to hack our own users," Apple CEO Tim Cook wrote in February in an online letter to the company's customers. "The same engineers who built strong **encryption** into the iPhone to protect our users would . . . be ordered to weaken those protections."

Debating Encryption

To the FBI, the iPhone used by the San Bernardino shooter is evidence in a crime. "Fourteen people were slaughtered," FBI Director James Comey recently wrote. "We owe them a thorough and professional investigation under law."

Yet Apple believes that obeying the order would set a dangerous example and threaten privacy rights. "The implications of the government's demands are chilling," Cook said in his online letter.

The relationship between Apple and the authorities was not always so tense. The company has helped unlock thousands of devices for the government in the past. But recent events have changed Apple's position. In 2013, Edward Snowden, who had worked for the National Security Agency (NSA), revealed that the agency was collecting the personal **metadata** of millions of Americans. Apple and other tech companies were embarrassed that the NSA had accessed data through their systems.

Apple was already concerned about government intrusion. The company was encrypting data on its iPhones. In late 2014, it went further. It began making iPhones with unique codes that not even the company could open. (Google uses similar security on its Android phones.)

Government and law enforcement agencies have grown increasingly frustrated with such digital locks. They say the locks keep them from going after criminals or keeping up with what terrorists are doing in cyberspace.

"If the challenges of [reading digital data] threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place," Comey said in a speech last November.

"Encryption threatens to lead all of us to a very dark place."

—JAMES COMEY, FBI

"You can't have a back door that's only for the good guys."

—TIM COOK, APPLE

A Major Precedent

In recent years, government officials have debated whether Congress should write laws requiring tech companies to make a "back door" for law enforcement to access the data in locked devices. These debates have made little progress. Without such laws in place, the FBI is currently relying on a law passed in 1789 to make its case in court against Apple. *(See "Old Law, New World," below, right.)*

Apple argues that a back door could, in effect, allow the government—and perhaps hackers—to get into anyone's phone. Once created, that back door could also be used by authoritarian rulers in other countries against human rights activists or anyone who opposed them.

"You can't have a back door that's only for the good guys," Cook has said. "Any back door is something that bad guys can exploit."

For now, Apple is challenging the judge's order with its own legal action. Eventually, say experts, the matter may reach the U.S. Supreme Court. The final decision could set a major **precedent**, determining when tech companies can be forced to cooperate with authorities.

The FBI has said that it is interested only in the San Bernardino shooter's phone. But lawyers for Apple point out that the U.S. Justice Department* has already asked for at least nine iPhones to be unlocked in other cases.

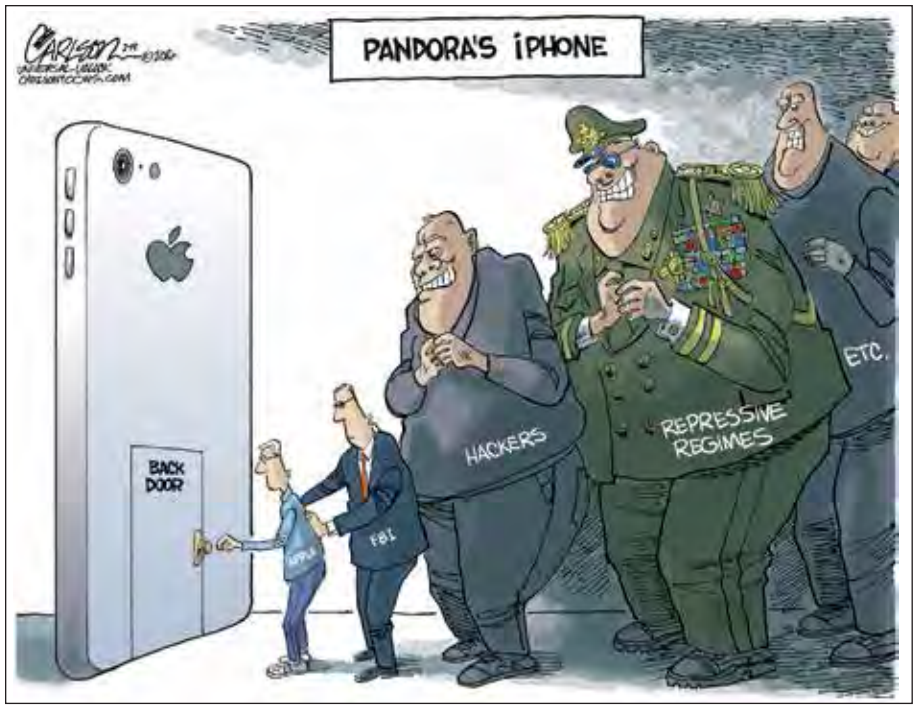
That number will only grow if the government wins its argument, said Dan Guido. He is a co-founder of Trail of Bits, a company that consults with corporations on Internet security. Guido believes that additional requests from other law enforcement agencies could number in the tens of thousands worldwide. That would create an enormous burden for Apple. "They're going to end up having to build a new building and fill it with all kinds of workers," he said.

