Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Restored Privacy Board Lends Crucial Eye To Data Practices

By **Allison Grande**

Law360, New York (May 09, 2013, 9:07 PM ET) -- In finally confirming a long-dormant privacy board's chair Tuesday, the U.S. Senate restored to full strength an oversight mechanism that industry watchers say will change the way both the public and private sectors gather and share information, despite the board's lack of resources and binding authority.

Following a nearly two-year delay, the Senate **in a 53-45 vote** divided along party lines confirmed former WilmerHale partner David Medine to head the Privacy and Civil Liberties Oversight Board, which was last staffed in 2008 and is tasked with providing a check on the government's use and sharing of data for national security purposes.

While the Senate had confirmed the four other part-time members in August, Republicans had blocked the critical appointment of Medine — the only full-time member who has the power to appoint and fix compensation for staff that will enable the board to carry out its functions — because of concerns about his views on national security statues like the Patriot Act.

But with Tuesday's confirmation, the board can begin to use its subpoena powers to obtain elusive information about how the government is using its statutory authority to investigate national security threats since the 9/11 terrorist attacks.

“The PCLOB can now get to full work investigating the rampant secret law of the Obama administration, the government's use of national security letters and many of the other core privacy problems that continue to fester behind closed doors that the administration has been reluctant to open up,” Electronic Frontier Foundation policy analyst and legislative assistant Mark M. Jaycox told Law360 on Thursday.

At a March meeting, the four active members identified three areas of initial interest: 2008 amendments to the Foreign Intelligence Surveillance Act that allow the government to intercept international communications without individual warrants; authority recently given to the National Counterterrorism Center to request and hold large volumes of data on individuals for up to five years; and an order issued in February that charges the board with assessing the government's information-sharing practices for cybersecurity purposes.

“The very existence of many of these national security programs is classified or little is known, so having members of an independent board have the security clearance to look at the privacy and civil liberties issues raised by them and make sure that appropriate safeguards are incorporated is critical,” the Constitution Project's senior counsel Sharon Bradford Franklin, who attended the board's March

meeting, said.

The board's oversight activities are likely to have a significant impact not just on the way that the government uses the troves of data it collects to protect the country from terrorism, but also on how the private sector handles information that is routinely subject to government access requests.

“While [the board] was created to have oversight over the federal government's activities, it's likely that some of the information-access questions it deals with will touch the private sector, such as the debate over what the appropriate standard is for accessing emails from third parties, and it's likely that the body could help guide some of the policy decisions of the administration in this area,” Jenner & Block LLP privacy and information governance practice group chair and former U.S. Department of Homeland Security Chief Privacy Officer Mary Ellen Callahan said.

While privacy professionals who work primarily in the commercial arena may be inclined to pay little attention to PCLOB because of its focus on government surveillance, this approach may be a mistake, according to Daniel Weitzner, director of the Decentralized Information Group at MIT's Computer Science and Artificial Intelligence Laboratory and former White House deputy chief technology officer for Internet policy.

“The new PCLOB is in a unique position to examine the internal and classified activities of NCTC and other intelligence agencies to make sure that they are complying with relevant rules,” Weitzner said in a post on the International Association of Privacy Professionals' blog. “And more likely than not, the PCLOB may discover that existing laws are not quite up to the challenge posed by powerful new data analytic tools.”

A change in the law would not only have an impact on federal agencies, but also on companies that are using similar “big data” practices to discover and link sensitive information about individuals, Weitzner said.

“As the PCLOB comes face-to-face with some of the more challenging questions of how to monitor privacy practices in new Big Data environments, the entire privacy community ought to be paying attention,” he said.

One product of the big data era that could fall under the board's watch is fusion centers, which were jointly created between 2003 and 2007 by the DHS and the U.S. Department of Justice to promote information sharing between federal and local agencies, but they also receive information from some private-sector partners and operate under a cloak of secrecy, according to University of Maryland law professor Danielle Citron.

“We have over 70 fusion centers with access to extraordinary reservoirs of data from the public and private sector, and it's a little like the Wild West,” she said.

The board can also influence the swapping of vast amounts of data between the public and private sectors to protect the country from growing cybersecurity threats.

The executive order President Barack Obama signed in February specifically directs DHS to consult with PCLOB in producing an assessment of the privacy and civil liberties risks of the government's sharing of threat data with the private sector, and legislation being mulled in the U.S. Senate and House of Representatives envisions similar oversight roles for the board, according to Franklin.

“It's even more important for the board to have this oversight role if we do get legislation, [which] presents an even greater risk to individual liberties because it is likely to exempt the sharing of information from the requirements of existing privacy laws in a way that an executive order can't do,” she said.

While Congress strengthened the board in 2007 by making it independent of the White House and giving it subpoena powers, experts noted that issues still remain regarding the authority of the five-member board, which also includes U.S. Chamber of Commerce attorney Rachel Brand, former D.C. Circuit Chief Judge Patricia Wald, WilmerHale counsel Elisebeth Collins Cook and the Center for Democracy & Technology vice president for public policy James Dempsey.

“There are legal constraints on what they can do since they are not an executing body,” Fisher said. “What they can do is make assessments and insist on accountability, but they can't do it all themselves.”

But despite limitations, experts remain optimistic that the new oversight board will be both influential and effective in guarding against privacy and civil liberties abuses committed in the name of counterterrorism.

“Having an oversight board may give more structure and discipline to some of the national security requests for information, and that's a good thing,” Callahan said. “It will push everyone to take a fresh look at what the intelligence community is doing and help to ensure that it is doing the right thing.”

--Editing by Elizabeth Bowen and Chris Yates.