NAAUSA Joins Other Groups Opposing Parts of the Email Protection Act

NAAUSA is participating in the ongoing Congressional debate over modernizing the Electronic Communications Privacy Act (ECPA) and is working to assure that Congress considers legitimate law enforcement and civil enforcement needs in any rebalancing of the law to satisfy privacy expectations.

The current debate in Congress over modernizing the 30-year old ECPA has generated significant interest among lawmakers over how and when government authorities can access email, texts, and other content from electronic communications service providers, when warrants should be required, and how much notice the subscriber of the account should receive. Under current law, unless the service provider discloses content voluntarily, the government, must secure a warrant to gain access to email stored with a service provider that's 180 days old or less. No warrant requirement applies to emails stored for more than 180 days.

Legislation with over 300 cosponsors in the House, the Email Privacy Act, H.R. 699, would change that framework and require the government to secure a warrant to access email regardless how long it's been stored. This change would bring the statute in line with the Sixth Circuit's opinion in *United States v. Warshak,* 631 F.3d 266 (6th Cir. 2010). More important, the legislation also would impose broad, unprecedented notice and disclosure obligations on the government. NAAUSA and other law enforcement groups have raised concerns with Congress over these procedural requirements, and the absence of necessary law enforcement-related exceptions to the statutorily-created warrant requirement. Similar reservations have been expressed by the Department of Justice.

The breadth of bipartisan support for the legislation, offset by the depth of law enforcement concerns about its notice and disclosure obligations, has elevated its attention on Capitol Hill. House Judiciary Committee Chairman Robert Goodlatte (R-VA) sympathizes with those law enforcement concerns and fears the Email Privacy Act, as written, could impede investigations without the addition of exceptions. Goodlatte is not a co-sponsor of the legislation, though more than half of the Judiciary Committee's members are. "Congress can ensure that we are furthering the legitimate needs of law enforcement . . . by joining with the warrant requirement recognized exceptions and procedures," Goodlatte has said.

Given those views, Goodlatte invited NAAUSA President Steve Cook to provide to the Judiciary Committee the front-line AUSA's perspective over how the of the nation's criminal and civil laws would be altered by the Email Privacy Act. In testimony before the House Judiciary Committee on December 1, NAAUSA President Cook pointed to the numerous problems the bill would generate and the way that public safety would be undermined. Cook said:

NAAUSA agrees that imposing a warrant requirement for the government to secure stored email in a criminal investigation is appropriate as a general rule. The Email

Privacy Act, unfortunately, goes much further and in the process creates more problems than it solves First, and most importantly, the Email Privacy Act creates unprecedented and unnecessary barriers to this often lifesaving information—barriers that substantially exceed what would be required to search any other location, including the search of a home. Second, the Email Privacy Act will further complicate an already confusing area of the law by creating internally inconsistent definitions and layering more unfamiliar, unprecedented and unique legal requirements. Third, the Email Privacy Act does nothing to address the antiquated, inappropriate, and confusing provisions of the existing version of the SCA.

Steve Cook's testimony at the hearing, which occurred in a packed hearing room before C-SPAN cameras, played a significant role in raising questions about the Email Privacy Act to the attention of members of the House Judiciary Committee, many who have already cosponsored the legislation. The Email Privacy Act has attracted more cosponsors than any other bill pending in the House of Representatives.

"Mr. Cook's testimony was valuable in educating members of the House Judiciary Committee on the complicated nuances involved in updating the ECPA," said Caroline Lynch, majority staff director of the House Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. "NAAUSA performed a valuable service in explaining the important role that current exceptions to the warrant rule play and the need for their continued recognition in further changes to the statute."

During his appearance, Cook explained how the Email Privacy Act as written fails to recognize the exceptions to the warrant requirement including the emergency aid, exigent circumstances, and consent exceptions. "These exceptions," Cook noted, "are longstanding rules of Fourth Amendment law that have been recognized and applied by the Supreme Court for decades." "By failing to specify these exception for email searches covered by the Act, Congress will be creating an unprecedented and unnecessary barrier to law enforcement access. It is also creating a dangerous barrier—a barrier that will lead to the loss of potentially lifesaving information in cases where time is of the essence. It is well settled that a warrantless search may be conducted of a person's most private place—his or her home—if exigent circumstances exist. There is simply no reason to provide email communications with more protection than that afforded to a person's home …. Put another way, the Email Privacy Act provides *greater* protection to email communications than *any* other item or place. That simply does not make sense. And, it could cripple law enforcement efforts in cases where time is an unavailable luxury."

Rep. Kevin Yoder (R-KA), lead sponsor of the Email Privacy Act, said after the December 1 hearing that the concerns that Steve Cook raised are legitimate ones and should be discussed further. Efforts to rewrite the legislation, however, will be further complicated by additional proposals to add exceptions to the warrant requirement for civil agencies, like the Securities and Exchange Commission.

The SEC has raised concerns about the legislation because it would require the agency to obtain a warrant to access emails directly from a service provider, in contrast to

current authority that permits it to issue subpoenas upon individuals for some material. The SEC does not have the authority to obtain warrants for civil investigations, but desires a change in the law to permit it to obtain stored electronic information directly from services providers, especially when an individual involved has not responded fully to a subpoena. The change is opposed by many lawmakers and service providers, including Google. The issue has distracted attention from the need for the addition of law enforcement exceptions to the warrant requirement.

House Judiciary Chairman Goodlatte said at the December 1 hearing that he plans to take up another bill that would prohibit law enforcement agencies from compelling tech companies to turn over information on foreign customers held in servers overseas and will be holding a hearing on that measure. He did not announce a hearing date, but it is likely sometime early in 2016.