KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

July 30, 2014

Chairman Fred Upton
Ranking Member Henry A. Waxman
House Committee on Energy and Commerce
Rayburn House Office Building Room 2124
Washington, DC 20515

Re: Kelsey Smith Act, H.R. 1575

Dear Chairman Upton and Ranking Member Waxman:

We are writing to signal our opposition to the Kelsey Smith Act, H.R. 1575, as it would be amended by the amendment in the substitute that the Energy and Commerce Committee ("Committee") is expected to adopt at today's markup of the bill. The bill would require telecommunications companies to disclose information about the location of their users whenever law enforcement officers believe there is an emergency even if the provider has determined there is no emergency and the user has not consented to the disclosure. There have been no hearings on the legislation; it was noticed for markup only three business days ago. While we appreciate the efforts of staff to address concerns about the legislation, we remain concerned that if adopted, the bill as amended will result in disclosure of user location information in non-emergency situations to the detriment of user privacy.

The bill provides a sweeping exception to the rule in current law that law enforcement can compel disclosure of user location information only with a prior court order. It appears to apply both to stored location information and to information about the location of a user at the moment the demand is made, and would also apparently permit mass disclosure of location information pertaining to many users. It provides no remedy to the user whose location information is disclosed as a result of an improper demand for such information.

As amended, the bill would add a new Section 222A to the Telecommunications Act of 1934 that would, "require a provider of covered services to provide call location information concerning the telecommunications device of a user of such service" to any investigative or law enforcement officer – whether from a state, local or federal agency – who demands it. The demand must be accompanied by a sworn written statement establishing the officer's probable cause to believe that disclosure without delay is required by an emergency involving risk of death or serious physical injury or in order to respond to the user's call for emergency services. Within 48 hours of making the demand, the law enforcement agency must "request a court order stating whether such officer had probable cause to believe" that the emergency conditions existed at the time of the demand. The disclosure can be compelled both in connection with the investigation of a crime or in non-criminal situations, such as in the case of a missing person when there is no evidence of foul play. Providers who make disclosures pursuant to new

Section 222A would be protected against all liability for doing so.

Current law permits providers covered by this bill to disclose *voluntarily* a user's location information when the user has consented to such disclosure, or when the provider is persuaded by law enforcement (or by any other person, for that matter, or even on its own volition) that the emergency conditions described in the bill pertain. 18 U.S.C. 2702. Consequently, the bill will operate generally when there is no consent and the provider disagrees with law enforcement about whether there is an emergency.

Tens of thousands of emergency disclosures of user information are made every year under the emergency provision in current law. Some disclosures pertain to location information and some to other types of information, including communications content. According to their transparency reports, two major providers, AT&T and Verizon, made emergency disclosures under this provision almost 70,000 times in 2013 alone. This is an astounding number. Yet, to our knowledge, the Committee has engaged in no fact finding to determine the extent to which these disclosures are being made in circumstances that are not true emergencies, or, conversely, that providers have frequently failed to make disclosures in true emergencies. It has engaged in no fact finding to determine whether providers that now make prompt, voluntary emergency disclosures would, if the bill became law, demand that law enforcement produce the affidavit called for in the bill to compel a disclosure, thus slowing a disclosure that would have otherwise been made promptly. We respectfully submit that such fact-finding should be a pre-requisite to consideration of legislation to compel emergency disclosures.

Removing from providers discretion about whether an emergency disclosure of user information is warranted increases the risk that user information will be disclosed in non-emergency situations. While the bill requires a subsequent court order based on a finding of probable cause that there was an emergency, it imposes no consequences for failure to obtain such order. The bill gives no suppression remedy to a defendant convicted on the basis of location information disclosed under the bill and it gives the user whose location information is improperly disclosed no civil remedy against a law enforcement agency that fails to obtain the court order provided for in the bill. While we favor the court order requirement and suggest that it be strengthened by providing for such redress, we would be remiss if we did not caution the Committee that the court order requirement may rest on shaky ground: courts may dismiss requests for the probable cause findings contemplated in the bill because they may find there is no "case or controversy" at issue that gives them jurisdiction. We would suggest further inquiry is necessary to determine whether the court order requirement will be an effective deterrent to abusive demands for emergency disclosure of location information in non-emergency situations.

Finally, we are concerned about the scope of the emergency exception. It would appear to cover "tower dumps" – a demand by law enforcement for emergency disclosure of the location of all of a provider's users who are proximate to the scene of a claimed emergency. The bill makes no provision for what happens to the thousands of records user location information after it is disclosed to law enforcement in such circumstances. Furthermore, the bill includes no requirement that the user location information disclosed to law enforcement includes only the information relating to the claimed emergency.

The location information covered by the bill can be very revealing. The Eleventh Circuit court of appeals has already found that it is covered by the Fourth amendment when disclosed from storage or when disclosed in response to a one-time "ping" from law enforcement. *United States v. Davis* – No. 12-12928 – D.C. Docket No. 1:10-cr-20896-JAL-2 (11th Cir., June 11,

2014), *available at* https://www.aclu.org/sites/default/files/assets/q_davis_opinion.pdf. Accordingly, we urge the Committee to reconsider this legislation and conduct a hearing first to determine whether it is needed and if so, what additional safeguards should be added.

Sincerely,

Gregory T. Nojeim, Director of the Project on Freedom, Security & Technology

cc: Members of the Committee and members of the House Judiciary Committee