

Short Summary Of HB 444

This Act would

- Require the government to get a warrant to force service providers to disclose wire or electronic communications content, such as emails and voicemails;
- Require the government to serve notice on users when the government forces service providers to disclose their users' content;
- Permit courts to authorize the government to delay notice under narrow circumstances;
- Create a suppression remedy for evidence obtained in violation of the Act;
- Authorize the state AG to seek injunctions and file for civil actions to compel government compliance with the Act;
- Make clear that the Act does not alter any state subpoena power over corporate records;
- Provide standing to providers seeking to challenge processes that are inconsistent with the Act;
- Bar a cause of action against providers for giving information or assistance in accordance with the terms of the Act; and
- Make clear that the Act does not prohibit voluntary disclosure by providers where the law does not otherwise disclosure the disclosure, such as for emergencies or when the provider obtains user consent.

Section-By-Section Summary Of HB444

Section 1 – Definitions

- “Contents” means any information concerning the substance or meaning of a communication.

[Note: The bill’s definition matches the current federal definition of “contents.”¹
1 18 U.S.C. 2510(8).

- “Electronic communication” includes any aural transfer or transfer of data, writing, images, or sounds transmitted by radio, wire, or electric means.

[Note: The bill’s definition includes the content of virtually all online communications, such as emails, social networking messages, files stored with cloud services, and voicemails. The bill’s definition matches the current federal definitions of “electronic communication” and “wire communication.”²]

- “Electronic communication service” includes services that provide users the ability to send and receive electronic communications, services that provide users computer storage or processing services, or services that act as intermediaries in the transmission of electronic communications.

[Note: The bill’s definition encompasses the current federal definitions of “electronic communication service” and “remote computing service,” covering virtually all third parties that store information online for users.³]

Section 2 – Search warrant required.

- Governmental entities must get a warrant to force an electronic communications service provider to disclose the contents of an electronic communication.

[Note: Under current federal law, the government can compel providers to turn over digital content, such as an email message, that is more than 180 days old without a warrant. The federal government also argues that it can obtain email messages that are less than 180 days old, but that have been opened or read, without a warrant.⁴ Instead, the government can obtain this information with a subpoena or a court order based on “specific and articulable facts” (and notice to the user).⁵ This bill would apply a simple warrant protection rule for content, regardless of age or whether the content is opened or unopened.]

Section 3 – Notice, delayed notice.

- Governmental entities that force an electronic communications service provider to disclose the electronic communication content must give notice to the user or customer. The notice must be served no later than when the government receives the contents of the electronic communication. The notice must include a copy of the warrant and a description of the information obtained from the provider.

[Note: Under current federal law, the government must provide prior notice to users if the government obtains digital content with a subpoena or a court order, but current federal law does not require notice if the government obtains a warrant. This bill would require the government to provide notice to users if the government obtains the content with a warrant.]

- Governmental entities seeking electronic communication content pursuant to a warrant may request that the court grant a delay of the required notice to the user or customer. The court must grant the government’s request for delayed notification if it has reason to believe the notification may, among other things, endanger the life or safety of an individual, seriously jeopardize an investigation, or result in the destruction or tampering of evidence. The court order to delay notice can forbid any other person from revealing the existence of the warrant. The delay can last up to 90 days, and the government can request extensions of the delay of up to 90 days each. Once the delay expires, the government must provide notification to the user or customer.

[Note: Similar provisions of federal law allow the government to request that courts delay the required notice to users when the government obtains digital content without a warrant, and to request extensions of the delay.⁶ This bill would allow the government to request that courts delay the required notice when the government obtains content with a warrant.]

Section 4 – Rules of construction.

- With the exception of the delayed notice provision, nothing in this bill would be construed to limit any party from discussing a government request for electronic communication information.
- This bill would not limit any authority of the government to use a subpoena to obtain electronic communication content about an entity’s employees, officers, or agents that are stored or maintained on the entity’s own electronic communications service.

This provision is intended to preserve the government’s existing authority to obtain a company’s business records on the company’s own electronic communication system.⁷ For example, this would prevent a company from putting records related to the duties of its own employees on its own email system and then claiming that the government needs a warrant to obtain the records, which could hamper an investigation into corporate malfeasance.

Section 5 – Admissibility of proof, violations.

- Evidence obtained in violation of this Act is not admissible in state court.

[Note: Current federal law does not include a suppression remedy.⁸ Under federal law, if the government illegally obtains email messages, that evidence could still be admitted in a criminal trial. This bill ensures that illegally obtained digital content cannot be admitted as evidence.]

- The state Attorney General may use injunctions and civil actions against government entities to compel compliance with the law.

Section 6 – Standing to challenge.

- Electronic communications service providers may challenge government demands for data in state court on behalf of their users.

Section 7 – No Cause Of Action Against Providers.

- Electronic communications service providers are not liable in state court for providing information or assistance to the government in accordance with the terms of this Act.

[Note: This provision matches the provider liability protection in current federal law.⁹]

Section 8 – Voluntary disclosure of electronic communications.

- Electronic communications service providers may voluntarily disclose electronic communications content to the government when otherwise not prohibited by law.

[Note: Federal law prohibits service providers from voluntarily disclosing their users' digital content to the government in most circumstances.¹⁰ However, federal law contains exceptions to this general prohibition. For example: Providers may disclose content to the government in emergencies, with the consent of the user, or to NCMEC in connection with child pornography cases.¹¹ This bill preserves those exceptions as they currently exist in federal law.]

¹ 18 U.S.C. 2510(8).

² 18 U.S.C. 2510(12) and 2510(1), respectively.

³ 18 U.S.C. 2510(15) and 2711(2), respectively.

⁴ See "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," Office of Legal Education, U.S. Dept. of Justice, pg. 138, available at <http://justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf#page=150> (accessed Jan. 6, 2015.)

⁵ 18 U.S.C. 2703(a)-(d).

⁶ 18 U.S.C. 2705.

⁷ The bill's provision matches language proposed in Section 3(a)(2) of Senator Patrick Leahy's Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong., available at www.gpo.gov/fdsys/pkg/BILLS-113s607rs/pdf/BILLS-113s607rs.pdf#page=5 (last accessed Jan. 6, 2015).

⁸ See "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," Office of Legal Education, U.S. Dept. of Justice, pg. 147, available at www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf#page=159 (accessed Jan. 6, 2015.)

⁹ 18 U.S.C. 2703(e).

¹⁰ 18 USC 2702(a).

¹¹ 18 U.S.C. 2702(c).