Greater Email Privacy Won't Hinder Law Enforcement

Richard Lardner, Associated Press

WASHINGTON — A Senate bill to protect the privacy of electronic communications won't keep federal agents from combing through your inbox if they believe a crime has been committed, legal experts say. Federal and state authorities still will have a robust set of tools to track down lawbreakers even as these officials oppose changes supported by a broad coalition of technology companies and public interest groups.

The legislation, which the Senate Judiciary Committee was expected to consider Thursday, would update a 26-year-old law by requiring police to obtain a search warrant from a judge before accessing the content of all emails and other private information from Google, Yahoo and other Internet providers. Under the current law, the 1986 Electronic Communications Privacy Act, a warrant is needed only for emails less than 6 months old.

Supporters of the bill, sponsored by Judiciary Committee Chairman Patrick Leahy, D-Vt., say the changes are necessary to overhaul a law that is outdated in an era of cloud computing, cheaper electronic storage, social networking and wireless phones. Such advances in technology have dramatically increased the amount of stored communications in ways no one anticipated a quarter of a century ago.

The Justice Department has resisted the changes. The associate deputy attorney general, James Baker, urged the committee last year to consider the adverse impact on criminal and national security investigations if a warrant were the only means for law enforcement officials to obtain emails and other digital files.

But setting the bar higher doesn't prevent law enforcement agencies from doing their jobs, according to current and former prosecutors, judges and attorneys who specialize in privacy issues. Federal law enforcement authorities in four Midwestern and Southern states have been working with the more demanding warrant requirement since 2010 after an appeals court ruled warrantless access to emails was unconstitutional. To get a warrant, a judge must have proof of probable cause that a crime is being committed.

"I don't see anything (in the Senate bill) that's going to seriously concern law enforcement in terms of our ability to request warrants and to get the contents of the material that we need," said Joseph Cassilly, the state's attorney in Harford County, Md., and a former president of the National District Attorneys Association. "Since you've already got to get warrants for the stuff that's less than 180 days, it's obviously not an insurmountable standard."

Nor does the legislation weaken other methods used by law enforcement for

collecting electronic information. A subpoena signed by a federal prosecutor — not a judge — will continue to be sufficient for obtaining routing data from third-party Internet providers that can identify the sender of an email and the location where the message was sent.

Police also can use what is known as a "D order" to get the "to" and "from" addresses of an email, but not the contents. These orders must be issued by a judge, but the agency seeking one need only show there is reasonable suspicion of a crime — a lower legal standard than probable cause.

In a Nov. 21 letter to Leahy, 30 former federal and state prosecutors and judges said the bill would provide "a much needed judicial check on when the government can access our private digital information." Concerns that the bill would keep law enforcement from acting quickly during emergencies are unfounded, they added, because the Senate bill does not change a provision in the existing law that compels third-party providers to give the government information in situations where lives are at risk or children are being exploited or abused.

Digital Due Process, a wide-ranging coalition that includes Google, Microsoft and Twitter, as well as the American Civil Liberties Union and Grover Norquist's Americans for Tax Reform, has mounted a public relations campaign supporting the Senate bill. The coalition says updating the law will clear the "murky legal landscape" for companies and consumers alike and provide the proper safeguards for the vast amounts of information stored in server farms.

There's money at stake, too. The global market for cloud computing via the Internet is estimated to be $240 billion by 2020. But the Business Software Alliance, a coalition member that represents Apple, Intel and Microsoft, said U.S. cloud providers are at a disadvantage unless online privacy and security laws are changed. If consumers aren't sure their information is being properly protected on the remote, networked computer servers that make up the cloud, they'll take their business elsewhere.

Use of the law has been interpreted inconsistently by the courts, further fuel for those pushing for an overhaul. In a 2010 decision, the 6th U.S. Circuit Court of Appeals in Cincinnati ruled that an Ohio businessman's constitutional rights were violated when federal investigators obtained thousands of his emails without warrants. Now investigators in states covered by the 6th Circuit — Ohio, Michigan, Kentucky and Tennessee — must obtain warrants for all emails. But that's not the law in other federal circuits.

In the 9th Circuit Court of Appeals, which covers California, Washington, Oregon and six other Western states, judges ruled that a search warrant was required for both opened and unopened email, but only if left on a server for less than 180 days. The Justice Department has argued that a search warrant is required for unopened email left on a server for less than 180 days, but not for opened email less than 180 days old.

The decisions mean different rules apply depending where an investigation begins.

How should emails be treated if a case starts in Pennsylvania and the messages are stored on a server in California, the hub for Google, Yahoo and other major Internet businesses?

"It's very confusing," said Hanni Fakhoury, a staff attorney at the Electronic Frontier Foundation in San Francisco. "Law enforcement will never admit this, but a uniform search warrant standard is easier for them."