



Trump's Top Cop May Face Privacy, Encryption Speed Bump

Daniel R. Stoller

January 10, 2017

Attorney general nominee Sen. Jeff Sessions' (R-Ala.) well-publicized stances on consumer encryption and e-mail privacy may come under scrutiny during his nomination hearing, analysts told Bloomberg BNA.

Senate Democrats have called for enhanced vetting for President-elect Donald Trump's Cabinet nominations, but the Senate GOP leadership has scheduled the nomination hearing for Sessions to begin Jan. 10. Sessions' opposition to e-mail privacy reform and calls for the tech sector to provide backdoors for law enforcement to access smartphones and other encrypted consumer devices may create a speed bump during the highly-anticipated confirmation hearing. Regardless of questioning on privacy issues, analysts expect Sessions will be confirmed as U.S. Attorney General.

Senate Majority Leader Mitch McConnell (R-Ky.) told reporters after a meeting with Trump Jan. 9 in New York that all Cabinet nominations "will be properly vetted as they have been in the past." McConnell also hopes to have "up to six or seven—particularly the national security team—in place" by Trump's first day in office.

However, don't expect Sessions to have an easy path through the U.S. Senate Committee on the Judiciary, even though he remains friendly with Senate Minority Leader Chuck Schumer (D-N.Y.). Schumer told reporters Jan. 9 that it is worth a slight delay to ensure candidates are properly vetted.

Neema Singh Guliani, legislative counsel at the American Civil Liberties Union told Bloomberg BNA Jan. 9 that Sen. Sessions "should expect to hear from his own party, industry and civil society who feel that he shouldn't turn the clock backward." The Senate Judiciary Committee should "probe into his history and ask the tough questions surrounding privacy, encryption and surveillance," among other important issues, she said.

Julian Sanchez, senior fellow at conservative think-tank Cato Institute in Washington, told Bloomberg BNA Jan. 9 that "Sessions is still a prosecutor at heart." When there is a "policy

conflict between the interests of privacy and data security, he seems to instinctively come down on the side of the government.”

It will be important for the Senate committee to find out how Sessions “sees these issues, because the law is riddled with ambiguities and unanswered questions where the prospective AG’s views will either determine de facto policy—possibly for years—or force certain policy issues to the forefront of debate,” Sanchez said.

Representatives for Sessions and the Senate Judiciary Committee, as well as the Trump transition team, didn’t respond to Bloomberg BNA’s e-mail requests for comment.

Encryption Challenges

Sessions’ stance on the early 2016 battle between Apple Inc. and the Federal Bureau of Investigation over government access to an encrypted iPhone used by one of the shooters in the San Bernardino, Calif. shooting massacre may be a focus of the confirmation hearing.

Laura Jehl, partner at Sheppard, Mullin, Richter and Hampton LLP and co-leader of the firm’s Privacy and Cybersecurity Practice in Washington, told Bloomberg BNA Jan. 9 that the next attorney general will have to tackle a “wide range of matters under the DOJ’s jurisdiction,” including “cyber, privacy and technology issues.” Sessions, if confirmed, will “need to take a stand in the series of long-running debates with Silicon Valley and civil libertarians over encryption and backdoors,” she said.

If confirmed, Sessions will oversee the Department of Justice, which is tasked with defending lawful government surveillance requests. If Sessions had been the head of the DOJ during the Apple-FBI dispute the outcome may have been entirely different, cybersecurity pros said.

Christopher Sanders, founder and chief operating officer of computer consulting company CYGRU, told Bloomberg BNA Jan. 9 that Sessions “has often been at odds with Silicon Valley and privacy advocates on issues that include cooperation with law enforcement investigations.”

Sessions “seems to lean more in favor of expansion of government’s ability to access data for investigative purposes,” Sanders said. Because of this, there may be “tough battles ahead between the law firms of Silicon Valley and the DOJ,” he said.

Sessions previously told Bloomberg News that the tech sector may not see the encryption debate “as a serious issue.” Although Sessions said that access to phones is critical to law enforcement, he’s advocated that the government’s ability to access an encrypted phone shouldn’t be abused.

Sanchez said that Sessions “was probably the most hostile to Apple’s lawyers and the most dismissive of their concerns about the security consequences of enabling government access to encrypted data.” Sessions seems to treat “the most modest civil liberties safeguards” as “frivolous efforts to slander and hamstring law enforcement and intelligence agencies,” he said.

If Sessions holds the line on his encryption stance, he may be going against ranking members of his own party, Guliani said. Both sides of the aisle established an encryption working group that have said “backdoors aren’t a solution” and may increase cybersecurity risks to companies, citizens and the U.S. government, she said.

Government Surveillance

Sessions is a leading advocate for domestic government surveillance at levels not seen since the aftermath of the Sept. 11, 2011 terrorist attacks.

Daniel Schuman, policy director for the privacy advocacy group Demand Progress, previously told Bloomberg BNA that if Sessions is confirmed the U.S.'s "already over-powerful surveillance state" is about to "be let loose on the American people."

For example, Sessions argued that expanded surveillance powers are needed, especially because of the threat of small, deadly terrorist plots that are hard to detect, such as the killing of 49 people at a gay nightclub in Orlando, Fla., and 14 people in San Bernardino, Calif.

Guiliani said that it is imperative that Senate Judiciary Committee members on both sides of the aisle ask questions on "what position he'll take around NSA reform and whether he'll continue Bush-era surveillance programs."

E-Mail Privacy Reform

If Sessions is confirmed he'll have to "take a strong stance on vastly complex cybercrime issues and to consider whether the outdated legal tools (CFAA, SCA and ECPA, among others) at the DOJ's disposal are up to the task," Jehl said.

Sessions has supported legislation to expand the types of internet data the FBI can intercept without warrants and was an opponent to the E-Mail Privacy Act. The act, which ultimately stalled in the Senate, would revamp ECPA by prohibiting government entities from forcing e-mail providers to hand over the contents of user e-mails without a warrant.

Reps. Jared Polis (D-Colo.) and Kevin Yoder (R-Kan.) reintroduced Jan. 9 the E-Mail Privacy Act. As a result of congressional inaction "every American is at risk of having their e-mails warrantlessly searched by government agencies," Polis said. It is unclear whether the bill will have the same fate as its predecessor.

Sanders said that Sessions needs to take "strong stances in protecting the privacy rights of Americans, while balancing the needs for exceptions to ECPA that allows government exceptions when there is" an immediate threat to national security.