WASHINGTON
LEGISLATIVE OFFICE

July 29, 2014

Chairman Fred Upton
Ranking Member Henry A. Waxman
House Committee on Energy and Commerce
Rayburn House Office Building
Room 2125
Washington, DC 20515

Re: H.R. 1575, Kelsey Smith Act, as amended

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

LAURA W. MURPHY
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

Dear Chairman Upton and Ranking Member Waxman:

The American Civil Liberties Union writes today to express our continuing concern regarding H.R. 1575, Kelsey Smith Act, as amended. We appreciate the committee's willingness to address issues affecting personal privacy in the legislation, but two crucial issues remain unresolved: the definition of 'emergency' and an individual's remedy when information on his or her location is collected in violation of the law. In order to protect personal privacy, and before we take a formal position on the legislation, we urge you to work with other relevant committees of jurisdiction to ensure that both issues are addressed before H.R. 1575 receives consideration before the full House of Representatives.[1]

- **Remedy for law enforcement abuse of emergency designation**

H.R. 1575, in its current form, requires certain telecommunications carriers to provide location information to law enforcement any time "disclosure without delay is required by an emergency involving the risk of death of serious physical injury." This disclosure would be mandatory on the part of the provider and the provider in turn would be indemnified against any lawsuit stemming from the sharing of this information as long as it operates in good faith. While the objectives of this legislation are laudable – to assure speedy access to location information in the case of emergencies – there are already effective and timely mechanisms in place to share location information. The danger is that this legislation would not improve

[1]For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. With more than a million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

on those mechanisms, but instead simply expand the number of wrongful disclosures in non-emergency circumstances.

Under current law, providers of electronic communications are required to keep the records and personal information of users confidential from the general public and the government.[2] Given the technical realities of modern communications, this protection is critical. Cell phones are capable of tracking each American's movements continuously and for an extended duration. As such, location information is some of the most revealing information possessed by carriers. As Justice Sonya Sotomayor said in her concurrence in a recent Supreme Court decision regarding location tracking, *U.S. v. Jones*:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. … Disclosed in [GPS] data ... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on. … The Government can store such records and efficiently mine them for information years into the future.[3]

However Congress has also recognized that there are times when, consistent with the idea of exigency in the Fourth Amendment, providers must breach this confidentiality and share information, including location information, with the government. As such, an existing federal statute already allows disclosure by a provider "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency."[4]

This current process works. According to the transparency reports of two major providers, Verizon and AT&T, they supplied emergency information (unrelated to 911 calls) almost 70,000 times just in 2013.[5] However not all emergency requests meet the existing standard for emergencies. In fact, according to reporting by Google, approximately 20% of the emergency requests they received in 2013 were rejected because they did not meet this standard.[6] This demonstrates the critical role that permissive disclosure plays in the process of responding to emergencies. If providers must turn over records once law enforcement characterizes them as an

---

[2] 18 U.S.C. 2701 et. seq.

[3] U.S. v Jones, 132 S.Ct. 945, 955-956.

[4] 18 U.S.C. 2702 (c)(4).

[5] 2014 Verizon Transparency Report, available at : http://transparency.verizon.com/us-report; 2014 AT&T Transparency Report available at: http://about.att.com/content/dam/csr/transpreport/ATT_Transparency%20Report.pdf

[6] 2014 Google Transparency Report available at: http://www.google.com/transparencyreport/userdatarequests/US/

emergency, there is a very real danger of significant oversharing stemming from law enforcement's incorrect use of the emergency exception.

We appreciate efforts to address this concern in H.R. 1575, as amended, by creating an after the fact court review of whether the criteria for an emergency have been meet. The amended proposal now requires a sworn written statement memorializing the facts that led police to characterize it as an emergency. It also creates an after the fact judicial review of whether this standard has been met. This could be a crucial check preventing police from labeling every situation an emergency, either through poor training or bad faith.

Unfortunately as currently drafted, this after the fact court review suffers from two infirmities – one major and one minor. The more significant problem is that the legislation as drafted does not create any penalty if the court finds a violation of the law. There is no penalty for police misconduct, nor is there any remedy allowing a criminal or civil defendant to suppress evidence gathered from this illegal data collection. The result is that a defendant could be harmed by clearly illegal conduct, but have no remedy – a gross injustice and at odds with criminal procedural remedies in other contexts.

The secondary issue is that the standard under H.R. 1575, as amended, for any court proceeding is whether the conditions for an emergency existed at the time of the request. That standard allows after the fact justifications based on facts not in evidence at the time of the application. Instead, the court should judge the appropriateness of the application based on the facts from the sworn written statement and suppress any evidence gathered when that statement does not meet the standard.

- **Emergency designation must be clarified and narrowed**

The final major problem with H.R. 1575, as amended, is that the definition of emergency is too expansive. Under the bill in its current form, a provider must share location information when the officer has "probable cause to believe that disclosure without delay is required by an emergency involving risk of death or serious physical injury." However under existing statute, sharing can occur only in relation to "an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information *relating to the emergency*."[7] (emphasis added). In other words under existing law there must be a connection between the emergency and the records being sought.

Under the bill in its current form, information would be could be shared any time there is an emergency. For example, it could become common practice in response to a bomb threat to an office building for police to seek records on everyone in that building. Police might believe such a large data dump is required by an emergency, but without an expectation that the location of all those individuals was in any way directly related to the risk of death or serious physical injury. The practical result

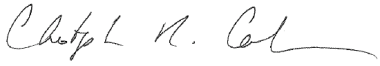
[7] 18 U.S.C. 2702 (c)(4).

would be that large amounts of unrelated location information could be revealed in response to any perceived emergency. Instead the proposed legislation should be amended to track the existing emergency framework delineated in 18 U.S.C. 2702 (c)(4).

The ACLU appreciates the work the Committee has done to improve H.R. 1575. As a final matter, we believe both issues would also likely benefit from the informed participation of the other relevant committee of jurisdiction, the House Judiciary Committee, with which we urge the members of the committee to consult.

We encourage the committee to protect personal privacy by addressing these two issues – definition of emergency and an individual remedy –before the bill receives consideration by the full House of Representatives. If you need additional information please do not hesitate to contact Chris Calabrese at ccalabrese@aclu.org.

Sincerely



Laura W. Murphy
Director, Washington Legislative Office

Christopher R. Calabrese
Legislative Counsel

Cc: Members, House Energy and Commerce Committee