epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

☎ +1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

March 16, 2017

The Honorable Robert Latta, Chairman
The Honorable Janice Schakowsky, Ranking Member
U.S. House Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection
2125 Rayburn House Office Building
Washington, DC 20515

RE: Hearing on "Disrupter Series: Smart Communities"

Dear Chairman Latta and Ranking Member Schakowsky:

We write to you regarding the upcoming Disrupter Series hearing on "Smart Communities" that will be held on March 16, 2017. The implications of Internet of Things ("IoT") for consumer privacy and security are far-reaching. EPIC urges the Committee to consider the substantial privacy and security implications that come with the increased use of connected and "smart" devices. Specifically, core considerations in the development of smart communities should be prioritizing cybersecurity, protecting individual privacy, and minimizing data collection and sharing.

The Electronic Privacy Information Center was established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC is a leading advocate for consumer privacy and has appeared before this Committee on several occasions, and has actively participated in the proceedings of the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC").[1] EPIC has considerable expertise in the Internet of Things. EPIC has testified before Congress on "the Internet of Cars" and Smart Grid.[2]

[1] *See, e.g,* Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. House Energy & Commerce Subcommittee on Communications and Technology, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows* (November 13, 2015), https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf; Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. House Energy & Commerce Subcommittee on Communications and Technology, *Communications Networks and Consumer Privacy: Recent Developments* (April 23, 2009), https://epic.org/privacy/dpi/rotenberg_HouseCom_4-09.pdf; Letter from EPIC to the U.S. House Committee on Energy and Commerce on FCC Privacy Rules (June 13, 2016), https://epic.org/privacy/consumer/EPIC-FCC-Privacy-Rules.pdf; Letter from EPIC to the U.S. Senate Committee on Commerce, Science, and Transportation on FTC Oversight (Sept. 26, 2016), https://epic.org/privacy/consumer/EPIC-Letter-Sen-Comm-CST-FTC-Oversight.pdf.

[2] EPIC Associate Director Khaliah Barnes, Testimony Before the U.S. House of Representatives, Committee on Oversight and Government Reform, Subcommittees on Information Technology and Transportation and Public Assets, *The Internet of Cars.* Nov. 18, 2015, https://epic.org/privacy/edrs/EPIC- Connected-Cars-Testimony- Nov-18-2015.pdf; EPIC Associate Director Lillie Coney, Testimony Before the U.S. House of Representatives Committee on Science and Technology, Subcommittee on Technology and Innovation, *Smart Grid Architecture and Standards:*

The need for strong cybersecurity measure in cities is already evident. Shortly before the 2017 Presidential Inauguration, the Washington Metropolitan Police Department's closed-circuit television cameras were hacked and unable to record for three days.[4] In November, hackers infiltrated San Francisco's public transportation system and threatened to release customer and employee data unless a ransom was paid.[5] Hackers have also targeted police departments across the country by breaching their computer systems, holding files for ransom, and deleting files when they are not paid.[6]

A recent DHS report found that cybersecurity was a top concern in both the public and private sector.[7] That same report also noted that most states acknowledged their lack of understanding of cybersecurity practices.[8] For smart communities to be successful they will need to have support from state governments – and those governments will need to have a strong understanding of how to keep their communities secure from cyber threats. The potential benefits of smart cities will not be achieved if the systems are insecure and cities are subject to hacks that threaten public safety.

Protecting individual privacy must also be a priority in the development of smart communities. As these communities develop, special care must be taken to safeguard data generated by private individuals. For example, several cities have already entered into data disclosure agreements with popular traffic apps that rely on self-reporting.[9] Communities must be transparent with the public about how the data they receive is used and ensure that consumer data is protected.

Transparency is also essential. The public has a right to know if data will be used to determine changes in how first responders operate, especially law enforcement. An increased police presence could lead to the impression that some communities are being treated differently than others and that some individuals are viewed differently because of where they live or who

Assessing Coordination and Progress, https://epic.org/privacy/smartgrid/Smart_Grid_Testimony_2010-07-01.pdf.

[4] Clarence Williams, *Hackers Hit D.C. Police Closed-Circuit Camera Network, City Officials Disclose,* Washington Post, Jan. 27, 2017, https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html.

[5] Robert Hackett, *Hackers Threaten to Release 30GB of Stolen Data From San Francisco's Municipal Railway,* Fortune, Nov. 28, 2016, http://fortune.com/2016/11/28/muni-hack-san-francisco/.

[6] Chris Francescani, *Ransomware Hackers Blackmail U.S. Police Departments,* CNBC, Apr. 26, 2016, http://www.cnbc.com/2016/04/26/ransomware-hackers-blackmail-us-police-departments.html.

[7] *National Preparedness Report,* DHS, Mar. 30, 2016, https://www.fema.gov/media-library-data/1476817353589-987d6a58e2eb124ac6b19ef1f7c9a77d/2016NPR_508c_052716_1600_alla.pdf.

[8] *Id.*

[9] Parmy Olson, *Why Google's Waze Is Trading User Data With Local Governments,* Forbes, Jul. 7, 2014, https://www.forbes.com/sites/parmyolson/2014/07/07/why-google-waze-helps-local-governments-track-its-users/; Nick Stockton, *Boston Is Partnering With Waze To Make Its Roads Less Of A Nightmare,* Wired, Feb. 20, 2015, https://www.wired.com/2015/02/boston-partnering-waze-make-roads- less-nightmare/.

they know.[10] Predictive policing tools are already in use throughout the criminal justice system, although little is known about how these tools, which rely on social and personal information, operate. EPIC has filed a Freedom of Information Act suit to obtain documents related to the use of "risk assessment" tools in the criminal justice system.[11] We urge the Committee to question what role, if any, these tools will have in law enforcement and criminal justice in smart communities.

Finally, we would urge the Committee to stress that data collection must be minimized in the development of smart communities. Smart communities should promote Privacy Enhancing Techniques (PETs) that minimize or eliminate the collection of personal information. The collection of personally identifiable information will necessarily require new privacy laws and safeguards. If smart communities fail to minimize data collection and establish strong privacy and security measures to safeguard the data that is collected, they will almost necessarily place their inhabitants at risk of system failure and cyber attacks.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

/s/ Kim Miller
Kim Miller
EPIC Policy Fellow

[10] Matt Stroud, *The Minority Report: Chicago's New Police Computer Predicts Crimes, But Is It Racist?*, The Verge, Feb. 19, 2014, http://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer- predicts-crime-but-is-it-racist; John Eligon, Timothy Williams, *Police Program Aims to Pinpoint Those Most Likely To Commit Crimes,* New York Times, Sept. 24, 2015, https://www.nytimes.com/2015/09/25/us/police-program-aims-to-pinpoint-those-most-likely-to-commit-crimes.html.

[11] EPIC v. DOJ, No. 17-410, (D.C. Cir. filed Mar. 7, 2017), https://epic.org/foia/doj/criminal-justice-algorithms/EPIC-v-DOJ-criminal-justice-algorithms-complaint.pdf.