



July 6, 2015

The Honorable Kevin Yoder
Third District, Kansas
United States House of Representatives
214 Cannon House Office Building
Washington, DC 20515

RE: HR 699 – Updating the Electronic Communications Privacy Act (ECPA) and Reducing the Effects of Non-Technical Barriers on Lawful Access of Electronic Evidence

Dear Congressman Yoder:

We, the undersigned organizations representing federal, state and local prosecutors, chiefs, sheriffs, and rank and file officers, understand the intent of HR 699 - the "Email Privacy Act" - is to update the law to ensure that Americans' privacy rights are reinforced in the digital age. While we support efforts to guarantee the privacy rights of all citizens, it is imperative that we ensure that law enforcement, with appropriate judicial supervision and approval, maintain its ability to access and recover digital evidence in order to protect the public and successfully prosecute those guilty of crimes.

Therefore, we ask that any legislation relating to this issue also address the very real challenges that law enforcement faces as it attempts to gather electronic evidence. Failure to address these challenges will result in more missed leads, longer investigative timelines, less safety for Americans and less justice for victims of crime.

The amount of evidence that exists in the digital space is growing explosively. Our society is powered by data that lies at rest and moves across a vast range of devices. Some of that data becomes evidence every time a crime is committed, and this electronic evidence is critical to investigators who need it to generate leads, corroborate stories, identify suspects and conspirators, challenge alibis, exonerate the innocent, and obtain justice for victims of crime.

Evidence takes a variety of forms in the digital space. Evidence can be found in the content of communications and in the data that surrounds communications events. Evidence can be gathered while at rest on devices and in real time while it is in motion across networks. Law enforcement is concerned about anything that creates a barrier to lawfully accessing that evidence. Some of the barriers that degrade our effectiveness are technological, like encryption, and others are non-technological, like elevated legal standards and a lack of responsiveness by private companies who possess electronic evidence.

The attached fact sheet provides an overview of these barriers along with a number of possible solutions that would help ensure that law enforcement maintain access to the critical digital evidence it needs to fulfill its mission. Law enforcement collects much of the electronic evidence it needs by exchanging legal process with service providers like wireless phone companies, internet providers, and

application developers. The logistics of requesting and receiving information from service providers in response to these lawful process demands are antiquated, non-standardized, and often haphazard, causing a very real and under-publicized set of problems. Bringing consistency to the standard of proof that governs law enforcement access to evidence is meaningless if law enforcement cannot obtain the evidence because it hasn't been retained, because the court order is lost after being transmitted, or because the response takes weeks or months to process by the service provider.

To be clear, law enforcement is not asking for new surveillance capabilities above and beyond what is currently authorized by the U.S. Constitution or by lawful court orders, nor are we attempting to access or monitor the digital communications of all citizens. Law enforcement simply needs to be able to lawfully access information that has been duly authorized by a court in the limited circumstances prescribed in specific court orders—information of potentially significant consequence for investigations of serious crimes and terrorism.

We would welcome the opportunity to discuss our concerns and potential solutions to these issues with you at your earliest convenience.

Thank you for your attention to this matter.

Sincerely,

Association of Prosecuting Attorneys (APA)
Association of State Criminal Investigative Agencies (ASCIA)
Federal Law Enforcement Officers Association (FLEOA)
Fraternal Order of Police (FOP)
International Association of Chiefs of Police (IACP)
Major Cities Chiefs Association (MCCA)
Major County Sheriffs' Association (MCSA)
National Association of Assistant United States Attorneys (NAAUSA)
National Association of Police Organizations (NAPO)
National District Attorneys Association (NDAA)
National Fusion Center Association (NFCA)
National Narcotic Officers' Associations' Coalition (NNOAC)
National Sheriffs' Association (NSA)

cc: House Judiciary Committee
Senate Judiciary Committee