ELLEN F. ROSENBLUM
Attorney General

FREDERICK M. BOSS
Deputy Attorney General

DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL

MEMORANDUM

DATE: March 17, 2015

TO: Honorable Floyd Prozanski, Chair
Senate Committee on Judiciary

FROM: Michael Slauson, Special Counsel on Public Safety

SUBJECT: SB 316 – Prohibiting the Disclosure of Service Provider Records

This testimony is presented in opposition to SB 316.

BACKGROUND

The Electronic Communications Privacy Act of 1986 (ECPA), PL 99-508, 100 Stat. 1968, 18 USC § 2510 *et seq*., currently governs the collection of information that is generated, stored, or transmitted by electronic service providers and remote computing services. The Stored Communications Act (SCA), 18 USC §§2701-2712, which is part of the ECPA, limits law enforcement access to the stored records of service providers. Those acts, collectively, generally require the government to issue some process, *e.g.*, a subpoena, court order, or warrant, to obtain information from service providers. Broadly speaking, the more private the information sought by the government, the more burdensome the process required by federal law.

PUBLIC BODIES

SB 316 would prohibit any non-law enforcement public body from obtaining information from service providers. SB 316 requires *any* public body—not just law enforcement— to obtain a criminal search warrant in order to access information from a service provider. But almost all public bodies are prohibited from applying for a criminal search warrant by ORS 133.545(4)("Application for a search warrant may be made only by a district attorney, a police officer or a special agent employed under ORS 131.805). Accordingly, SB 319 would make it impossible for public bodies to obtain information from service providers.

SB 316 precludes access to information from service providers for a non-criminal purpose. Under the ECPA, a governmental entity may obtain basic information about a subscriber, such as the subscriber's name and address, by issuing a subpoena to the service provider. Conversely, SB 316 would require a public body to obtain a search warrant to access the same information. Because a judge may issue a search warrant only upon a finding of probable cause that a crime has been committed, SB 316 would preclude a public body from obtaining records from a service provider for civil violations.

LAW ENFORCEMENT

SB 316 requires information unavailable to law enforcement at the onset of a criminal investigation. In any investigation, whether civil or criminal, identifying the target of the investigation is usually the first step. In computer-related cases, obtaining records from a service provider is often the only way to learn a defendant's identity or location. SB 316 requires a search warrant in order to obtain even basic identifying information about a subscriber, including identity. Requiring law enforcement to obtain a search warrant before identifying the target of an investigation imposes an impossible burden that will stop many investigations before they start.

SB 316 adopts an unreasonable, one-size-fits-all methodology. As noted, federal law employs a tiered approach to privacy which weighs the scope of the intrusion against the showing of necessity required to access it. This is consistent with the approach taken by the judiciary in weighing these competing interests. SB 316 abandons this approach by requiring a warrant regardless of the nature of the underlying privacy interests.

The notice and reporting provisions in SB 316 are unworkable. SB 316 requires a public body that obtains records from a service provider to provide notice to the subscriber. The notice provisions contained in SB 316 are onerous, impose unrealistic deadlines, and would unduly impair law enforcement's ability to effectively process cases. Requiring notice to a defendant within 3 days presupposes that a defendant's identity is known, and will in many cases require petitions to the court for an extension of notice to avoid providing a defendant with a blueprint of the evidence against them prior to indictment.

SB 316 requires the exclusion of evidence for technical, non-privacy related violations. For example, even a technical violation of the legislative reporting requirement would require suppression. Given the complexity of the notice and procedure required by this proposal, the exclusion of otherwise relevant information should be expected.

SB 316 eliminates the requirement of standing. Under the federal and state constitution, only the person whose rights have been violated has a basis to object to the admission of unlawfully obtained evidence. SB 316 eliminates that requirement as it applies for these records and instead allows any litigant to challenge the admission of evidence regardless of whether the litigant had any privacy interest in the evidence (*e.g.*, a defendant could object to the admission of a victim's telephone records).

Contact: Aaron Knott, Legislative Director, 503-798-0987 or aaron.d.knott@doj.state.or.us