KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

September 19, 2012

The Honorable Patrick J. Leahy
Chairman
The Honorable Charles Grassley, Ranking Member
Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Leahy and Senator Grassley:

The Center for Democracy & Technology supports Senator Leahy's amendment to H.R. 2471. It would, among other things, update the Electronic Communications Privacy Act (ECPA) to protect with a warrant requirement the contents of sensitive personal and proprietary communications stored in "the cloud." We commend this effort to help the law keep pace with the huge technological changes that have occurred since ECPA was signed into law in 1986.

I am writing today to respond to questions about the Leahy amendment that state and local law enforcement agencies raised in a September 18, 2012 letter ("law enforcement letter.") Law enforcement officers do critically important work to fight crime and electronic evidence is increasingly important in law enforcement investigations. That is why the Leahy amendment carefully preserves the building blocks of law enforcement investigations – such as subpoenas for customer information and 2703(d) orders for transactional records – the kind of information law enforcement agents use to build probable cause.

(1) The Leahy Amendment Remedies Well-Established Deficiencies in ECPA

The law enforcement letter asks about the problem the Leahy amendment is intended to address, but the problem is well known and has been debated for years. Though the law was forward-looking when enacted in 1986, communications technology has advanced dramatically and ECPA has been outpaced. Today, people store information indefinitely in the Internet cloud that they used to store in their desks. It makes sense to protect both.

In 2010, the Sixth Circuit Court of Appeals determined in *U.S. v. Warshak* that the part of ECPA that allows warrantless law enforcement access to email stored for over 180 days is unconstitutional. The Department of Justice did not appeal the decision and other circuits have not yet ruled definitively on the matter. Many

providers do not know where their users are located but it is reasonable to assume that some users are in the Sixth Circuit and that their communications are protected under this decision. As a result, large providers are already insisting that law enforcement obtain a warrant to access communications content regardless of its age. The Leahy amendment would apply the warrant requirement nationwide, thus reducing the friction between law enforcement and providers that is slowing some responses to law enforcement demands for communications content.

The law enforcement letter suggests that to address the conflicting standards and illogical distinctions that result when the 26-year old ECPA is applied to current technology that the law should be "harmonized" to the lower standards for government access, rather than be "elevated" to probable cause. But the Sixth Circuit Court of Appeals has held that a provision of ECPA allowing the government to obtain the contents of a person's older email without a warrant is unconstitutional. The law cannot be "harmonized" to the weaker standards for content because they are unconstitutional in at least one circuit. Rather, in order for the law to be applied consistently and to avoid jeopardizing law enforcement investigations that may meet legal challenges, Congress should update ECPA to set a clear warrant standard for government access to the contents of private communications held by communication service providers.

ECPA must also be reformed because the current law hampers U.S. competitiveness in cloud computing and risks losing American jobs to foreign competitors of the U.S. cloud industry. Currently, ECPA allows the government to, without a warrant and without timely notice to the customer, compel a cloud provider to produce communications or materials it may hold for the customer. If the customer stored the same information locally, the government would have to either get a warrant or serve a subpoena directly on the target of the investigation, giving the target the opportunity to assert its rights. Because customers are concerned about law enforcement access to their sensitive information, they either are discouraged from using these services altogether, or they may opt to hire cloud computing firms in Europe, which claim that their non-US hosting services provide better protection than their US competitors can.

(2) Law Enforcement Concerns Have Been Aired in Committee

The law enforcement letter suggests that the Senate Judiciary Committee's consideration of changes to ECPA has not included a sufficiently detailed examination of law enforcement interaction with communications service providers. The Committee has been looking at this issue for over two years and it held hearings on ECPA reform on September 22, 2010 and April 6, 2011. The latter hearing was specifically devoted to governmental perspectives. The Department of Justice testified at both hearings. Law enforcement concerns on ECPA reform have been articulated and heard by the Committee.

(3) The Leahy Amendment Would Maintain Existing Emergency Exceptions and Backup Preservation Requirements

The law enforcement letter indicates that sometimes, law enforcement needs immediate access to electronic communications without undue delay, including in child exploitation cases. ECPA already includes emergency exceptions that

allow service providers to disclose to law enforcement the contents of communications and records concerning communications immediately if there is an emergency involving danger of death or serious injury. See 18 USC 2702(b)(8) and 2702(c)(4). And, a service provider is required to turn over any information to the government, regardless of whether there is an emergency, if it is evidence of child pornography, child abuse or child exploitation. See 18 USC 2258A. Nothing in Senator Leahy's ECPA reform proposal would touch those exceptions. There is no need to create new exceptions to account for these crimes because the exceptions are already in the law and will remain there should the Leahy amendment become law.

The law enforcement letter indicates that the government should be able to "freeze" the electronic information it seeks with a warrant to make sure that the information is not destroyed or otherwise purged by the service provider. The law already empowers law enforcement to compel providers to preserve evidence, and they can compel preservation without meeting any criminal standard and without any judicial involvement. Under 18 USC 2704, a service provider can be directed by the government to create a backup copy of the information the government is seeking if the government fears the information will be destroyed or tampered with. Nothing in the Leahy amendment to H.R. 2471 would change this.

(4) Leahy Amendment's Notice Requirement Is Based on Current Law

The law enforcement letter suggests that the requirement that law enforcement give notice to a user within three days of disclosure of content pursuant to a warrant is arbitrary. The three-day period for notice of disclosure pursuant to a warrant is consistent with the three-day period for notice that a user's communications have been preserved at the request of law enforcement. 18 USC 2704(a)(2). In addition, the Leahy substitute and 2704(a)(2) both provide for notice to be delayed under the circumstances set forth in 18 USC 2705.

We would be happy to provide further information upon request.

Sincerely,

Gregory T. Nojeim, Director, Project on Freedom, Security & Technology

cc: Members of the Senate Judiciary Committee