ECPA Amendment Adopted Despite Flurry of Law Enforcement Letters

by Greg Nojeim [1]
September 20, 2012

Today, the Senate Judiciary Committee adopted an amendment that would require law enforcement officers to obtain a warrant in order to access the contents of email and other personal and proprietary electronic communications. The warrant-for-content amendment to the Senate version of H.R. 2471 would update the 1986 Electronic Communications Privacy Act (ECPA), which currently extends the warrant requirement only to email 180 days old or less, and does not protect documents stored "in the cloud" by remote computing services. The Committee is expected to take up the bill again when it returns after the November elections.

The vote is particularly significant because it comes in face of a flurry of letters from law enforcement entities [states and locals [2], FLEOA [3], FBIAA [4]] that raised concerns about the warrant-for-content amendment that Judiciary Committee Chairman Patrick Leahy (D-VT) championed and that the companies and privacy organizations who signed this letter [5] supported as well as civil rights organizations [6]. Law enforcement officers do critically important work to fight crime, and electronic evidence is important to their investigations. Their views carry great weight. But, some of the concerns raised in their letters are simply not raised by the legislation.

For example, the Federal Law Enforcement Officers Association speculated that legislation requiring a warrant for content in criminal investigations could effect the standard for pen registers, trap and trace devices, and National Security Letters in intelligence investigations, none of which can even be used to obtain content. Six state and local law enforcement agencies argued that the bill should be amended to give law enforcement the power to "freeze" electronic evidence in place while a warrant for the evidence is sought. But they ignored the provision of ECPA that already gives law enforcement this authority, without meeting any standard and without judicial authorization - 18 USC 2704. We responded to this, and to other concerns raised by state and local law enforcement, in this letter [7].

Understanding the concerns of law enforcement is absolutely critical to advancing the goals of privacy, security, and business innovation. We are committed to continuing to work with law enforcement entities, former law enforcement officials, providers of communication service and congressional staff to understand and address law enforcement concerns as ECPA reform legislation moves forward.

Links:
[1] https://www.cdt.org/personnel/greg-nojeim
[2] https://www.cdt.org/files/file/Law-Enforcement-Letter-ECPA-Reform.pdf
[3] https://www.cdt.org/files/file/Law-Enforcement-Opposition-Section-203.pdf
[4] https://www.cdt.org/files/file/FBI-Letter-ECPA-Reform.pdf
[5] https://www.cdt.org/files/file/Leahy-ECPA-Amendment-Sign-On-Letter.pdf
[6] https://www.cdt.org/files/file/Civil-Rights-Letter-Supporting-ECPA-Reform.pdf
[7] https://www.cdt.org/files/file/CDT-Letter-On-Law-Enforcement-Concerns_0.pdf