February 28, 2017

**Comments from the Future of Privacy Forum to the National Coordination Office for Networking and Information Technology Research and Development (NITRD)**

On behalf of the Future of Privacy Forum, we are pleased to submit these comments regarding the Request for Comment on the *Draft Smart Cities and Communities Federal Strategic Plan*, published in the Federal Register on January 9, 2017.

## Introduction

Today's cities and communities are already pervaded by growing networks of connected technologies to generate actionable, often real-time data about the city or community and its citizens. Sensor networks and always-on data flows are already supporting new service models and generating analytics that make modern cities and local communities faster and safer, as well as more sustainable, livable, and equitable. At the same time, connected smart city devices raise concerns about individuals' privacy, autonomy, freedom of choice, and potential discrimination by institutions.

We commend NITRD for its forward-looking guidance and the acknowledgement that privacy will play a key role in promoting trust in smart cities and communities. This guidance and its emphasis on privacy is an important first step in building that trust.

The Future of Privacy Forum (FPF) is a DC-based non-profit organization that serves as a catalyst for privacy leadership and scholarship, and advances principled data practices in support of emerging technologies. We run a Smart City Working Group composed of over ninety representatives from local government, technology suppliers, connectivity providers, consumer advocacy organizations, and academia. This group serves as an ongoing collaborative effort to pursue best practices for data in the smart city/community ecosystem.[1]

We strongly agree that the path forward for city/community innovation in both the U.S. and globally lies through data and knowledge-sharing, best practices, and collaboration. Federal support to advance secure, privacy-preserving data sharing is critical to achieving this goal. In our work with smart city and community stakeholders, we have identified several key domains that we believe are ripe for Federal support and should be considered for this group's next steps.

## Federal Support to Advance Secure, Privacy-Preserving Data Sharing

***De-identification resources, training, and expertise.*** Many smart cities/communities have committed to making civic data available to partners, vendors, peers, advocates, academics, and citizens around the world via a range of mechanisms, including everything from public open data portals to private, custom data sharing agreements. While these data-sharing efforts serve important scientific and societal goals, city/community leaders must also ensure that individuals' personal data are kept private and secure in the process.

One of the greatest risks of sharing government datasets or opening them to the public is the possibility that individuals may be re-identified or singled out from those datasets, revealing data about them that could be embarrassing, damaging or even life threatening. Recent advances in

[1] The views herein do not necessarily reflect those of our members or our Advisory Board.

smart city data-collection technologies, re-identification science, data marketplaces, and Big Data analytics raise the risk of re-identification. These concerns loom all the larger as open data efforts continue to mature, no longer simply publishing historic data and statistics but increasingly making granular, searchable data about the city's – and its citizens' – activities available to anyone in the world.[2]

De-identification – the process of modifying personal data to ensure that data subjects are no longer identifiable—is one of the primary measures that organizations take to protect and share data in a privacy-preserving manner. Nevertheless, de-identification may be one of the most difficult tools for cities/communities to implement.

Governments and scholars have recently begun to tackle the difficulty question of publishing and de-identifying record-level government data. In 2015, for example, the National Institute of Standards and Technology (NIST) released a level-setting report on *De-Identification of Personal Information*, followed up by a specific guide to *De-Identifying Government Datasets* in 2016.[3] Municipalities are beginning to join in these efforts as well, focusing primarily on de-identification in the context of open data programs. For example, the City of San Francisco published the first iteration of an "*Open Data Release Toolkit*" in 2016.[4] FPF and the City of Seattle are currently developing an "*Open Data Risk Assessment*" in collaboration with a community advisory board and local academics, to be published in July 2017.

Despite these emerging toolkits and guidance documents, municipalities lack easy access to experts and new developments in de-identification science. Federal support for a central repository of resources, training, and experts would support the capacity of city nationwide to incorporate effective de-identification when appropriate for the data they collect, share, and handle. Federal support for continued research into expertise and best practices around de-identification would facilitate municipal decision-making, protect individual privacy, and accelerate smart city/community innovations.

