Can Your Phone Testify Against You?

The Supreme Court is figuring out how to apply the 225-year-old Constitution to today's digital world

BY PATRICIA SMITH

David Riley was pulled over by San Diego police in 2009 because his car registration had expired. During the traffic stop, police found two loaded guns and on examining his smartphone discovered text messages and videos they associated with a local gang. The police arrested Riley and seized his phone.

Later, police found information on Riley's phone linking him to a shooting. Riley was convicted of attempted murder and sentenced to 15 years to life in prison.

But in a landmark ruling about privacy rights this summer, the Supreme Court overturned Riley's conviction. The justices ruled that police need to ask permission or get a warrant from a judge to search someone's phone—just as the police need permission to search inside someone's home.

The ruling, which was applauded by privacy advocates, is the latest example of how the courts are trying to apply the basic rights enshrined in the Constitution to life in the 21st century.

"It's the Supreme Court's job these days to try to balance the Constitution's somewhat antique values with today's technology," says Supreme Court expert Lyle Denniston.

When the Founding Fathers sat down to write the Constitution and the Bill of Rights in the late 1700s, they made sure that the First Amendment protected the right to free speech (among other things) and that the Fourth Amendment protected the right to privacy. But the Framers could never have imagined anything like smartphones, Facebook, and Google—or how...
This section of the Bill of Rights prohibits "unreasonable searches and seizures." A quick guide to your rights.

When the police ask you if they can search something—whether it's your house, your car, or your phone—you always have the right to say no.

If you say no, the police need a court-issued warrant to do a search. They also need a warrant to listen in on the phone calls of suspected criminals.

If you say yes to a search, you're giving up your Fourth Amendment rights.

much of the world's interactions today, from socializing to conducting business, would take place digitally.

In the past few years, the courts have begun wrestling with a host of questions raised by technology: Can students be punished for criticizing their teachers on Facebook? Can websites be required to reveal the identities of those who post anonymous negative reviews? Do laws against cyberbullying violate freedom of speech? (See box, p. 16.)

The cellphone privacy ruling, in Riley v. California, was probably the most important case about digital rights yet decided by the nation's highest court. The nine justices unanimously ruled that because police hadn't obtained a warrant (permission granted by a judge) or Riley's permission before searching his phone, they had violated his Fourth Amendment right to privacy.

What the Framers Thought

The Fourth Amendment prohibits "unreasonable searches and seizures" (see box, below), but figuring out how to apply that 18th-century phrase to 21st-century electronic devices is a challenge. When the Framers wrote the Fourth Amendment, they had in mind the British soldiers before the Revolution who could enter colonists' homes, search their property, and seize...
their belongings without permission. Today, people's most private information, from bank records to personal correspondence and intimate photos, is all accessible from a device that leaves home when they do.

"The fact that technology now allows an individual to carry such information in his hand," Chief Justice John G. Roberts Jr. wrote in his opinion for the Court, "does not make the information any less worthy of the protection for which the Founders fought."

According to the Pew Research Center, 90 percent of Americans have cellphones; almost 60 percent have smartphones. Most of us are rarely without our phones; as Roberts noted in his opinion, 12 percent of Americans even use their phones in the shower.

An average smartphone can hold 100 times more information than the entire 72,000-page collection of James Madison's papers in the Library of Congress, according to privacy advocates. It also contains things simply not available in the physical world: A cellphone's GPS, for example, provides a precise record of a person's whereabouts over time.

These smartphones are, the chief justice said, "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." And, he added, "they could just as easily be called cameras, video players, Rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."

The courts have long allowed warrantless searches in connection with arrests, saying they are justified by the need to protect police officers—from suspects who might be armed, for example—and to prevent the destruction of evidence such as drugs that could be flushed down the toilet.

But the Court said neither justification made sense in the case of cellphones. The possibility that evidence could be destroyed or hidden by "remote wiping" or encryption programs could be addressed by an officer turning off the phone or placing it in a special evidence bag that blocks the signal until a warrant can be obtained.

Tablets & Laptops
The stereotype of Supreme Court justices is that they're old-fashioned and out of touch with today's technology. But all nine justices—who range in age from 54 to 81—have cellphones, and they seemed to understand what was at stake in the case. In an era when 5-to-4 rulings—pitting the conservative block of justices against the liberal one—have become almost standard, the Court spoke with
one 9-to-0 voice on cellphone searches.

Chief Justice Roberts acknowledged that the ruling will make things harder for police. Cellphones "can provide valuable incriminating information about dangerous criminals," he wrote. But, he emphasized, "Privacy comes at a cost."

Besides, Roberts noted, these days law enforcement can sometimes use e-mail to get a warrant within 15 minutes. In a true now-or-never situation—like finding a ticking bomb or a kidnapped child—a warrantless search could be permitted under the Fourth Amendment's exception for emergency circumstances.

In the most basic terms, the ruling will mean that for the 12 million people who are arrested every year—many of them for minor offenses—police won't be allowed to search their cellphones without getting a warrant first. But the ruling's impact will likely be much broader, experts say:

It almost certainly means police will also need a warrant to search other electronic devices, like tablets and laptops, which can also hold the most intimate details of a person's life.

"The big takeaway here is that the Court gets it," says Alan Butler of the Electronic Privacy Information Center. "The Court understands that digital information is different than paper and cabinets and lockboxes."

Butler says the ruling also has huge implications for future privacy cases. "Courts will now be more likely to rule in favor of greater privacy protection for digital records," he says.

And the ruling has implications for various lawsuits challenging the government's widespread collection of Americans' phone call data by the National Security Agency; the NSA surveillance program was revealed to the public last year by Edward Snowden, an NSA contractor who fled the U.S. and is now facing espionage charges.

The cellphone ruling was the second time in the past few years that the Supreme Court has rejected government claims that it needs freedom to use new technologies to fight crime: In 2012, the Court ruled unanimously in United States v. Jones that police violated a drug suspect's privacy rights by placing a GPS tracking device on his car without a warrant.

'The Right to Be Forgotten'

American courts aren't alone in tackling digital issues. In the European Union, the highest court ruled in May on a question vital to anyone who posts updates or photos on Facebook, Twitter, or Instagram: Do people have the right to erase themselves from the Internet, which seems to remember things forever? The court decided that Google and other search engines must consider individuals' requests to remove links that they say contain embarrassing or negative information or otherwise infringe on their privacy.

Google, which received more than 41,000 requests to remove search results in the first month after the ruling, has begun complying with a principle that's already being called "the right to be forgotten." (The ruling doesn't apply to search engines outside Europe, and the links will still be available on Google in the U.S.)

Jeffrey Chester, director of the Center for Digital Democracy, in Washington, D.C., says there are still a lot of big digital issues for the courts to tackle: Who ultimately controls the digital pathways that make up the Internet? Is the vast information gathering of private companies like Google an invasion of privacy? Should every American have equal access to the Internet?

"Our society is going through dramatic changes, and at the heart of it is our relationship with the use of technology," Chester says. "A lot of these issues will wind up before the Supreme Court sooner or later."