CNET News
Politics and Law
March 29, 2010 6:06 PM PDT

# Tech coalition pushes rewrite of online privacy law

by Declan McCullagh



A broad coalition of companies including Google, Microsoft, and AT&T, joined by liberal and conservative advocacy groups, will announce a major push Tuesday to update federal privacy laws to protect mobile and cloud computing users, CNET has learned.


They hope to convince the U.S. Congress to update a 1986 law--written in the pre-Internet era of telephone modems and the black-and-white **Macintosh Plus**--to sweep in location privacy and documents stored on the Web through services like Google Docs, Flickr, and Picasa.

That law, the Electronic Communications Privacy Act, or ECPA, is notoriously convoluted and difficult even for judges to follow. The coalition hopes to simplify the wording while requiring police to **obtain a search warrant** to access private communications and the locations of mobile devices--which is not always the case today.

Under current law, Internet users enjoy more privacy rights if they store data locally, a legal hiccup that some companies fear could slow the shift to cloud-based services unless it's changed. "The main thing that's broken about ECPA is that it penalizes you for using cloud computing," says **Marc Zwillinger**, a partner at Zwillinger Genetski in Washington, D.C. who specializes in data privacy law and has provided the coalition with legal advice.

What's unusual about the coalition to be announced Tuesday is that it includes occasional rivals including AOL, Loopt, and Salesforce.com, sources told CNET. The nonprofit participants, too, have sharply different political views: the American Civil Liberties Union, Americans for Tax Reform, the Center for Democracy and Technology, the Progress and Freedom Foundation, the Electronic Frontier Foundation, and Citizens Against Government Waste have signed on.

This push for cell phone privacy is likely to put the coalition at odds with the Obama Justice Department. A few weeks ago, Justice Department prosecutors **told** a federal appeals court that Americans enjoy no reasonable expectation of privacy in their mobile device's location and that no search warrant should be required to access location logs.

Sen. Patrick Leahy, the Democratic chair of the Judiciary committee, **said** at the time that it was necessary to "update and clarify the law to reflect the realities of our times." One coalition participant said the group has had meetings with the FBI, the White House counsel, and several congressional staffers.

There have been dozens of cases in the last year or so where the police have asked wireless companies for logs of which cell phones contacted a tower at a specific time, says **Al Gidari**, an attorney who advises wireless carriers. The proposed ECPA changes would require a search warrant for that information as well.

Facebook is not participating formally in the coalition at this point, a spokesman said on Monday, but the company is "interested in monitoring the discussion and plan to evaluate joining in the future."

"It's rare for there to be such a broad consensus that reform is needed," says **Ryan Radia**, a technology policy analyst at the free-market **Competitive Enterprise Institute**, one of the coalition members. "Federal privacy law today doesn't really reflect the realities of the

Possible fixes to ECPA have been talked about before, of course, at law school conferences and occasionally on Capitol Hill as well. Zwillinger, the data protection lawyer, co-authored a **2007 law review article (PDF)** proposing more privacy protections. But until now, there has been no broad coalition pushing to enact them.

**Julian Sanchez** of the **Cato Institute**, which is sympathetic to the coalition's efforts but has not joined, notes that judges have reached different conclusions about how ECPA applies to criminal investigations. "It's absurd that in 2010, we're publicly unclear about what level of protection our e-mails are entitled to," Sanchez says.

## Four privacy principles

The groups plan to announce four principles, buttressed by legal analyses including one by **Jamie Gorelick**, a former deputy attorney general now in private practice at a Washington, D.C. law firm, according to one source. The principles apply only to government access to data stored by Internet and telecommunications companies and do not regulate the private sector or private litigants.

First, police may obtain "communications that are not readily accessible to the public only with a search warrant." Second, police may access "location information regarding a mobile communications device only with a warrant." Third, additional privacy protections would be extended to legal requests for outgoing and incoming call records, which are known as pen registers and trap and trace devices.

Fourth, police may use "subpoenas only for information related to a specified account or individual"--which would bar a subpoena to AT&T asking for information about anyone connecting to one cell site at a certain time, or prevent a subpoena to Google asking for anyone searching for "weaponized anthrax" on a specified date. (That information might still be available, however, to law enforcement officials armed with valid search warrants.)

The last point is important because not all companies that store such data push back as much as they should, says Gidari, the partner at Perkins Coie in Seattle who contributed to the coalition's principles. "You've got to have a set of standards that make users comfortable that the government is not willy-nilly accessing things without judicial oversight," he says.

Gidari likens the current state of the law to what existed after the U.S. Supreme Court's 1928 **Olmstead v. United States** case, which said that federal agents' warrantless wiretapping of phone conversations did not violate the Fourth Amendment and the conversations could be used as evidence in a criminal prosecution. The decision was not overturned until the 1967 **Katz v. United States** case, in which the majority said: "Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."

Just as the Katz decision said that the right to privacy accompanies a person no matter where he or she travels, today's coalition proposes that the right to privacy should accompany data no matter where it is stored. At the moment, "when you put your digital bits out where a third party can touch them, you're waiving your Fourth Amendment rights," Gidari says. "It almost seems like a throwback."

**Update on March 29 at 8 p.m.:** I've heard back from Brian Knapp, the chief operating officer of social location-mapping firm **Loopt** in Mountain View, Calif. He sent me e-mail saying: "We've already enacted the highest legal standard when it comes to government requests -- a warrant based on probable cause is required under our Information Requests Policy and has been for some time now. Enacting principle #2 under this initiative clearly makes the law what Loopt already believes to be the applicable standard in its case."

Declan McCullagh has covered the intersection of politics and technology for over a decade. E-mail Declan.