Is Your Gmail Safe From the G-Men? | Print |

Written by Michael Tennant

Monday, 11 April 2011 15:23

0 Like 0

Does the Fourth Amendment's requirement that the government obtain a warrant to search one's effects based on probable cause apply to e-mail communications? It all depends on where those e-mails are being stored.

Under the 1986 Electronic Communications Privacy Act (ECPA), if the e-mail is downloaded to the recipient's computer and stored there, the Fourth Amendment applies. If, however, the e-mail is being stored "in the cloud" (i.e., on a third-party server), then the Fourth Amendment only applies for the first 180 days of storage.

Or maybe not. "The current standards are messy, inconsistent, and unclear," the Cato Institute's Julian Sanchez told CNET's Declan McCullagh, who writes that ECPA "is so notoriously convoluted, it's difficult even for judges to follow."

Digital Due Process, a coalition of technology and telecommunications companies and advocacy groups that is pushing for reform of ECPA, details some of the difficulties in interpreting the law on its website:

> In the past 5 years, no fewer than 30 federal opinions have been published on government access to cell phone location information, reaching a variety of conclusions….
>
> A district court in Oregon recently opined that email is not covered by the constitutional protections, while the Ninth Circuit has held precisely the opposite. Last year, a panel of the Sixth Circuit first ruled that email was protected by the Constitution and then a larger panel of the court vacated the opinion.

The law, McCullagh points out, "was enacted in the pre-Internet era of telephone modems," when online time and storage were both expensive, so most e-mails were downloaded to local computers for reading and storage. ECPA considers e-mails stored in the cloud for more than 180 days to be abandoned and therefore not protected by the Fourth Amendment, a provision that might have made sense 25 years ago but is clearly outmoded today. Similarly, cellphones were relatively scarce in 1986, so the law does not address government's attempts to obtain location data from these and other mobile devices, leading to conflicting judicial opinions on the subject.

Digital Due Process and other reformers are asking for ECPA to be simplified and made consistent, protecting e-mail and other forms of electronic communication regardless of where those messages have been stored and whether or not they have been accessed. They also want mobile device location data similarly protected. In short, they simply request that the law apply the Constitution to electronic data, requiring government to obtain a warrant to search it.

Naturally, the Justice Department doesn't see things that way, preferring the relatively free hand that ECPA gives law enforcement to search e-mails and location data. Thus, Associate Deputy Attorney General James Baker told the Senate Judiciary Committee that forcing the government to obtain a search warrant before it can access stored e-mail could have an "adverse impact on criminal as well as national security investigations." Furthermore, he testified, "some courts' requirement of probable cause has hampered the government's ability to obtain important information in investigations of serious crimes." He also, as Wired.com's David Kravetz noted, "invoked the usual parade of horribles in his argument," from spies to organized criminals to kidnappers to the all-purpose bogeyman of the 21st century, terrorists. Potential abuse of such unfettered search powers, as has occurred, for instance, with the Patriot Act's "National Security Letters," did not manage to find its way into Baker's testimony.

Whose arguments carry more weight with Congress, the private sector's or the federal government's? Based on Judiciary Committee Ranking Member Chuck Grassley's (R-Iowa) remarks in response to Baker's testimony, it seems clear that he sides with the government. McCullagh writes:

> It's crucial, [Grassley] 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."

Kravetz isn't surprised, saying, "Don't expect Congress to come out in favor of expanding Americans' civil liberties in the post–Sept. 11 world." He points out that

> Congress has held countless hearings about reforming the Patriot Act, too. In the end, however, lawmakers have repeatedly punted on that issue, and we suspect they will embark on the same course when it comes to reforming EPCA.

Perhaps so; perhaps not. Judiciary Committee Chairman Patrick Leahy (D-Vt.) was more open to addressing EPCA's "shortcomings," McCullagh reports. Even the Obama administration, he adds, isn't opposed to the general notion of reform and could be persuaded to move in the right direction:

> 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 that's more favorable toward privacy and business interests.

If ECPA reform takes place at all, let us hope it moves in the direction of "privacy and business interests" and away from untrammeled state power. The future of electronic communications, increasingly dependent on cloud technology, depends on protecting such communications from the prying eyes of state snoops. Liberty is enhanced by it. And the Constitution demands it.