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 Rebuffs Wider Privacy Rights In Recent Term

By **Dietrich Knauth**

Law360, New York (August 23, 2011) -- The U.S. Supreme Court showed a reluctance to extend privacy privileges beyond rock-solid precedent in its recent term, shooting down a Vermont law that sought to protect doctors' prescription histories from data mining marketers and denying AT&T Inc.'s bid to extend personal privacy protection to corporations.

Technology has muddled definitions for both “privacy” and “free speech,”and they're clashing in a new legal gray area that raises questions about when data collection crosses privacy lines, as in the recently decided Vermont case and in an upcoming case that will examine questions the legality of police tracking a suspect with GPS data, attorneys said.

The Supreme Court's approach over the past term indicates that the answers will be found in close readings of the particular facts and the language of the relevant laws in each case, rather than broad interpretation of privacy rights, they said.

“Privacy means so many different things that you always have to look closely at what someone is claiming when they say there is a right to privacy,” said Rex Heinke, co-head of Akin Gump's Supreme Court and appellate practices."New technologies create new versions of these same problems.”

One closely watched case from the past term, Sorrell v. IMS Health Inc., could be a harbinger of future privacy disputes over large-scale commercial data collection and analysis, Heinke said. In a 6-3 split, the high court struck down a Vermont law aimed at preventing pharmacies from selling to marketers information about doctors' prescribing practices, gleaned from the prescriptions they fill.

While the high court ruled narrowly on the case, allowing a marketer's free speech right to publish collected prescription data to trump a doctor's right to professional privacy, the decision has raised larger concerns about the privacy implications of data mining, which has become an ever-growing industry.

“There was a lot of speculation that there were greater privacy issues at stake and that the Vermont decision could have broader negative impacts on privacy protections,” said Deven McGraw, the director of the Health Privacy Project at the Center for Democracy and Technology.

The Supreme Court's ruling and dissenting opinion focused on the balance between the marketers' First Amendment rights and Vermont's goal of fighting an increase in drug costs. Justice Anthony Kennedy, writing for the majority, said that Vermont's law did not protect a legitimate privacy right because it allowed disclosure of the doctor's data to some parties, but not to pharmaceutical marketers.

“Privacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers,” Justice Kennedy said.

Both Vermont and the Electronic Privacy Information Center, in an amicus brief, invited a potentially broader ruling by raising concerns about doctors' professional privacy and risk to the privacy of patient data, according to McGraw.

CDT didn't file an amicus brief in the case, and was skeptical about attempts to position the case as a battle between free speech and privacy — a battle that privacy tends to lose, she said.

While CDT shares some of the concerns that EPIC raised about the safety of so-called deidentified medical data, which can be sold after removing information that could identify a patient, it believed that the case wasn't the right place for those arguments, she said.

In a worst-case scenario, an overly broad ruling could make new law and damage privacy by discouraging the use of deidentified data, McGraw said.

“Those are policy issues that haven't been sufficiently discussed by Congress and regulators, who are better suited to handle them,” she said.

In rejecting the privacy defense, the Supreme Court established a clear rule that the government cannot pick and choose which groups get access to controlled information, potentially allowing greater access to government information than ever, according to Tom Julin of Hunton & Williams LLP, who represented IMS Health and other marketers in the Supreme Court case.

In another ruling with significant consequences for privacy, AT&T v. FCC, the court held that personal privacy protections under the Freedom of Information Act do not apply to corporations. AT&T had tried to stop the Federal Communications Commission from disclosing embarrassing information about an agency investigation to AT&T's rivals, based on a personal privacy exemption in FOIA.

This time, in contrast to its 2010 ruling in Citizens United v. FEC, which found no distinction between a corporation and an individual when it comes to protected political speech, the Supreme Court held that corporations, while “persons,” did not have a right to personal privacy.

In an 8-0 opinion written by Chief Justice John Roberts, the court found that Congress didn't intend for companies to be entitled to personal privacy protection in the literal sense. Adjectives generally relate to their corresponding nouns, but some vary widely, Justice Roberts wrote, adding by way of example that nouns such as “corn” and “crank” have little to do with the adjectives “corny” and “cranky.”

"The protection in FOIA against disclosure of law enforcement information on the ground that it would constitute an unwarranted invasion of personal privacy does not extend to corporations,” the opinion said. “We trust that AT&T will not take it personally.”

The ruling removes an argument available to companies seeking to prevent disclosures under FOIA, leaving them reliant on the government to redact information that is confidential or sensitive under a separate exemption, as the FCC did in the AT&T case. But the wordplay and dictionary-reliant definitions in the decision made the ruling broader than it would have been if it had focused narrowly on the question of Congress' intent, according to Julin.

“The court just went too far in that case in saying that in no circumstances should a corporation have any right to privacy over information held by the government,” he said.

In the upcoming term, the high court will hear U.S. v. Jones, which raises the question of whether police violated a suspect's right to privacy by placing GPS tracking device on his car and tracking his movements.

The high court drew a clear line for when police may enter a private home this term in Kentucky v. King – but that case did not really raise new privacy concerns, attorneys said.

In Kentucky v. King, attorneys for a man who was arrested for drug possession argued that the police created a false "emergency situation" as an excuse to enter his home, specifically by knocking on his door, then breaking in out of fear that he would destroy evidence in response to the police presence.

The court ruled 8-1 in favor of the police, saying that their actions wouldn't be illegal unless they violated the Fourth Amendment or threatened to violate the Fourth Amendment in creating the emergency situation.

U.S. v. Jones raises two new privacy concerns related to technology, according to Heinke. First, the court must decide whether the data compiling all of a suspect's car's movements, once collected, can be used without violating privacy, and second, whether planting the device is itself a violation of privacy. The government has argued that the data was no different from what would have been compiled by having agents trail the suspect around town and that a person would have no reasonable expectation of privacy for a vehicle on public streets.

While Heinke said he was sympathetic to the government's arguments that collecting GPS data was similar to tailing a suspect, the fact that the device was planted in a vehicle changes the picture because the vehicle is private property.

“You're intruding into someone's private space, their car, where it seems one would have a reasonable expectation of privacy,” he said.

Because the Constitution does not explicitly include the right to privacy, the government can act to uphold privacy in some cases, while arguing against it in others, especially when dealing with legal frontiers created by new technologies, according to Julin. He sees the Jones case, in which the government was collecting information, and the Sorrell case, in which the government tried to block the distribution of information, as “opposite sides of the same issue.”

The “enormous industry” of data collection and analysis is not going away any time soon, and in the absence of clear laws, there will be many more legal fights over what data can be collected and how it can be used, Julin said.

While individual information often has no economic value, it becomes very valuable when aggregated in large quantities, according to Heinke. Who owns that information, and who can profit from it, are still unsettled legal questions.

Congress is already mulling several laws aimed at putting limits on data mining and targeted and behavioral advertising, according to Julin, but the Sorrell ruling could slow those efforts.

“I think its going to be very difficult for them to pass some kind of law,” Julin said. “The Supreme Court is really saying that its not a proper role for government to protect individuals from targeted marketing.”

Any new laws would have to take into account the First Amendment issue of discrimination, which sank the Vermont law, according to Heinke.

“What killed the statute in Sorrell was that it essentially allowed the information to be used for any purpose except for promoting the branding of the drug,” Heinke said. “If you had a statute that had no exemptions or very narrow exemptions, then it's still an open question as to how that would do in the court.”

--Editing by Pamela Wilkinson and Chris Giganti.