SUMMARY OF THE
ELECTRONIC COMMUNICATIONS PRIVACY ACT AMENDMENTS ACT OF 2013

The Leahy-Lee Electronic Communications Privacy Act Amendments Act *would update the privacy protections for Americans' email and other electronic communications for the digital age. The Electronic Communications Privacy Act (ECPA) is one of the nation's premier digital privacy laws. After three decades, ECPA has become outdated by vast technological advances and changing law enforcement missions since the law's initial enactment. The bill would update this law to improve the privacy protections for electronic communications information that is stored or maintained by third-party service providers. The bill maintains the careful balance that Congress struck when it first enacted the law – to continue to protect and promote consumer privacy interests, law enforcement needs, and American innovation in the digital age.*

SECTION 1 – SHORT TITLE.

This section designates the Act as the *Electronic Communications Privacy Act Amendments Act of 2013*.

SECTION 2 – CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS.

Section 2 amends Title 18, United States Code, Section 2702 (the Electronic Communications Privacy Act or "ECPA") to prohibit an electronic communications or remote computing service provider from voluntarily disclosing the contents of its customers' email or other electronic communications to the government. There are limited exceptions to this prohibition under current law, including customer consent and disclosure to law enforcement to address criminal activity.

SECTION 3 – ELIMINATION OF 180 DAY RULE; SEARCH WARRANT REQUIREMENT FOR CONTENT; REQUIRED DISCLOSURE OF CUSTOMER RECORDS.

Section 3 amends the ECPA so that the disclosure of the content of email and other electronic communications by an electronic communications or remote computing service provider to the government is subject to one clear legal standard -- a search

warrant issued based on a showing of probable cause. The provision eliminates the confusing and outdated "180-day" rule that calls for different legal standards for the government to obtain email content, depending upon the email's age and whether the email has been opened. The provision also requires that the government notify the individual whose account was disclosed, and provide that individual with a copy of the search warrant and other details about the information obtained. Such notice must be provided within ten business days of a law enforcement agency's receipt of the communications, unless the notice is delayed pursuant to Section 4 of the bill.

Section 3 also reaffirms current law to clarify that the government may use an administrative or grand jury subpoena in order to obtain certain kinds of electronic communication records from a service provider, including customer name, address, session time records, length of service information, subscriber number and temporarily assigned network address, and means and source of payment information.

At the request of the Department of Justice and the Federal Trade Commission, Section 3 also contains a provision that adds civil discovery subpoenas to the types of subpoenas that may be used under existing law (administrative subpoena authorized by Federal or State law, Federal or State grand jury subpoena and trial subpoena) to obtain routing and other non-content information from a third-party provider.

Lastly, the section contains a rule of construction regarding government access to internal corporate email that makes clear that nothing in the bill precludes the government from using a subpoena to obtain email and other electronic communications content obtained from an intended recipient or original sender, or to obtain such communications directly from a company when the communications are to or from an officer, agent or employee of a company and the company is acting as an electronic communications service provider for its own internal email system.

SECTION 4 – DELAYED NOTICE.

Section 4 amends section 2705 of the ECPA to provide that the government may seek a court order to delay notifying an individual of the fact that the government has accessed the contents of the individual's electronic communications for up to 180 days if the requesting government entity is a law enforcement agency, and for up to 90 days if the requesting government entity is a civil or administrative enforcement agency. A court may extend the delay periods for a period of up to an additional 180 or 90 days at a time, respectively.

Section 4 also establishes a time limit on the period that the government could preclude a service provider from informing its customer about the disclosure of electronic communications information to the government. If the government entity is a civil or administrative enforcement agency, the applicable time period for preclusion of notice is 90 days. The time period for preclusion may extend up to 180 days if the requesting government entity is a law enforcement agency. These time periods may also be extended by a court for up to an additional 180 or 90 days at a time, respectively.

Lastly, Section 4 requires that service providers notify the government of their intent to inform a customer or subscriber of the fact that the provider has disclosed the individual's electronic communications information to the government at least three business days before the provider gives such notice to the customer or subscriber. The purpose of this provision is to ensure that the government has an opportunity to protect the integrity of its investigation and, if warranted, to ask a court to delay the notification, before such notice is given.

SECTION 5 - RULE OF CONSTRUCTION.

Section 5 provides that the search warrant requirement for electronic communications content contained in Section 3 of the bill does not apply to any other Federal criminal or national security laws, including Title III of the Omnibus Crime Control and Safe Streets Act of 1986 (commonly known as the "Wiretap Act") and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801, *et seq*. (commonly known as "FISA")).