March 20, 2017

Governor Steve Bullock
Office of the Governor
PO Box 200801
Helena, MT 59620-0801

RE: Veto Request - HB 148 (Zolnikov): Electronic communications

Dear Governor Bullock:

The Center for Democracy & Technology (CDT) and Electronic Frontier Foundation (EFF) respectfully requests an **AMENDATORY VETO** of **HB 148 (Zolnikov)** to address the concerns stated below. CDT is a nonpartisan, nonprofit technology policy advocacy organization dedicated to protecting civil liberties and human rights, including privacy, free speech and access to information. EFF is a member-supported non-profit civil liberties organization that works to protect free speech and privacy in the digital world. We are experts in the Electronic Communications Privacy Act, the federal analogue to HB 148, and have long argued for its modernization.[1]

While we applaud the underlying purpose of the bill – to secure the content of communications held by third parties – key provisions of the bill undercut that goal, harming the privacy of internet users, both at home and abroad, and may suffer from serious constitutional infirmity.

As an initial matter, section 2 of the bill (authorizing the use of investigative subpoenas to gather the contents of communications from an electronic communication service) risks violating the Fourth Amendment to the U.S. Constitution as interpreted by at least one federal appellate court. In 2010, in *U.S. v. Warshak*, the Sixth Circuit ruled that people have a reasonable expectation of privacy in email content and that it should only be accessed with a search warrant.[2]

While the *Warshak* decision is technically only applicable in the Sixth Circuit, the difficulty in determining where a particular user was located and the persuasiveness of the court's reasoning has

---

[1] *Reforming the Electronic Communications Privacy Act: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. (2015) (Calabrese testimony); *H.R. 699, the "Email Privacy Act.": Hearing before the H. Comm. on the Judiciary*, 114th Cong. (2015) (Calabrese testimony).
[2] *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

led most, if not all, major technology companies to adopt a warrant standard for all stored content. As such the inclusion of a provision allowing access to the contents of communication with an investigative subpoena could be a step backward for the privacy rights of Montana citizens. While Montana law has a very strong subpoena requirement which requires a probable cause determination for "constitutionally protected material," the bill does not require the content of communication be treated as per se constitutionally protected.[3] We request that the provision authorizing the use of an investigative subpoena be stricken or the legislation be amended to make clear that all contents of communication held by 3rd parties be deemed constitutionally protected.

Next, while the requirement of the section to notify users is laudatory, section 3 of the legislation may also ultimately be struck down on different constitutional grounds: it allows the government to seek to bar a provider from notifying its users of a government investigation in violation of that provider's First Amendment rights.

A similar provision is currently being challenged on First Amendment grounds in *Microsoft vs. The Department of Justice* and recently survived a motion to dismiss.[4] Given that the provision in section 3 closely mirrors that of 18 USC 2705 (the provision at stake in the federal suit), it is likely that if federal law is invalidated, section 3 would be as well. Further, it's noteworthy that section 3 is actually weaker than existing federal law. Federal law requires that a request for delayed notice be granted if notification of the existence of an order "will" result in one of 5 enumerated harms.[5] Section 3 grants a delay of notice when the order "may" cause such harms.

Finally, another provision of section 3 may create a dangerous precedent for the privacy of Americans. Specifically, section 3(3)(B) requires providers to produce the contents of communications regardless of where they are held. Such a requirement would mean providers would have to disclose information on users no matter where in the world they reside or their citizenship. A comparable rule in by a foreign country such as Russia or China would mean those nations would be able to compel information on any individual as well, including those in the United States. Such a result is at odds with both Americans' privacy expectations and international rights.

For all of these reasons we respectfully request your **AMENDATORY VETO** of **HB 148** to remove these problematic provisions. We'd be happy to answer any questions about this letter or the federal

---

[3] Mont. Code Ann. § 46-4-301.

[4] For more information on the case see: https://cdt.org/press/ruling-in-microsofts-challenge-to-gag-order-a-win-for-transparency/

[5] 18 USC 2705(b).

Electronic Communications Privacy Act. The best point of contact is Chris Calabrese, Vice President for Policy at CDT who can be reached at CCalabrese@cdt.org or (202) 407-8824.

Sincerely,

Center for Democracy & Technology
Electronic Frontier Foundation