Privacy or Security?

As the Apple-FBI showdown has played out in the media, most tech companies, including Microsoft, Google, Facebook, Twitter, and Yahoo!, have lined up behind Apple. So have other crusaders against government intrusion. "The FBI

SAUL LOEB/AFP/GETTY IMAGES (JAMES COMEY); STEPHEN LAM/REUTERS (TIM COOK)

*The FBI is part of the U.S. Department of Justice.



◀What's the risk from an iPhone back door? A cartoonist looks to Greek mythology for a possible answer.

is creating a world where citizens rely on Apple to defend their rights, rather than the other way around," Edward Snowden recently tweeted.

The American public, meanwhile, is divided over the matter. But they are leaning in the government's direction. In a recent survey by the Pew Research Center, 51 percent of the people polled said that Apple should unlock the iPhone. Just 38 percent said that it should not.

As *JS* went to press, news accounts reported that Apple engineers were already working on stronger iPhone encryption. That would put future devices beyond government reach even if Apple loses its case. Legal experts say that there could be an endless series of court fights over each technology upgrade.

"We are in for an **arms race** unless and until Congress decides to [clear up] who has obligations in situations like this," Benjamin Wittes told *The New York Times*. Wittes works for the Brookings Institution, a public policy nonprofit.

Indeed, both Apple and the Justice Department say that they want direction from Congress. Some lawmakers have proposed a commission to examine what new laws might be necessary to satisfy the needs of both private citizens and law enforcement.

During testimony before the House Judiciary Committee early last month, supporters of both sides as well as members of Congress agreed that defining the limits of freedom will be difficult. "The big question for our country is, how much privacy are we going to give up in the name of security?" said U.S. Representative Jason Chaffetz, a Utah Republican. "And there's no easy answer to that." ◆

OLD LAW, NEW WORLD

In arguing that Apple should unlock an iPhone, the FBI is reaching back to a statute signed into law by George Washington. The All Writs Act, passed in 1789, allows federal judges to issue a court order compelling a person to supply information that's needed in a legal proceeding.

No one knows if the 227-year-old act will stand up if Apple's case reaches the Supreme Court. Some legal experts believe that the sheer amount of information that Apple might have to supply couldn't have been foreseen in 1789, and having to provide it would impose too much of a burden.

But other experts say the All Writs Act has been adapted to fit different circumstances in the past, and could be again in the future. "The law actually seems to be keeping up with technology by being so broad that we're just reinterpreting it all the time," Internet scholar Irina Raicu told NPR.

YOUR TURN **Which argument—that of Apple or of the FBI—do you find most persuasive, and why?**

Download our **skills sheets** at **junior.scholastic.com**.

STUART CARLSON/UNIVERSAL UCLICK