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 to the City of New York Mayor's Office of Information Privacy Re: Request for Input on Citywide Privacy Protection Policies

January 2019

In 2019, the Chief Privacy Officer for New York City sought input from stakeholders on how the City could best serve the public's privacy interests while continuing to advance the programs and services that aid New Yorkers every day.

The Future of Privacy Forum (FPF) submitted the following comments via the CPO's online contact form. FPF is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF is supported by the privacy officers of more than 150 companies and by leading foundations, with an advisory board of academic, civil society, and industry members.[1]

What do you believe are the most important privacy interests of New Yorkers?

In today's hyperconnected world, protecting individuals' privacy interests is as much a matter of ethics and equity as it is about protecting personal data. In particular, the CPO and MOIP should consider New Yorkers' interests in:

- Knowing when, how, and why their personal data is being collected, used, shared, and retained by their local government and its partners. Such information should be clear, easy to understand, and accessible to all New Yorkers.
- Being able to make meaningful choices about when and how their personal data is collected and used by their local government, or, where that is not feasible, in having their voices heard and considered through robust, data and privacy-focused public engagement processes.
- Ensuring that any personal data held by the City is appropriately secured and protected from inadvertent disclosure or misuse. This means that the City must invest in appropriate data security, including measures to prevent data breaches and ransomware attacks, and that no personal data should be disclosed by City agencies without appropriate safeguards in place. Further, when City agencies disclose data publicly, such as through a FOIL request or an open data initiative, heightened measures should be taken to prevent New Yorkers' personally identifiable data from being exposed. The 2014 re-identification of hashed records from the Taxi & Limousine Commission, for example, highlights the

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

need for strong and consistent privacy safeguards around public disclosure of personally identifiable data.[2]

- Whether individuals will be discriminated against or treated inequitably based on data collected from and about them, particularly in the context of automated or algorithmic decision making. Without appropriate protections in place, New Yorkers could be at risk for a number of significant harms, including loss of opportunity, economic loss, social detriment, and loss of liberty.[3]
- The impact of new technologies and surveillance tools on New Yorkers' long-held sense of urban anonymity. Sensor and camera networks are already prevalent throughout the City, and the rapid emergence of commercial facial recognition and AI-based systems threatens to create an environment in which entering the public realm means entering a panopticon. Appropriate safeguards are necessary to ensure that New Yorkers retain an ability to move and act in public without the chilling effects of constant, ubiquitous surveillance.
- City agencies' desire to use New Yorkers' personal data for research. Whether City agencies conduct research internally, partner with academics or institutions, or share personal data with other organizations for such purposes, serious ethical concerns are implicated. While such research may promise significant benefits for society, personal data collected by the City for other reasons should not be repurposed without undergoing an ethical review process.[4]

How do you think New Yorkers' privacy interests can be best addressed in citywide policies and protocols regarding the collection retention and disclosure of identifying information by City agencies?

In building a citywide framework for collecting, retaining, and disclosing identifying information, the City should:

- Adopt a consistent, flexible framework based on the Fair Information Practice Principles (FIPPs).
- Meaningfully and inclusively engage New Yorkers and their communities in the development and implementation of such policies and protocols.
- Create clear oversight and accountability mechanisms, such as a public privacy advisory board or ombudsperson.

---

[2] https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-detailsanonymised-data-researchers-warn.

[3] See https://fpf.org/wpcontent/uploads/2017/12/FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf.

[4] For example, https://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1005399.

- Invest in privacy and data protection education and training for all City employees. o Consistently evaluate and document the anticipated benefits and privacy risks of City activities collecting or using personal data.
- Ensure that service providers or other recipients of personal data are held to equivalent standards of privacy protection.
- Provide for appropriate administrative, legal, and technical safeguards throughout the full information lifecycle.

Do you think any additional types of City contracts and subcontracts for services should be covered by the Identifying Information Law? What types of contracts or subcontracts should be covered?
Yes. Any contracts or subcontracts in which New Yorkers' personal data is shared or disclosed.

Additional comments on selected topics to be specifically addressed by the CPO's new policies and procedures, per the mandates of the Identifying Information Law.

