SECTION–BY–SECTION SUMMARY

Sec. 1 – Short Title

The Online Communications and Geolocation Protection Act

Sec. 2 – Warrant Required for Contents of Communications

Warrant standard: This section establishes a clear, consistent warrant standard for government access to wire or electronic communications content – regardless of the age of the content, whether the content is in transit or in the "cloud", or whether the service provider accesses or uses the content in its business operations.

Current law: 18 U.S.C. 2703 requires the government to obtain a warrant to compel service providers to disclose stored communications only in some circumstances, but not in others. As a result, ECPA subjects content (such as an email or digital document) to multiple legal standards during its lifecycle – depending on its age, transit or storage status, and whether the content is opened or unopened. Service providers are prohibited from divulging communications content to the government without the appropriate process.

Notice: This section also requires the government to serve the user or account holder with a copy of the warrant within three days after acquiring the content – but this notice can be delayed under the existing 2705 authorities.

Current law: 18 USC 2703(b) requires government to give prior *notification to the user or account holder when a subpoena is used to access wire or electronic communications held in a remote computing service. This notice can be delayed for up to 90 days under sec. 2705 if a court has reason to believe the notice may result in danger to the safety of an individual, flight from prosecution, intimidation of potential witnesses, or otherwise jeopardizing an investigation or delaying a trial.*

Existing exceptions not modified: To minimize the impact on law enforcement, this section does not modify the exceptions built into current law. For example, the section does not modify exceptions permitting disclosures by service providers to the government in emergency situations. The section does not restrict the authority to access communications readily accessible to the public. The section does not alter foreign intelligence surveillance authorities. The section also does not restrict the ability of authorized recipients of communications (other than the service provider) to voluntarily disclose content to the government without process (i.e., a user with authorized access to shared photos can still voluntarily disclose the photos to the government).

Sec. 3 – Geolocation Information Protection

Geolocation information defined: This section creates a chapter addressing geolocation information in the criminal code. The section defines geolocation information as information that is not content of a communication, concerning the location of a wireless communication or tracking device that can be used to determine or infer the present, prospective, or historical location of the individual.

Current law: Current law does not clearly address government access to location information. Prior to 2005, law enforcement agencies routinely sought court orders to obtain location information based on a certification that such information was "relevant to an ongoing investigation."[1] *In 2005, courts began to split on whether the government's legal theory was appropriate or whether a warrant was required for location information.*[2] *Since 2005, courts have issued widely diverging opinions on the appropriate standard for various types of location information, using different standards depending on the precision of the location information and whether the information was in real time, prospective, or historical.*[3]

Prohibition on government interception of geolocation information, and exceptions: The section makes it unlawful for government to intentionally intercept geolocation information pertaining to an individual, or to disclose or use geolocation information acquired in violation of the chapter. These prohibitions are subject to several exceptions:

1) The government may intercept or compel disclosure of geolocation information pursuant to a warrant.
2) The section permits the government to conduct electronic surveillance under existing Foreign Intelligence Surveillance Act authorities.
3) The section allows government to obtain an individual's geolocation information if the individual provides the government with prior consent.
4) The government may intercept or access geolocation information that is made readily accessible to the general public.
5) Emergency services (including law enforcement officers) may intercept or access an individual's geolocation information in emergency situations.
6) Any investigative or law enforcement officer specially designated by the Attorney General, Deputy Attorney General, Associate Attorney General, or State Attorney

[1] See Department of Justice, *Electronic Surveillance* Manual at 41, 43-45 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

[2] See *In re Application of the United States of America for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. Oct. 14, 2005).

[3] See, e.g., *In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information*, No. 10-MC-987 (NGG), 2011 U.S. Dist. LEXIS 93494 (E.D.N.Y. Aug. 22, 2011); compare with *U.S. v. Skinner*, No. 09-6497, 2012 WL 3289801 (6th Cir. Aug. 14, 2012); compare with *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, No. 08-4227 (3d Cir. Sept. 7, 2010).

General may intercept geolocation if the officer a) reasonably determines an emergency situation exists that involves immediate danger of death or serious physical injury to any person, conspiratorial activities threatening national security, or conspiratorial activities indicating organized crime, b) the geolocation information must be intercepted prior to an order authorizing interception can be obtained, c) there are grounds upon which an order could be obtained to authorize the interception, and d) the officer applies for the order within 48 hours after the interception begins to occur. If the officer fails to obtain a court order or the order is denied, the interception must be terminated and the acquired geolocation information cannot be used as evidence.

Prohibition on disclosure to government by service providers, and exceptions: The section prohibits geolocation service providers from intentionally disclosing to the government geolocation information pertaining to an individual. This prohibition is subject to the above exceptions for government interception, disclosure, and use. In addition, geolocation service providers may provide geolocation information to law enforcement if such information was inadvertently obtained and appears to pertain to the commission of a crime.

Prohibition of use as evidence if violation: The section prohibits geolocation information that has been intercepted, used, or disclosed in violation of the chapter from being received in evidence in any trial, hearing or proceeding, except in a civil action to obtain relief for a violation of this chapter.

Relief for violations: Individuals whose geolocation information was intercepted, disclosed, or intentionally used in violation of the chapter may recover from the person – other than the United States – in a civil action. Remedies included equitable relief, the greater of actual or statutory (the greater of $100 per day of violation or $10,000) damages, and punitive damages as appropriate. It is a defense against civil actions for conduct in violation of the chapter for the defendant to have acted in good faith reliance on a warrant, court order, grand jury subpoena, authorization, law enforcement request, or a good faith determination that an exception permitted the conduct. The civil action may not be initiated later than two years after the date upon which the claimant had a reasonably opportunity to discover the violation. If a court or appropriate agency determines that government employees or officials violated any provision of the chapter, the court or agency must initiate disciplinary proceedings if the circumstances raise serious questions about whether the violation was willful or intentional.

END