

# Justice Department opposes digital privacy reforms

by [Declan McCullagh](#)

The U.S. Justice Department today offered what amounts to a frontal attack on proposals to amend federal law to better protect Americans' privacy.

James Baker, the associate deputy attorney general, warned that rewriting a 1986 privacy law to grant cloud computing users more privacy protections and to require court approval before tracking Americans' cell phones would hinder police investigations.

This appears the first time that the Justice Department has publicly responded to a set of digital privacy proposals [unveiled last year](#) by a coalition of businesses and advocacy groups including AT&T, Google, Microsoft, eBay, the American Civil Liberties Union, and Americans for Tax Reform.

Baker told ([PDF](#)) a Senate committee that requiring a search warrant to obtain stored e-mail could have an "adverse impact" on criminal investigations. And making location information only available with a search warrant, he said, would hinder "the government's ability to obtain important information in investigations of serious crimes."



James Baker, associate deputy attorney general  
(Credit: U.S. Senate)

Sen. Chuck Grassley, an Iowa Republican, seemed to agree. It's crucial, he said, "to ensure we don't limit (law enforcement's) ability to obtain information necessary to catch criminals and terrorists who use electronic communication." He also suggested that requiring warrants would lead to "increased burdens on the court system."

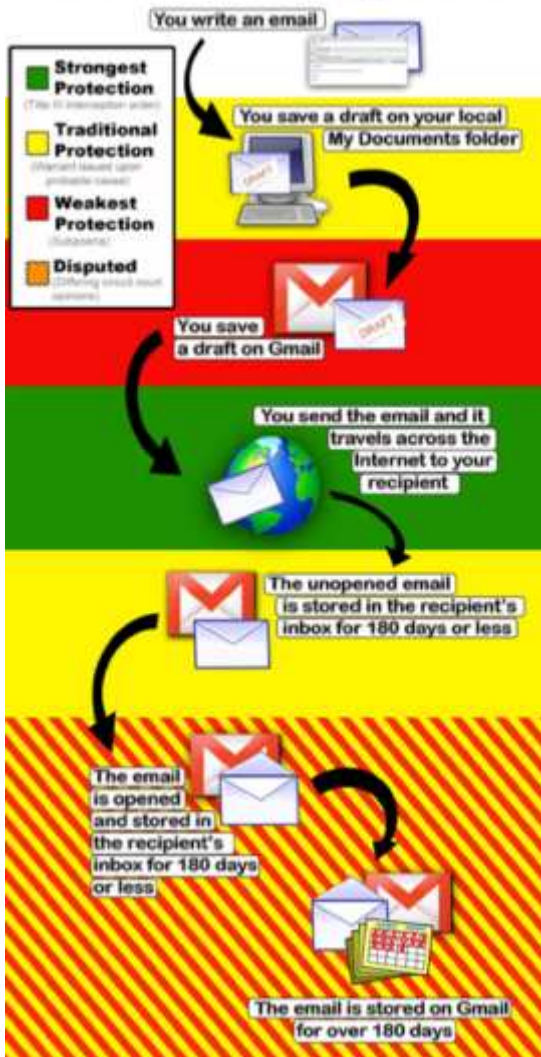
The question at hand is rewriting the [Electronic Communications Privacy Act](#), or ECPA, which was enacted in the pre-Internet era of telephone modems and is so notoriously convoluted, it's difficult even for judges to follow.

The [Digital Due Process 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 could slow the shift to cloud-based services unless it's changed.

Baker did make it clear that the broader Obama administration does not--at least not yet--have a position on how ECPA should be changed. An interagency task force has been meeting, but has not reached a consensus or produced a recommendation, and the Commerce Department has taken a position ([PDF](#)) that's more favorable toward privacy and business interests.

But the Justice Department, Baker said, was concerned that requiring more judicial approval would hinder investigations. "Speed is essential," he said. "If Congress slows down the process, this would have real-life consequences, particularly where human life is involved."

### The Different Stages of Privacy Protection for a Single Email



Caption: The odd ways a 1986 privacy law provides less (or more) protection to an e-mail message, depending on what stage it's in.

