FUTURE OF PRIVACY FORUM

1400 Eye Street NW, Suite 450, Washington, DC 20005 | 202-768-8950 | fpf.org

Comments of the Future of Privacy Forum on the Array of Things Governance & Privacy Policy

June 2016

The Future of Privacy Forum (FPF) is a think tank seeking to advance responsible data practices and is supported by leaders in business, academia and consumer advocacy.[1]

We would like to thank the Array of Things (AoT) project for this opportunity to provide feedback on the proposed Governance and Privacy Policies, and to engage with the broader Chicago and smart city communities. We applaud the AoT's commitment to building a transparent and responsive program.

While this initial privacy policy proposal provides a useful starting point, we urge the AoT's Security and Privacy Group and Executive Oversight Council to expand or revise it in several ways to better achieve its goals of balancing privacy, transparency, and openness.

(1) The Privacy Policy should reflect a FIPs-based framework.

The Fair Information Principles (FIPs) are "the framework for most modern privacy laws around the world" and NIST recommends that in order to "establish a comprehensive privacy program that addresses the range of privacy issues that organizations face, organizations should take steps to establish policies and procedures that address all of the Fair Information Practices."[2]

The current AoT Privacy Policy addresses some, but not all, of these principles. In a more robust FIPs-based Privacy Policy, we would also expect to see meaningful details regarding:

- What rights or mechanisms, if any, individuals might have to **access, correct, or request the deletion** of their PII?
- What mechanisms, if any, provide individuals with **redress** regarding the use of their PII?
- In addition to discipline and confidentiality promises, what a**ccountability controls** (such as employee training, vendor audits, or data use agreements) will help ensure employees, contractors, and approved partners with access to PII comply with the privacy policy.
- How long will PII be **retained**, how PII will be disposed of after it is no longer reasonably necessary for the purposes for which it was collected, and how PII will be treated if the AoT program dissolves or transfers ownership.
- How and when PII will be **deleted or de-identified**.

[1] The views herein do not necessarily reflect those of the Advisory Board or supporters of FPF.
[2] http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

- How the program operators will respond to requests from local, state, or federal civil or **law enforcement** agencies to access PII (such as when presented with a warrant or subpoena) and to what extent PII is subject to Freedom of Information Act disclosure requests.
- Information on how to **contact AoT officials** regarding any privacy or data security breaches.
- How will PII be **secured** through appropriate administrative, technical, and physical safeguards (such as encryption at rest and in transit, local processing or storage, etc.) against a variety of risks, such as data loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- What mechanisms, if any, are available for individuals to exercise **control** or **choice** over the collection of PII (e.g., could individuals turn off their phones or participate in an opt out to avoid certain kinds of tracking?)
- How the AoT **minimizes** the collection of PII.

Importantly, given the significant amount of information that residents of and visitors to Chicago might be expected to digest, a **layered privacy notice** highlighting key points would be appropriate. Additional notifications, such as public signage on or around AoT nodes or just-in-time mobile notices pointing to the full privacy policy might also help provide meaningful notice.

(2) More meaningful technical details within the Privacy Policy would improve trust and transparency for the wide array of stakeholders interested in assessing the program's privacy and security promises and practices.

The AoT's Privacy Policy is relevant not just to the citizens and communities of Chicago but also a wide range of civil society organizations; other local, state, and federal government officials; academics; potential vendors or research partners; technologists and privacy professionals; and the media. Accordingly, we recommend that the Privacy Policy further expand or clarify:

- **Distinguishing clearly between PII and sensitive data collected by the AoT**. The Privacy Policy states that because of their "potential sensitivity," location information, electronic device identifiers, or vehicle license plate information should be regarded as PII. This conflates between the concept of PII and that of sensitive data, missing the clear consensus among regulators and privacy experts that regardless of sensitivity, these data fields are PII.[3] In privacy nomenclature, describing data as PII typically means that the data

[3] See, e.g., NIST Report on De-Identification, http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf; FTC Director Jessica Rich on persistent device identifiers https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry; *Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757709.

can be linked to an identifiable individual, whereas considering data "sensitive" typically signals that the data will be treated to a *higher* standard of privacy protection. In order to avoid confusion, we suggest clarifying these terms.

- **When audio or image files may contain PII, what specific kind of PII is collected**. There is a stark difference in privacy impact between software used to simply detect faces (facial detection) and software capable of identifying individuals in photos via biometric templates (facial recognition). A similar distinction is made between speech detection and speech recognition capabilities. Given the general public unease about loss of anonymity and privacy in public spaces, it is key to clarify what technologies are being used in this context and what capabilities they have for processing PII. This will help allay fears regarding the use of PII from image and audio files captured in public spaces.

- **How the AoT will ensure adequate de-identification for data made public through the City's data portal.** Open data enables important scientific research and urban innovation. Given the AoT's intent to make its data available freely, it must implement the strongest possible protections against the intentional or inadvertent re-identification of any individuals within the data set. AoT should clarify publicly how it will ensure that the risk of re-identification is sufficiently low that individual privacy can be guaranteed. What is the acceptable threshold for re-identification risk, and how is it calculated? Will the AoT use differential privacy solutions? How will AoT handle the de-identification within image or audio files as opposed to structured textual data? Will any legal controls or commitments (such as agreements to not attempt to re-identify data) be required before accessing de-identified data? While not expected to publish every detail of its de-identification strategy or lock itself into a particular set of practices, the AoT should make known important parameters to increase trust and transparency.

(3) Additionally, FPF recommends that all smart city initiatives, including the AoT, implement a variety of other organizational and technical measures to safeguard personal data, including:

- Mapping data flows, including where data is collected and how it is used throughout the entire AoT ecosystem.
- Classifying data according to sources, identifiability, sensitivity, and uses.
- Documenting processes and procedures for sharing data with third parties and monitoring vendors, including data use agreements, audit and standard contractual terms, and transparency about how and by whom scientific partners are "approved."
- Safeguards to protect against unfair or discriminatory uses of data.
- Identifying what data sets are owned by which stakeholders, and any relevant copyright, licensing, or access provisions.
- Documenting risk-benefit assessments and structured ethical review processes for evaluating new research or uses of PII.

Thank you for this opportunity to share our thoughts on this important initiative.

Sincerely,

Kelsey Finch
Policy Counsel
Future of Privacy Forum