FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION

1100 Connecticut Avenue NW ▪ Suite 900 ▪ Washington, DC 20036

Phone: 202-293-1550 ▪ www.fleoa.org

February 13, 2017

Chairman Charles Grassley
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

Ranking Member Diane Feinstein
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

Dear Chairman Grassley and Ranking Member Feinstein:

On behalf of the 26,000 members of the Federal Law Enforcement Officers Association (FLEOA), we are writing to express our collective expertise regarding the Electronic Communications Privacy Act (ECPA) and any proposed changes to this important tool in the law enforcement arsenal.

Experts have said cell phone, texting and email usage has risen over 400 percent within the last decade. The realities are that this is the way people, including criminals, communicate. For criminals, this has become a choice venue to commit crimes.

Since the genesis of electronic communications, its benefits have been used by criminals and terrorists to hide their activities in the cyber world. In many cases, law enforcement isn't alerted to these crimes until days after. As such, it makes tracking these cyber criminals a game of catch up. Making it more difficult for law enforcement to access this information is like barring the doors to the hospital emergency room after a catastrophe.

As a matter of math, it's not a far guess why electronic communications corporations and privacy advocacy groups have lobbied together - they appear to want to reduce the amount of requests law enforcement officers make to access critical electronic information.

Last year, we wrote to both the Senate and House Judiciary Committees about our disappointment with both the content of proposed amendments to ECPA, and the exclusion of federal law enforcement stakeholder input. This year, we request that you utilize stakeholder input and the valuable lessons learned for federal law enforcements for every facet of ECPA.

Our local and state counterparts agree and submitted a letter to the Senate Judiciary Committee (Law Enforcement Perspectives on ECPA Reform – September 18th, 2012), which FLEOA endorses.

Yet from all appearances, it continues to seem that efforts to reform ECPA represent only the interests of the electronic communications industry and privacy

advocate groups. This approach is fraught with unintended consequences as these groups represent narrow interests and don't possess the broader experiences of federal law enforcement or expertise in the tracking and apprehension of criminals and terrorists in the cyber age.

Adding to this, the courts have begun to step-in and clarify ad hoc rules related to ECPA, further muddying the electronic crimes world. A recent three-judge Second Circuit panel opinion, which was upheld by the full appeals court in a 4-4 vote in January, emphasized the location of the data rather than its access point in concluding that the act (ECPA) — which was enacted in 1986 — does not authorize a U.S. court to issue and enforce a warrant against a U.S.-based service provider for the contents of electronic communications stored outside the U.S. Microsoft, the plaintiff in the case, contended in its warrant fight that the customer data being requested by the government was statically stored in Ireland, and that requiring Microsoft to go into the country to retrieve the data would constitute an extraterritorial application of the SCA that was not intended by Congress.

This ruling by the Second Circuit effectively sends a message to data companies and criminals that, if you store your information overseas, you are out of reach of U.S. law enforcement.

Conversely, a U.S. Magistrate Judge in the Eastern District of Pennsylvania, recently ruled in a case brought by Google that warrants issued to Google under the act were legitimate because the invasion of the data owner's privacy interests would not take place outside of the U.S., but rather within the country once the government began looking through the data. This ruling ran head first into the Second Circuit's July decision finding that Microsoft couldn't be forced to turn over user data stored on a server located in Ireland, which Google had argued supported its position that the latest round of government warrants was unlawful.

In the end, due to a lack of clear and updated laws, the courts are now creating the laws. This is problematic and will ultimately lead to different applications and use of ECPA across the judicial system creating a further inability of law enforcement to do its job.

A FLEOA letter previously sent to the Senate Judiciary Committee, stated our opposition to the elimination of the 180-Day Rule. We also opposed the implementation of a three-day notification requirement of suspects who are under investigation. Furthermore, it remains unclear what impact the last proposed Senate ECPA changes would have on law enforcement's use of pen registers, subpoenas and court orders. Our membership is also concerned with the possible impact of ECPA changes on national security letters issued under section 2709, and the lack of responsiveness of providers to lawful requests.

Our position has been clear. In the age of cyber-crimes, our federal law enforcement officers need 21st century tools to combat criminals and keep pace with electronic criminals. Think of it this way, if someone is a victim of identity theft or has their life savings stolen in a data breach that takes seconds, it takes law enforcement upwards of three days to obtain a federal subpoena and up to a week to have a court order or search warrant signed. That already puts law enforcement out seven days from the crime – yet it took just seconds to perpetrate it and delete the evidence.

Yet, previous proposed ECPA reforms seemed miss-guided and more focused on making it more burdensome for law enforcement to obtain electronic information. The proposed reforms had also raised questions as to how it would impact law enforcement's access to other forms of online information, i.e., information provided to third parties such as accountants or online retailers and how to access the data if it is not stored in the U.S. Since the original Senate ECPA amendment did not distinguish between public and private providers, will a grand jury subpoena no longer be a valid legal instrument to obtain an employee's work emails from a corporation?

{}

It is clear that the position of privacy advocates and lobbyists for the electronic communications industry continue to resonate with Congress despite the proliferation of the use of the cyber world to commit crimes. FLEOA asks if anyone queried the federal Inspector General community and the Office of Professional Responsibility to determine if there was a pattern of federal law enforcement abuses of ECPA related statues?

The mission of federal law enforcement officers is: to defeat terrorists, stop money launders, investigate international financial crimes, and thwart drug and weapon traffickers. Investigating all of these crimes entails a varied, expedited and continuous use of ECPA provisions.

We respectfully request that this process include the views of FLEOA, the largest federal law enforcement stakeholder association and an association whose members have a deep expertise with the actual application of the provisions.

We also request that this letter be distributed to the full committee as well, and look forward to working with the committee to ensure federal law enforcement officers have all the tools necessary to combat crime, stop terrorists and keep all Americans safe.

Thank you for considering the perspective of federal law enforcement officers nationwide.

Respectfully,

Nathan R. Catura

Nathan R. Catura
National President FLEOA

CC: U.S. Senate Judiciary Committee Members

{}