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 640 – Prohibiting the Disclosure of Service Provider Records

This testimony is presented in opposition to SB 640.

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. Basically speaking, the more private the information sought by the government, the more burdensome the process required by federal law.

IMPACT OF SB 640

SB 640 would prohibit any non-law enforcement public body from obtaining information from service providers. SB 640 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 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). As a result, SB 640 would make it impossible for public bodies to obtain information from service providers beyond a subscriber's name and address.

SB 640 would hamper civil investigations. SB 640 sets the bar for obtaining a search warrant in civil cases much too high. That standard—probable cause of a civil violation—is akin to the burden to prove an entire civil case, which is by a preponderance of the evidence. Practically speaking, an agency, county or municipality would not be able to engage in pre-litigation investigation of third party communications unless already in possession of enough evidence to prove their case, in which case the evidence would generally be unnecessary.

SB 640 would prohibit any public body from obtaining phone numbers and IP addresses without a warrant. Given the broad definition of "location information," state agencies would be prohibited from utilizing such mundane tools as caller ID. Moreover, as an example in the criminal context, the Internet Crimes Against Children task force would no longer be able to process cybertips—which it is required to do under its federal grant—because the tips rely on IP addresses to identify suspects involved in child pornography. To be sure, most Internet-based investigations begin with identifying an IP address, which would be prohibited without a search warrant under this bill. SB 640 will substantially impair multiple types of investigation, including of internet based child-pornography.

SB 640 is inconsistent with federal law. SB 640 imposes obligations that are not found in federal law. For example, under the SCA, a governmental agency may obtain a person's phone records from a service provider with a lawfully issued subpoena. Obtaining the same information under SB 640 requires a search warrant.

The notice and reporting provisions in SB 640 are unworkable. SB 640 requires a public body that obtains records from a service provider to provide notice to the subscriber. The notice provisions contained in SB 640 are onerous, impose unrealistic deadlines, and would unduly impair law enforcement's ability to effectively process cases. Requiring notice to a defendant within 7 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 640 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 640 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 640 eliminates that requirement 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