(Credit: Ryan Radia/CEI)

Sen. Patrick Leahy, a Vermont Democrat and chairman of the Judiciary committee, said that current law has "shortcomings" that need to be addressed.

"It's very clear from the hearing today that Senator Leahy is interested in moving an ECPA reform bill," said Greg Nojeim, senior counsel at the [Center for Democracy and Technology](#), which is coordinating the Digital Due Process coalition. "DDP has had great success in keying up this issue and giving members of Congress a proposal that has moved the process forward."

Ross Schulman, counsel to the [Computer and Communications Industry Association](#), said he was optimistic that the Justice Department might alter its stance: "It doesn't mean that DOJ's final position would be to oppose (proposals) such as search warrants for electronic data." Google and AT&T referred questions to the Center for Democracy and Technology.

Also today, a group of conservative and libertarian groups sent a letter ([PDF](#)) to Leahy and Grassley urging them to move "immediately" to "extend the Fourth Amendment's protections against the unreasonable search and seizure of digital documents and other electronic information." It was signed by groups including [TechFreedom](#), the [Competitive Enterprise Institute](#), FreedomWorks, and the Liberty Coalition.

"The current standards are messy, inconsistent, and unclear," says [Julian Sanchez](#), a research fellow at the libertarian [Cato Institute](#), which is not part of either group. "I think DOJ has realized is that this is largely severable from the question of whether you...establish consistency in favor of uniformly protecting privacy--or uniformly permitting easier government access."

Baker, the associate deputy attorney general, also offered two suggestions: that any ECPA rewrite might include "the disclosure by service providers of customer information for commercial purposes," and that the practice of telecommunications companies charging fees for the time it takes to process routine police requests should be curbed.

The second suggestion, Sanchez suggested, might end up being used by the Justice Department as a bargaining chip "to splinter the telecom-civil libertarian coalition."

As for the first suggestion, Marc Rotenberg, director of the [Electronic Privacy Information Center](#), said his group never joined the Digital Due Process coalition because it was "unwilling to address that issue which, we believe, for users is straightforward and obvious."

"ECPA amendments should cover commercial use of user data," Rotenberg said.

---

Here's how the Justice Department's testimony squares with the coalition's principles:

**Digital Due Process Coalition Principle No. 1** An Internet or telecommunications provider may "disclose communications that are not readily accessible to the public only with a search warrant issued based on a showing of probable cause."

Justice Department's response ([PDF](#)): A warrant is too restrictive because "if a person stores documents in her home, the government may use a subpoena to compel production of those documents." In addition, "not all federal agencies have authority to obtain search warrants." Finally, there's the potential "adverse impact on criminal as well as national security investigations if a probable cause warrant were the only means to obtain such stored communications."

**Digital Due Process Coalition Principle No. 2:** Police may access "prospectively or retrospectively, location information regarding a mobile communications device only with a warrant."

Justice Department's response: For less precise information from cell towers, a "requirement of probable cause has hampered the government's ability to obtain important information in investigations of serious crimes." A warrant should be used only for "prospective E-911 Phase II geolocation data," typically "derived from GPS or multilateration."

**Digital Due Process Coalition Principle No. 3:** Police should be allowed to access "prospectively or in real time, dialed number information, e-mail to and from information, or other data currently covered by the authority for pen registers and trap and trace devices only after judicial review and a court finding" that specific and articulable facts show it's relevant and material to an ongoing criminal investigation. That's a lower standard than a search warrant's probable cause requirement, but in practice perhaps not that much lower.

Justice Department's response: It "makes sense that a person using a communication service should be able to consent to another person monitoring addressing information associated with her communications." (In a 2006 brief to the Sixth Circuit in Warshak, the DOJ argued there could be a terms of service exemption: "The Fourth Amendment allows a third party to consent to the search of another's container when the owner expressly authorize[s] the third party to give consent...Any expectation of privacy can be waived, even in a service available to the public.")

Read more: [http://news.cnet.com/8301-31921\\_3-20051461-281.html#ixzz1IqUWOSDu](http://news.cnet.com/8301-31921_3-20051461-281.html#ixzz1IqUWOSDu)