Written by **Michael Tennant** on May 30, 2016

FBI Gets Warrantless E-mail Snooping Added to Two Senate Bills

The Federal Bureau of Investigation wants to be able to obtain information on individuals' e-mails, and possibly their Web-browsing history, without a warrant, and now two bills in the Senate — one of them, ironically, aimed at strengthening e-mail-privacy protections — have been amended to give the agency this power.

The FBI already uses its controversial National Security Letters (NSLs) to obtain telephone billing records without a warrant while preventing service providers from informing anyone about the demands. Though once used sparingly, NSLs have been employed much more frequently since the September 11, 2001, terrorist attacks. "In 2015," reported Reuters, "requests for customer records via NSLs increased nearly 50 percent to 48,642 requests, up from 33,024 in 2014, according to a U.S. government transparency report."

The agency obtained e-mail subject lines and metadata and users' browsing history via NSLs until a 2008 Justice Department legal opinion stated that the agency "had interpreted its powers overly broadly," according to the *Intercept*, which noted that "ever since, the FBI has tried to get that power and has been rejected." FBI Director James Comey told the Senate Intelligence Committee in February that his agency's inability to get such electronic records resulted from a "typo" in the law and vowed to get Congress to change the law.

Last week, some in the Senate attempted to make Comey's dream a reality.

First, a provision was added to the Senate's annual intelligence-authorization bill to permit the FBI to use NSLs to obtain "electronic communication transactional records," which could include e-mail subject lines and metadata (such as time stamps) as well as a list of URLs accessed by an individual. This was a particularly underhanded way of getting the provision passed since the bill is debated in secret.

On Tuesday, the bill passed the Senate Intelligence Committee overwhelmingly. The lone dissenting vote came from Senator Ron Wyden (D-Ore.), who called the provision "a major expansion of federal surveillance powers."

"This bill takes a hatchet to important protections for Americans' liberty," Wyden said in a statement. "This bill would mean more government surveillance of Americans, less due process and less independent oversight of U.S. intelligence agencies. Worse, neither the intelligence agencies nor the

bill's sponsors have shown any evidence that these changes would do anything to make Americans more secure."

Wyden's colleague on the committee, Senator Martin Heinrich (D-N.M.), also raised concerns about the bill, though he apparently did not have the courage of his convictions when it came time to vote the bill out of committee.

"This represents a massive expansion of government surveillance that lacks independent oversight and potentially gives the FBI access to Americans' email and browser histories with little more than the approval of a manager in the field," Heinrich said in a statement.

Heinrich pointed out that the FBI can already get the information it is seeking by obtaining a warrant from the Foreign Intelligence Surveillance Act (FISA) court. Indeed, this should hardly be a burden at all given that the court, whose proceedings are shrouded in secrecy, rubber stamps practically every request brought before it. Heinrich also maintained that the FBI "has not made a convincing case that it needs any process other than the one that already exists, especially one that freely allows the FBI access to law-abiding Americans' emails and web activity."

"At this point, it should go without saying that the information the FBI wants to include in the statue [sic] is extremely revealing — URLs, for example, may reveal the content of a website that users have visited, their location, and so on," Andrew Crocker, staff attorney for the Electronic Frontier Foundation, told the *Intercept*.

Crocker further warned of NSLs' "sordid history" of abuse, including "targeting of journalists" and "collect[ing] an essentially unbounded amount of information."

The FBI gained another victory on Thursday when Senate Majority Whip John Cornyn (R-Texas) inserted a similar NSL provision into a bill whose purpose is to require the government to obtain a warrant before forcing technology companies to turn over old e-mails stored "in the cloud."

Under the 1986 Electronic Communications Privacy Act (ECPA), e-mails stored on remote servers for more than 180 days are considered abandoned, allowing authorities to search them at will. The provision might have made sense when the law was written; at that time, few people used e mail, and cloud computing (think Gmail or Outlook) was nonexistent. Now, however, that loophole is being exploited by government agencies to search e-mails that almost certainly have not been abandoned.

The bill before the Senate — a companion version has already passed the House of Representatives — would amend the ECPA to force authorities to get a warrant to search these allegedly abandoned e-mails just as they now have to do to search other e-mails. Adding the Cornyn amendment, along with a variety of other amendments that seem opposed to the law's spirit, might well act as a poison pill to prevent the ECPA from being changed — something that would suit federal agencies such as the FBI just fine.

"If [the provision] is added to ECPA, it'll kill the bill," Gabe Rottman, deputy director of the Center for Democracy and Technology's freedom, security, and technology project, told the *Intercept*. "If it passes independently, it'll create a gaping loophole. Either way, it's a big problem and a massive expansion of government surveillance authority."

The amendments have already delayed the ECPA's passage. The Senate Judiciary Committee postponed consideration of the legislation "to give time to lawmakers to review the amendments and other provisions of the bill that have prompted disagreement," according to Reuters.

In point of fact, only one amendment — the fourth one to the Constitution, which requires authorities to get a warrant before searching and seizing people's "effects" — should carry the day. But since Congress long ago abandoned its fealty to that document in favor of political expediency and deference to the national-security state, it's anybody's guess as to whether this time it will side with the Constitution or allow the FBI to Hoover up Americans' electronic data willy-nilly.