***Privacy risk assessment frameworks.*** When responsible organizations identify new ways to process data, for example, when launching a new program, product, system, or service, they utilize Privacy Impact Assessments (PIA) to conduct a systematic analysis to identify and address privacy issues. Current PIA practice includes detailed frameworks to help privacy professionals understand and quantify privacy risks. However, traditional private sector PIAs do not necessarily account for the unique risks created by smart city/community projects, which may include:

- Ethical, societal, and reputational risks, including concerns about power imbalances, discrimination, and government surveillance of citizens and vulnerable populations,

---

[2] *See, e.g.*, Lauren FitzPatrick, *CPS Privacy Breach Bared Confidential Student Information*, CHICAGO SUN TIMES (Feb. 25, 2017), http://chicago.suntimes.com/news/cps-privacy-breach-bared-confidential-student-information/; Alex Tockar, *Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset*, NEUSTAR RESEARCH (Sept. 15, 2014), https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/.

[3] *See* NISTIR 8053: DE-IDENTIFICATION OF PERSONAL INFORMATION, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2015), http://dx.doi.org/10.6028/NIST.IR.8053; DRAFT NIST SP 800-188: DE-IDENTIFYING GOVERNMENT DATASETS, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2016), http://csrc.nist.gov/publications/drafts/800-188/sp800_188_draft2.pdf.

[4] *See* OPEN DATA RELEASE TOOLKIT, DATASF (2016), https://datasf.org/resources/open-data-release-toolkit/.

- Public-private partnerships with complex data ownership, security, and management arrangements,
- Open data commitments and public records laws which may reveal individual information,
- Public spaces or circumstances in which individual notices or choices are not feasible (e.g., infrastructure upgrades that may incidentally capture personal data, but which would not be effective were citizens allowed to opt-out).

FPF is currently receiving input from our Working Group stakeholders on a PIA for smart city/community projects.

At the same time, accounting for risks is only part of a balanced value equation. Decision-makers must also assess, prioritize, and to the extent possible, quantify a project's benefits in order to understand whether assuming the risk is ethical, fair, legitimate and cost-effective. Municipalities in particular are stewards to the data of numerous, highly diverse populations, and must bear in mind that social and cultural priorities and sensitivities may vary just as widely among their constituent communities. Federally-supported guidance or convenings to help city/community leaders assess the sensitivity of particular data points would further strengthen city/communities' ability to collect, use, share, and dispose of data in a consistent and privacy-preserving manner.

***Formation of a network of privacy leaders for smart cities/communities.*** The most effective way to provide cities and communities with the types of privacy resources and expertise described above would be to establish a privacy-focused network of city innovation and technology leaders. FPF has recently established a School Leaders Privacy Network with funding from the Bill & Melinda Gates Foundation as part of its education and student privacy program, helping educators better communicate and collaboratively address core privacy issues and principles.

Currently, many local governments and officials lack the institutional resources and knowledge to assess and manage the range of privacy risks that might arise from the use of smart city/community technologies and services. The emergence of Chief Innovation Officers (CIOs), Chief Technology Officers (CTOs), Chief Privacy Officers (CPOs), and Chief Data Officers (CDOs) within municipal governments points towards a growing awareness that data privacy and security are a priority. Federal support for a network of city/community privacy leaders and a central repository of common tools, terminology, and training would enable privacy-preserving systems to scale across application areas and geographic boundaries.

**Conclusion**

This *Draft Smart Cities and Communities Federal Strategic Plan* is a productive first step in establishing a consistent path forward for smart city/community innovation. We thank NITRD for recognizing the importance of privacy and look forward to remaining engaged as the guidance evolves. Please contact FPF Policy Counsel Kelsey Finch, kfinch@fpf.org, with any follow-up or questions.

Sincerely,

| | | |
|---|---|---|
| Kelsey Finch | Omer Tene | Jules Polonetsky |
| Policy Counsel | Senior Fellow | CEO |