Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

High Court Ruling Bolsters Privacy Push By Consumers, ISPs

By **Allison Grande**

Law360, New York (June 25, 2014, 10:12 PM ET) -- The U.S. Supreme Court issued a resounding endorsement of digital privacy rights in its Wednesday decision restricting warrantless cellphone searches, using broad pro-privacy language that is likely to help plaintiffs targeting companies that seek to use their personal data without permission, as well as service providers fighting to limit government access to user data.

In a **unanimous decision** authored by Chief Justice John Roberts, the high court held that law enforcement officers must generally secure a warrant before conducting a search of the digital information on a cellphone seized from an individual who has been arrested.

The federal government and state of California **had urged the justices** to extend the established search-incident-to-arrest exception to the Fourth Amendment's warrant requirement to searches of data on cellphones, but the justices refused. Instead, they concluded that cellphones deserve heightened privacy protections because they implicate "substantially greater" individual privacy interests than other physical objects that may be found on an arrestee due to their capacity to hold vast amounts of personal data.

"The Supreme Court has basically decided that they were going to make a great leap forward and catch up to the 21st century," said Sorrels Udashen & Anton partner and criminal defense attorney Barry Sorrels. "The case shows that they're willing at long last to listen to arguments about the need to protect privacy interests in the ever-changing technological world."

While the high court's conclusion didn't strike many attorneys as surprising, they were caught slightly off-guard by the court's overwhelming support for applying Fourth Amendment protections to cellphone searches.

"That all nine justices agreed with the conclusion sends a clear message that maintaining privacy interests in cellphones is very important to this court," Goodwin Procter LLP partner and former federal prosecutor Grant Fondo said. "The strength of the court's message that data on cellphones is private will likely be a tool for privacy advocates."

Although Chief Justice Roberts made clear in his first footnote that the court's decision does not address the collection or inspection of aggregated digital information, attorneys agreed that both private plaintiffs and service providers are likely to seize on the opinion's broad language to give ammunition to their claims that digital data cannot be used or reviewed without prior authorization.

In the private litigation context, attorneys predict that the class action plaintiffs' bar could

use the ruling to support common-law invasion of privacy claims brought against companies that are accused of accessing and collecting user data without providing consumers with appropriate notice or consent.

"The high court's ruling, for example, flags Internet search history and historical location information as [elements] that individuals do have a privacy interest in," Fenwick & West LLP partner and former federal prosecutor Tyler Newby said. "Therefore, analytics companies and app developers would want to be aware of this opinion because it reinforces what a lot of privacy advocates have been saying in recent years that consumers should at least have the opportunity to be aware of this type of data collection."

Outside the class action setting, service providers such as Google Inc. and Facebook Inc. could also stand to benefit from the analysis put forth by the high court in their ongoing efforts to protect user data from overbroad government access demands. Even though the Electronic Communications Privacy Act only requires the government to obtain a warrant for subscriber data that is less than 180 days or unopened, service providers have been steadily electing to require warrants for older and opened records stored on the cloud or in data centers.

The high court's ruling — particularly its acknowledgement that historic location data can reveal a great deal about an individual — could help service providers erode some lingering resistance to the push for more equal protections for the user data they hold, attorneys say.

"The court's opinion doesn't answer the question that is currently being debated about whether individuals have a reasonable expectation of privacy in location data that is not stored on phones but is in the possession of service providers, but it does give some strength to the argument that there is a reasonable expectation of privacy in this information and that access should require a warrant," Newby said. "The dicta in this opinion is another arrow in the quiver for arguing that they need a warrant and that a subpoena or search warrant is not sufficient."

The decision could also provide a boost to stalled efforts to update the 1986 ECPA statute to require warrants for all content data regardless of its age, especially given Justice Samuel Alito's statement in a separate opinion concurring in part and concurring in judgment that legislatures are "in a better position" than courts to tackle thorny privacy issues.

"The court's decision appears to be an express invitation to Congress to act on ECPA reform and puts the ball in Congress' court to further define expectations of digital privacy," said Ed McNicholas, the co-leader of Sidley Austin LLP's privacy, data security and information law practice.

Indeed, in a statement issued immediately after the decision was handed down, Senate Judiciary Committee Chairman Patrick Leahy, D-Vt., who has been a leading advocate of ECPA reform, urged his colleagues to "act swiftly to pass" the digital privacy update, which last week achieved the milestone of earning co-sponsorship from more than half of the members of the U.S. House of Representatives.

More narrowly, the court's decision will also have an impact on the ability of law enforcement to combat crimes using the treasure trove of data available on cellphones, a potential downside that Chief Justice Roberts characterized as "a cost" of privacy.

But attorneys noted that the court's preservation of the police's ability to cite certain exigent circumstances, such as a fear that a phone might be used to detonate a bomb, provided enough leeway for law enforcement to carry out their duties.

"The court has clearly said that there has to be articulable facts that suggest that a

cellphone has to be searched then and there, which appears consistent with how the Constitution is intended to protect against warrantless searches," said Peter Toren, a Weisbrod Matteis & Copley PLLC partner and former federal prosecutor.

While the ruling put to rest the issue of the constitutionality of warrantless cellphone searches conducted at the time of arrest, attorneys noted that there are still a plenty of privacy issues left for the court to tackle.

"This is likely to be the first in a series of court battles that will address these issues," said former federal prosecutor Philip H. Hilder of Hilder & Associates PC. "If you take the rationale that the information stored on phones is protected and needs a warrant, then that can be extended to apply to wider circumstances, which is likely to spark court challenges."

Riley is represented by Jeffrey L. Fisher of Stanford Law School, Donald B. Ayer of Jones Day and Patrick Morgan Ford.

The state of California is represented by Solicitor General Edward C. DuMont.

Wurie is represented by Judith H. Mizner of the Federal Public Defender Office for the Districts of Massachusetts, New Hampshire and Rhode Island.

The federal government is represented by Deputy Solicitor General Michael Dreeben.

The cases are David Leon Riley v. State of California, case number 13-132, and U.S. v. Brima Wurie, case number 13-212, in the U.S. Supreme Court.

--Editing by Elizabeth Bowen and Christine Chun.