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

# COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

NATIONAL SCIENCE FOUNDATION

Smart Cities and Communities Federal Strategic Plan: Exploring Innovation Together

[Docket No. 2017-00501]

February 28, 2017

By notice published on January 9, 2017 the National Science Foundation ("NSF") requests public comments regarding the Smart Cities and Communities Federal Strategic Plan: Exploring Innovation Together ("Smart Cities Plan").[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to urge the NSF to revise the draft document to prioritize cybersecurity in smart city development, address privacy concerns, and minimize data collection.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and human rights issues and to protect privacy, the First Amendment, and constitutional values. EPIC has considerable expertise in the Internet of Things and other connected devices and has testified before Congress on connected vehicles and submitted numerous comments to various agencies concerning connected devices.[2] EPIC has also submitted comments on the privacy implications and need for transparency of the development and use of the Smart Grid.[3]

[1] *Request for Comment on "Smart Cities and Communities Federal Strategic Plan: Exploring Innovation Together,"* 82 Fed. Reg. 3810 (Jan. 9, 2017).

[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 Statement to the House Committee Subcommittee on Communications and technology, Feb. 2, 2017, https://epic.org/testimony/congress/EPIC-Statement-NTIA-02-02-2017.pdf; Comments to the NTIA "On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things," June 2, 2016, https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf.

[3] EPIC Comments to the California Public Utility Commission, "Proposed Policies and Findings Pertaining to the EISA Standard Regarding Smart grid and Customer Privacy," Mar. 9, 2010, https://epic.org/privacy/smartgrid/EPIC_03_10_CPUC_Comments.pdf

*The Smart Cities Plan Should Be Updated to Prioritize Cybersecurity and Privacy*

EPIC urges NSF to emphasize cybersecurity and privacy must be in all aspects of smart city planning. The long-term, sustainable goals mentioned in the Smart Cities Plan will be impossible without a secure system.

The need for strong cybersecurity measures in cities is already be 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] The DHS report also noted that most states acknowledge their lack of understanding of cybersecurity practices.[8] The benefits that smart cities could bring cannot be achieved if the systems are insecure and cities are subject to hacks that threaten public safety.

*Protecting Individual Privacy*

The Smart Cities Plan envisions monitoring roads and first-responder activity so that resources are used efficiently. However, the plan should explain how data from private individuals will be safeguarded. The Plan should also address the potential discriminatory effect of monitoring individual behavior through secretive algorithms. For example, several cities have entered into data sharing agreements with popular traffic apps that rely on self-reporting[9] If these agreements become the norm, cities must protect individual privacy and be transparent with the public about how they use the data they receive and ensure that consumer data is protected.

Additionally, using data points to determine where first responders, especially law enforcement, are most needed could potentially increase police presence in some communities. An

[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?utm_term=.c3df5f646abb

[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/#3fba10ed39ba; 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/.

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 and who they know.[10] While attempting to achieve efficient use of resources, the Smart Cities Plan should also consider the potential discriminatory effects and require transparency about how first responders use data they collect and algorithms that they use.[11]

*Data Minimization*

The collection of personally identifiable information ("PII") will necessarily requires new privacy laws and new privacy safeguards. Innovative solutions that reduce regulatory burdens will be based on Privacy Enhancing Techniques ("PETs") that minimize or eliminate the collection of PII.[12]

If "Smart Cities' 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 from system failure, and cyber attack.

*Conclusion*

The Smart Cities Plan raises profound privacy and security challenges. It would be foolhardy to proceed down this road without a clear understanding of the risks and an equally clear commitment to establish necessary safeguards.

*Marc Rotenberg*
Marc Rotenberg
EPIC President

*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?_r=0.

[11] *Algorithmic Transparency: End Secret Profiling*, EPIC, https://epic.org/algorithmic-transparency/.

[12] Marc Rotenberg, *Preserving privacy in the Information Society* (UNESCO 2000), http://www.unesco.org/webworld/infoethics_2/eng/papers/paper_10.htm