Anonymization/de-identification: The CPO should seek to minimize the amount of personally identifiable information held by the City, including by creating policies and procedures to delete or render data less- or unidentifiable whenever possible, depending on the purposes for which the data were collected. Nevertheless, adequately anonymizing personal data is an enormously difficult task, especially if the City intends to make "anonymized" data available to other organizations or the public. Whether and how personal data can be truly anonymized is a hotbed of ongoing scholarly debate, and advances in re-identification science and the increasing availability of rich public databases have led scientists and policymakers to doubt the long-term reliability of many traditional disclosure control techniques. Re-identification risks must be carefully evaluated and mitigated on an ongoing basis.

Given the state of current anonymization technology and policy, the CPO should:

- Create clear and consistent standards for what is considered "personally identifying" information and, conversely, what is considered "anonymized" or "anonymous" information.
- Seek to acquire provably private tools, such as differentially private or secure computing solutions, especially when the resulting data will be made available publicly.
- Partner with experts, conduct motivated intruder tests, and evaluate re-identification risks on an ongoing basis.
- Complement technical or mathematical safeguards with legal and administrative protections (such as contractual commitments not to attempt to re-identify individuals within a dataset).

For more recommendations around anonymization in the context of open data and other circumstances where City agencies may be making anonymized data available to the public, see FPF's recommendations for conducting an Open Data Privacy Risk Assessment.[5]

Disclosure agreements:
The City should be transparent with the public about what kinds of disclosure "circumstances" specifically will or will not trigger this documentation. The City should seek to be equally transparent about interagency disclosures of identifying and identifiable data, as well as the role for review by agency privacy officers in such circumstances.

Standard contract provisions:
This type of standardization is an important way to give New Yorkers consistent privacy expectations and experiences in their dealings with the City. Moreover, if the City sets strong standards for privacy protection in its contracts, it can help create or strengthen the market for privacy-preserving products and services more broadly, benefiting New Yorkers' privacy interests in the private sector as well. UW's Tech Policy Lab, for example, has published excellent research on these issues: http://techpolicylab.org/wp-content/uploads/2016/03/Push-Pull-Spill_Open-Government_2015.pdf

Complaint mechanisms:
The City should be transparent with New Yorkers not only in how complaints will be accepted and investigated, but also about what potential remedies will (or will not) be available to affected individuals should a violation occur.

Additional information or comments.

The City and the CPO should be commended for undertaking this important effort to protect the privacy interests of New Yorkers. Other safeguards that the CPO should consider implementing include:

- Expanding the scope of these policies and procedures to both personally identifying and personally identifiable information, if that is not already the City's intention. Mishandling or misuse of personally identifiable information can, in many circumstances, be just as harmful to New Yorkers' privacy interests as mishandling or misuse of explicitly identifying information.
- Conducting comprehensive Privacy Impact Assessments for all privacy-impacting technologies or services employed by the City and making them publicly available (see, for example, the Surveillance Impact Reports currently underway in the City of Seattle).

---

5 https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessmentfor-City-of-Seattle.pdf .

- Ensuring that decisions by City agencies about what personal data to collect are made with the full data lifecycle in mind, including what the repercussions would be if the data were the subject of a FOIL request,[6] a data breach,[7] or a state or federal inquiry.[8]
- Establishing strong protections for individuals in any situation where the City utilizes automated or algorithmic decision-making tools, in coordination with the City's Automated Decisions SystemsTask Force. This may include implementing disparate impact analysis, algorithmic audits or transparency reports, providing for human review of automated decisions, and other technical, legal, and administrative solutions.[9]

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

Sincerely,

Kelsey Finch
Policy Counsel
Future of Privacy Forum

---

[6] https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-detailsanonymised-data-researchers-warn.
[7] https://www.lexology.com/library/detail.aspx?g=11f87a58-2de8-4017-8fe3-06c1b36af674.
[8] https://www.nytimes.com/2018/07/10/nyregion/idnyc-fort-drum-silvabarrios.html.
[9] For more on addressing algorithmic harms, see FPF's work here: https://fpf.org/wpcontent/uploads/2017/12/FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf.