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

CITY OF NEW YORK MAYOR'S OFFICE OF INFORMATION PRIVACY

Request for Input on Citywide Privacy Protection Policies

By online notice, the City of New York Mayor's Office of Information Privacy requested input on Citywide Privacy Protection Policies.[1] The Mayor's Office of Information Privacy "works to protect the privacy of New Yorkers' identifying information" and "aims to increase access to and strengthen coordination of services for individuals and families, and to encourage innovative projects throughout the city that advance equity and opportunity."[2] The Request for Input asked commenters to identify the most important privacy interests of New Yorkers and how those interests are best protected in citywide policies and protocols. The Office also asked whether contractors or subcontractors beyond providers of "human services" or social services should be bound by the privacy policies. EPIC answers yes.

EPIC submits comments to the Mayor's Office of Information Privacy to (1) identify the most important privacy interests of New Yorkers; (2) identify key privacy issues facing cities that implicate privacy interests; and (3) highlight ways cities are tackling key privacy issues facing cities.

---

[1] NYC Mayor's Off. of Info. Privacy, *Request for Input on Citywide Privacy Protection Policies*, https://www1.nyc.gov/site/moip/contact/contact.page.
[2] NYC Mayor's Off. of Info. Privacy, *Welcome to the Mayor's Office of Information Privacy*, https://www1.nyc.gov/site/moip/index.page.

EPIC is a public interest research center in Washington, DC. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age.[3] Indeed, issues that EPIC has brought to the public's attention have been pursued by the New York Attorney General. For example, in 2009 EPIC sounded the alarm about a product marketed to protect children online that sold children's conversations to advertisers.[4] In a complaint to the Federal Trade Commission ("FTC"), EPIC explained that EchoMetrix offered a product to allow parents to monitor their children's activity, while simultaneously selling conversations and browsing history to marketers.[5] The FTC charged and settled with EchoMetrix, and the New York Attorney General also brought charges against the company and came to an important settlement with EchoMetrix.[6] The company ceased offering the marketing product after the New York Attorney General's investigation began.[7]

I. What are the most important privacy interests of New Yorkers?

Biometrics

Biometric data is personally identifiable information of an individual's physical characteristics or personality traits used for identification or authentication.[8] Biometric identifiers include—but are not limited to—facial recognition, fingerprints, palm prints, iris scans, voice

[3] EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.
[4] Complaint from EPIC to the Fed. Trade Comm'n, *Matter of Echometrixs, Inc.*, 1 (Sept. 25, 2009), https://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf.
[5] *Id.*
[6] Lesley Fair, *FTC's EchoMetrix Settlement: EULA-ppreciate This Guidance on Privacy Disclosures*, Fed. Trade Comm'n (Dec. 3, 2010), https://www.ftc.gov/news-events/blogs/business-blog/2010/12/ftcs-echometrix-settlement-eula-ppreciate-guidance-privacy; N.Y. Att'y Gen., *Cuomo Announces Agreement Stopping Software Company "Echometrix" from Selling Children's Private Online Conversations to Marketers* (Sept. 15, 2010), https://ag.ny.gov/press-release/cuomo-announces-agreement-stopping-software-company-echometrix-selling-childrens.
[7] N.Y. Att'y Gen., *supra* note 6. .
[8] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 Stan. L. Rev. 1461, 1494 (2000) (distinguishing that "identification" asks "who is this?" and "authentication" asks "what permissions does this person have?").

data, and gait recognition.[9] Biometric data is identifiable information that cannot be changed, even if compromised. Biometric information constitutes a principal privacy interest because it can contribute to identity theft, inaccurate identifications, and infringement on constitutional rights.

As technologies increasingly use the "body as [a] password" to access personal information, biometric data increases in value to hackers.[10] Biometric data can be used to access finances[11] and to unlock digital devices containing troves of additional personal information.[12] The immutability of citizens' biometric data significantly enhances its value to hackers seeking to access these services and devices. Once in the hands of hackers, citizens' "security and safety could be compromised for the rest of their lives."[13] The consequences of data breaches of biometric data are heightened by the fallibility of biometric authentication devices. Recent research has shown that fingerprint-based recognition systems can be deceived by fingerprints casted onto 3D printed hands[14] and computer-generated fingerprints.[15]

---

[9] Lucas D. Introna & Helen Nissenbaum, Facial Recognition Technology: A Survey of Policy and Implementation Issues 10 (2009); Richard W. Vorder Bruegge, *Facial Recognition and Identification Initiatives*, Fed. Bureau of Investigation Biometric Ctr. of Excellence, https://www.eff.org/files/filenode/vorder_bruegge-facial-recognition-and-identification-initiatives_0.pdf; Fed. Bureau of Investigation, *Next Generation Identification*, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi.

[10] *See* Froomkin, *supra* note 8, at 1495 (noting that biometric identifiers have supplanted conventional identifiers, such as the password, PIN, and hardware token); Introna & Nissenbaum, *supra* note 9, at 9 (recognizing that biometric technologies may remedy challenges associated with identifying individuals in exchanges that are increasingly devoid of direct and personal interactions).

[11] Mai Nguyen, *How to Bank with Your Fingerprint*, Chase (July 17, 2018), https://www.chase.com/news/071718-bank-with-voice; Wells Fargo, *Biometric Authentication*, https://www.wellsfargo.com/online-banking/biometric.

[12] Apple, *Use Touch ID on iPhone and iPad*, https://support.apple.com/en-us/HT201371.

[13] EPIC, *Comments on Docket CPCLO Order No. 002-2016: Notice of a Modified System of Records Notice: Privacy Act of 1974 System of Record & CPCLO Order No. 003-2016: Notice of Proposed Rulemaking: Privacy Act of 1974 Implementation* 8 (July 6, 2016), https://epic.org/apa/comments/EPIC-CPCLO-FBI-NGI-Comments.pdf [hereinafter EPIC, *Comments*].

[14] Joshua J. Engelsma et al., Universal 3D Wearable Fingerprint Targets: Advancing Fingerprint Reader Evaluations (2017), https://arxiv.org/pdf/1705.07972.pdf.

[15] Philip Bontrager et al., DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution (2018), https://arxiv.org/pdf/1705.07386.pdf.

Biometric data can be used on a mass scale to infringe upon First Amendment rights of free association and free expression. Biometric data, such as facial recognition, can identify people, in real-time or retroactively, to "reveal the protests one participate in, the groups one associate with, or the things one spoke out about,"[16] threatening to undermine and chill the exercise of these constitutional rights.[17] The mere belief that biometric data could be used to identify an individual can chill the exercise of these fundamental freedoms.[18]

Location Data

Location data, both real-time and historical, constitute principal privacy interests because they each reveal personal information about an individual. In recent years, the Supreme Court has repeatedly recognized this privacy interest, noting that location data not only reveals movements but also a person's "familial, political, professional, religious, and sexual associations."[19] The Court has explicitly recognized that this privacy interest in location data encompasses all long-term location monitoring—irrespective whether those movements occurred in public or private.[20]

Moreover, the Supreme Court has evinced the significant privacy interest in location data by expanding constitutional protections to abate privacy threats posed by increasingly pervasive and comprehensive tracking technology. Expounding upon an expectation of privacy against GPS monitoring, the *Carpenter* Court recently extended privacy protections to historical cell-site

[16] EPIC, *Comments*, *supra* note 13, at 10.
[17] *See* Anita L. Allen, *Associational Privacy and the First Amendment:* NAACP v. Alabama*, Privacy and Data Protection*, 1 Ala. C.R. & C.L. L. Rev. 1, 13 (2011) (advocating that technological advancements should not abridge the right of private free association safeguarded in *NAACP v. Alabama*, 357 U.S. 449 (1958)).
[18] *See* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 Ind. L.J. 1131, 1146 (2011) ("Many of the harms we associate with a person seeing us—embarrassment, chilling effects, loss of solitude—flow from the mere belief that one is being observed.").
[19] *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).
[20] *Id.* at 2215 (citing *Jones*, 565 U.S. at 430 (Alito, J., concurring)); *United States v. Karo*, 468 U.S. 705 (1984).

location information, stating that pervasive, inescapable tracking raises distinct privacy concerns.[21]

SSN and Financial Information

Social Security Numbers and financial information are a principal privacy interest of New Yorkers. The threat of identity theft underlines the necessity to safeguard these interests. Created in 1936 to administer social security laws, Social Security Numbers have since been linked to additional personal information.[22] A Social Security Number is now associated with an individual's taxpayer identification number, credit information, school records, and medical records.[23]

The valuable personal information associated with a Social Security Number is leveraged to commit identity theft. Identity theft occurs when someone uses another individual's Social Security Number or other financial information to open accounts, file a tax refund, authorize purchases, or receive other benefits in another person's name.[24] A person may obtain another individual's Social Security Number by, *inter alia*, stealing it from unsecured sources, purchasing it from "inside" sources, or posing as a legitimate official.[25]

Identity theft is a rampant problem plaguing U.S. citizens. A recent Department of Justice report highlights that approximately 26 million U.S. residents age 16 or older were victims of

---

[21] *Carpenter*, 138 S. Ct. at 2218 (majority opinion) (citing *Riley v. California*, 134 S. Ct. 2473, 2484, 2490 (2014)); *see* Froomkin, *supra* note 8, at 1480 (espousing that archives of historical cell-site location information dramatically increase "[t]he privacy-destroying consequences of cell phone tracking").
[22] Privacy Rts. Clearinghouse, *My Social Security Number-How Secure Is It?*, (June 1, 1993), https://www.privacyrights.org/consumer-guides/my-social-security-number-how-secure-it (last updated Aug. 29, 2018).
[23] *Id.*; U.S. Dep't of Health, Educ. & Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems: Records, Computers and the Rights of Citizens, at 118–21 (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf.
[24] Fed. Trade Comm'n, *Identity Theft*, https://www.consumer.ftc.gov/articles/0005-identity-theft.
[25] Soc. Security Admin., *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf; *see also* Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 Proc. Nat'l Acad. Sci. U.S. 10976, 10976–79 (2009) (demonstrating that public data can be used to deduce a narrow numerical range wherein a social security number is likely to fall).

identity theft,[26] and identity theft constituted the second largest category of complaints filed with the Federal Trade Commission in 2017.[27] Identity theft can debilitate its victims. A survey of 2016 identity theft victims reveals that, as a result of identity theft, 26% had to borrow funds from family and friends, 12% had to delay schooling, 15% had to relocate or move, and 22% had to forgo time with family.[28] Similarly, in 2017, identity theft caused 42.8% of identity theft victims to fall into debt while 40.5% could no longer pay their bills.[29]

II. Important Privacy Issues Facing Cities

Cities using technology and data to increase government efficiency, disseminate information, and improve the quality of life for their residents face a multitude of privacy and cybersecurity issues. These issues inextricably involve privacy interests of city residents, which must be protected when cities implement new technology and data collection practices. Some important privacy issues facing cities are the security of their IT systems, location tracking of residents, aggregation of data both cumulatively and in real-time, disclosure of data to third parties, implementation of machine learning and algorithmic fairness, transparency and accountability, and public participation.

Cybersecurity

Connected technology in cities creates more vulnerable points of entry for hackers, creating significant security issues surrounding the internet of things ("IoT").[30] Large scale

[26] Bureau of Justice Statistics, U.S. Dep't of Justice, Victims of Identity Theft, 2016, at 1 (2019), https://www.bjs.gov/content/pub/pdf/vit16.pdf.
[27] Fed. Trade Comm'n, Consumer Sentinel Network: Data Book 2017 6 (2018), https://www.ftc.gov/news-events/press-releases/2018/03/ftc-releases-annual-summary-complaints-reported-consumers.
[28] Identity Theft Res. Ctr., Identity Theft: The Aftermath 2017 7 (2017), https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf.
[29] Identity Theft Res. Ctr., The Aftermath: The Non-Economic Impacts of Identity Theft 7 (2018), https://www.idtheftcenter.org/wp-content/uploads/2018/09/ITRC_Aftermath-2018_Web_FINAL.pdf.
[30] Jathan Sadowski & Frank Pasquale, *The Spectrum of Control: A Social Theory of the Smart City*, First Monday vol. 20 no. 7, July 2015 1, https://firstmonday.org/article/view/5903/4660.

communication among city systems equate to large amounts of data accrued to provide services in the city. The data accrued can reveal sensitive information about an individual, such as their medical records and financial information. Each connection creates access points for hackers to access the trove of data collected by a city. Lack of data protection and strong security safeguards can result in the leak of this sensitive information.[31]

Cities and local governments constantly face cyberthreats from hackers due to the valuable nature of the data and weaknesses in their cybersecurity infrastructure. For example, 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.[32] In November 2017, hackers infiltrated San Francisco's public transportation system and threatened to release customer and employee data unless a ransom was paid.[33] In September 2018, security firm FireEye confirmed that local government-operated "Click2Gov" payment portals used to pay for local government services, such as utilities and permits, was targeted by hackers.[34] Residents in local governments across the country had credit card information, names, and addresses stolen by malware uploaded to Click2Gov servers.

Surveillance and Location Tracking

Cities implementing connected technology utilize technology that can receive, collect, and transmit data in real-time. Most of these technologies involve strategically placed cameras or

---

[31] *See* A. Michael Froomkin, *Government Data Breaches*, 24 Berkeley Tech. L.J. 1019, 1026 (2009) (identifying the causes of government data breaches in 2006 as 44% "human/software incompetence," 21% laptop theft, 17% other theft, 13% outside hackers, and 5% insider malfeasance).
[32] Clarence Williams, *Hackers Hit D.C. Police Closed-Circuit Camera Network, City Officials Disclose*, Wash. 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.
[33] 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.
[34] Zack Whittaker, *Hackers Have Planted Credit Card Stealing Malware on Local Government Payment Sites*, TechCrunch (Sept. 18, 2018), https://techcrunch.com/2018/09/19/hackers-have-planted-credit-card-stealing-malware-on-local-government-payment-sites.

devices with embedded recording sensors that are constantly recording people's movements throughout the city. Collecting location information without privacy protections, however, puts residents at risk of profiling and other surveillance risks.[35] Moreover, facial recognition is being implemented throughout cities and makes identifying people easier.[36] These cameras are always watching, listening, and tracking people in real time without their knowledge.[37] One example of smart technology raising privacy concerns is New York's LinkNYC kiosks—booths providing free public Wi-Fi and other services to New Yorkers and visitors in exchange for data to be used in advertising. Installed throughout New York City ("NYC"), these kiosks utilize three cameras, 30 sensors, and elevated sight lines to view above crowds. It has been recently revealed that the LinkNYC software has code capable of collecting a Wi-Fi user's geolocation, a user's browser and URL clickstreams, and device information into a database.[38] The 2016 LinkNYC privacy policy stated that it does not collect users' precise locations, yet it is unclear whether this code is currently running on any of the kiosks and whether any of the data that the kiosk already collected is shared with law enforcement and for what purpose.

Aggregation and Overcollection of Data

Cities implementing connected technology face issues surrounding the overcollection and aggregation of data. The collection, use, and retention of data by cities and their contractors pose privacy risks to individuals. Advances in data analytics tempt cities to collect more information than they need to accomplish their purposes. This can be seen at the federal government level

[35] *See* Colin J. Bennett & Priscilla M. Regan, *Surveillance and Mobilities*, 1 Surveillance & Soc'y 449, 454 (2004) ("[A]s surveillance systems collect more information, this leads to more detailed categorization of individuals and then to judgments based on those categorizations, leaving the concept of a unique individual in the dustbin of history.").
[36] *See* Introna & Nissenbaum, *supra* note 9, at 10 (recognizing that facial recognition has become the predominant biometric technology because it can identify individuals at a distance).
[37] Froomkin, *supra* note 8, at 1475; *see* Sadowski & Pasquale, *supra* note 30, at 9 (noting that surveillance systems in smart cities approach ubiquity, "always present, tirelessly watching" yet "rarely noticed").
[38] Ava Kofman, *Are New York's Free LinkNYC Internet Kiosks Tracking Your Movements?*, Intercept (Sept. 8, 2018), https://theintercept.com/2018/09/08/linknyc-free-wifi-kiosks.

and is not uncommon at the city level.[39] The capture of data from smart city technology results in aggregation of data. Aggregation of data combines various aspects about a person to identify a pattern of activity or trends and can lead to privacy consequences such as identity theft, real-time surveillance, and profiling.[40] Extended retention of this data also invites breach.

Cities must be conscientious of collecting data without violating Constitutional rights. Recently, a federal judge blocked a New York City law requiring online home sharing companies, such as Airbnb and HomeAway, to turn over, on a monthly basis, renter information about its users, including names, addresses, phone numbers, e-mail addresses, and details of how users use the booking services.[41] The New York City law was aimed to help the city curb short term rentals. The judge stated that the ordinance's breadth of information sought would be deemed excessively burdensome and unreasonably intrusive.[42]

Disclosure of Data to Non-governmental Parties

Another issue that cities face is the disclosure of data to non-governmental parties, particularly to companies that monetize this data for their products or for advertising. These data disclosure agreements implicate significant privacy interests for residents who cannot opt-out of their information being collected. While some data disclosure between cities and contractors are necessary to provide services, cities bear the responsibility of creating trustworthy data disclosure practices that protect citizen data. For example, cities have entered into data disclosure agreements with popular traffic app Waze, where Waze's Connected Citizens program

---

[39] *See, e.g.*, Comptroller Gen. of the U.S. Gene L. Dodaro, Testimony Before the U.S. House of Representatives, Committee on Oversight and Government Reform, Before the Subcommittees on Government Operations and Information Technology, *High-Risk Series: Urgent Actions are Needed to Address Cybersecurity Challenges Facing the Nation*, 29 (Nov. 18, 2015), https://www.gao.gov/assets/700/693405.pdf.

[40] *See* Alessandro Acquisti et al., *Face Recognition and Privacy in the Age of Augmented Reality*, 6 J. Privacy & Confidentiality 1, 9–12 (2014) (cross-referencing facial recognition technology with social media data to deduce social security numbers and infer personal interests).

[41] *Airbnb, Inc. v. City of New York*, 2019 WL 91990 (S.D.N.Y. Jan. 3, 2019).

[42] *Id.* at *16.

exchanges self-reported information from drivers in exchange for incident and road closure reports.[43]

Cities face challenges when they are competing for smart growth because some companies offering innovative technologies have poor reputations for protecting data privacy or have corporate interests adverse to residents living in the city. For example, in October 2017, Toronto and Sidewalk Labs, a city-building subsidiary of Google's parent company Alphabet, partnered to revitalize Toronto's Eastern Waterfront into a smart city—known as Quayside.[44] The partnership raised questions about how this smart city would collect and protect data. The proposal for Quayside included a centralized civic data trust, an identity management system that approves and manages the collection of information in the district.[45] While Sidewalk Labs asserts that it will de-identify data when it cannot provide individuals with meaningful control over their information,[46] it cannot guarantee that third-party developers will de-identify data and commit to privacy by design, undermining Sidewalk Labs's Privacy by Design safeguards.[47] These data privacy and security deficiencies prompted Sidewalk Labs privacy advisor Ann Cavoukian to resign, citing concerns that the civic data trust may become a centralized database of identifiable information vulnerable to unauthorized access and hacking.[48]

---

[43] *See Connected Citizens Program*, Waze (Oct. 16, 2017), https://wiki.waze.com/wiki/Connected_Citizens_Program.
[44] Press Release, Sidewalk Labs, New District in Toronto Will Tackle the Challenges of Urban Growth (Oct. 17, 2017), https://sidewalktoronto.ca/wp-content/uploads/2018/04/Sidewalk-Toronto-Press-Release.pdf.
[45] Sidewalk Labs, *Vision Sections of RFP Submission* (Oct. 27, 2017), https://sidewalktoronto.ca/wp-content/uploads/2018/05/Sidewalk-Labs-Vision-Sections-of-RFP-Submission.pdf
[46] Sidewalk Toronto, Responsible Data Use Policy Framework 4 (2018), https://sidewalktoronto.ca/wp-content/uploads/2018/05/Sidewalk-Toronto-Responsible_Data_Use_Framework_V0.2.pdf.
[47] *See* Sidney Fussell, *The City of the Future Is a Data-Collection Machine*, Atlantic (Nov. 21, 2018), https://www.theatlantic.com/technology/archive/2018/11/google-sidewalk-labs/575551.
[48] CBC News, *"Not Good Enough": Toronto Privacy Expert Resigns from Sidewalk Labs over Data Concerns* (Oct. 21, 2018), https://www.cbc.ca/news/canada/toronto/ann-cavoukian-sidewalk-data-privacy-1.4872223.

Machine Learning and Algorithmic Fairness

Cities are implementing connected AI technology that are capable of machine learning—but, with the implementation of AI technology comes the risk of bias.[49] Taking advantage of the troves of data collected, cities use AI and machine learning to make automated decisions about individuals. Today, algorithms are used to determine which individuals get a loan, get parole, qualify for government assistance, or get a job interview. Computers are neutral tools, but even if the code contains no bias, often the data it ingests does.[50] Cities will often use algorithms in predictive policing and sentencing. In 2014, then U.S. Attorney General Eric Holder expressed concern about the use of algorithms in sentencing determinations:

> Although these measures were crafted with the best of intentions, I am concerned that they inadvertently undermine our efforts to ensure individualized and equal justice . . . they may exacerbate unwarranted and unjust disparities that are already far too common in our criminal justice system and in our society.[51]

New York City, for example, uses black box algorithms to allocate fire stations, police officers, and food stamps.[52] The New York Police Department ("NYPD") predictive policing algorithms are also opaque when it uses Microsoft's Domain Awareness System of automated cameras, CCTV monitors, and traffic and audio sensors in public spaces for constant surveillance. These algorithms often target young men of color.

---

[49] *See generally* Batya Friedman & Helen Nissenbaum, *Bias in Computer Systems*, ACM Transactions on Info. Sys., July 1996, at 332 (defining biased computer systems as "computer systems that systematically and unfairly discriminate against certain individuals or groups of individuals in favor of others").
[50] Will Knight, *Biased Algorithms Are Everywhere, and No One Seems to Care*, MIT Tech. Rev. (July 12, 2017), https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care.
[51] Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
[52] Julia Powles, *New York City's Bold, Flawed Attempt to Make Algorithms Accountable*, New Yorker (Dec. 20, 2017), https://www.newyorker.com/tech/annals-of-technology/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable.

Transparency and Accountability

Cities face issues involving transparency and accountability in the smart city planning process. A lack of transparency in the collection, use, retention, and disclosure of data in government programs results in a secret surveillance state that fosters public mistrust. For instance, the NYPD faced criticism for its lack of transparency in using facial recognition technology for law enforcement.[53] Investigative reporting has also revealed that an IBM software used NYPD surveillance footage to develop a search feature that allows police departments to search video footage for images of people by skin tone, hair color, and facial hair.[54] The collaboration between IBM and NYPD was secretive, and New Yorkers were not aware that their physical data was used for IBM's surveillance technology development.

Public Participation

Cities also face the challenge of implementing policies that allow for greater public participation and citizen engagement in the smart city planning process. Cities will not reach their objectives if residents are not involved in the design, planning, and implementation stage. Moreover, residents cannot readily or reliably "opt-out" of data collection in the city where they live.[55] Therefore, as cities compete for social capital, residents need to be involved in the city

---

[53] *See* Anita L. Allen, *Driven into Society: Philosophies of Surveillance Take to the Streets of New York*, 1 Amsterdam L.F. 35, 38 (2009) (faulting the NYPD, *inter alia*, for failing to afford the public the right to know what data was being collected, stored, and shared; and failing to publicly disclose any security standard for retained data).

[54] George Joseph & Kenneth Lipp, *IBM Used NYPD Surveillance Footage to Develop Technology that Lets Police Search by Skin Color*, Intercept (Sept. 6, 2018), https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search.

[55] Several factors inhibit residents from opting out of data collection in their cities. First, many residents do not know about opt-out mechanisms due to inadequate notice. Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 Wash. L. Rev. 1033, 1072 (1999). Second, even if residents opt-out of data collection, the data collecting entities may not honor their opt-out requests. *See, e.g.*, Aleksandra Korolova, *Facebook's Illusion of Control over Location-Related Ad Targeting*, Medium (Dec. 18, 2018), https://medium.com/@korolova/facebooks-illusion-of-control-over-location-related-ad-targeting-de7f865aee78 (noting that Facebook continues collecting location data despite users disabling Location Services and Location History features); Ryan Nakashima, *Google Tracks Your Movements, Like It or Not*, Associated Press (Aug. 13, 2018), https://apnews.com/828aefab64d4411bac257a07c1af0ecb (revealing that Google services on cellphones

decision-making process. Individuals are entitled to the value of their data, and cities must construct mechanisms that allow for greater public participation and offer meaningful redress.

III. Ways Cities Are Addressing Key Privacy Issues and Protecting Privacy Interests

The privacy issues identified in these comments apply to all smart cities. But, cities confront these privacy issues differently based on the needs of their constituents and the amount of resources available. Below is a brief comparison of how cities are addressing key privacy issues and protecting privacy interests. Because many local privacy laws have been recently enacted and have been implemented for a short period of time, there is not enough sufficient data to analyze whether these local laws are effectively protecting individual privacy interests.

Cybersecurity

Cities should have robust cybersecurity infrastructures set in place to guard themselves from hackers. When cities suffer a compromise in their interconnected IT systems, cities should be transparent to the public about what occurred, whether any data had been impermissibly accessed or transferred to a third party, and ways in which the city is addressing these vulnerabilities. One example of poor practice is the city of Atlanta's handling of a ransomware attack that led to a destabilization of the city's operations. In March 2018, a ransomware attack shut down the city of Atlanta's online systems and services, such as water requests, online bill payment, validation of warrants, and inmate processing, for more than a week.[56] A January 2018 IT audit report found that the city of Atlanta's network had 1,500-2,000 security vulnerabilities,

---

continue to record location information despite users "turning off" location history settings). Finally, residents may not be able to "opt-out" of their city data collection practices by moving out of the city due to significant financial, economic, and social costs associated with relocating. *See* Charles M. Tiebout, *A Pure Theory of Local Expenditures*, 64 J. Pol. Econ. 416, 418 (1956) (conceptualizing that citizens "vote with their feet"— by moving to, or out of, a jurisdiction—to convey their preferences and satisfaction regarding public policy decisions).

[56] Alan Blinder & Nicole Perlroth, *A Cyberattack Hobbles Atlanta, and Security Experts Shudder*, N.Y. Times (Mar. 27, 2018), https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.

and there was no evidence that the city had mitigated the underlying issue for at least a year.[57] The city failed the security compliance assessment because its Information Security Management System had gaps, such as a "lack of formal processes to identify, assess, and mitigate risks."[58] Atlanta city officials kept the public in the dark about specifics of the attack for months and blamed the attack, in part, on lack of resources.[59]

Collection Limitations

The best practice cities engage in when collecting data is to collect only the data needed to fulfill the objective and not exploit the data for secondary uses. Data not collected cannot be compromised. Both Seattle and New York City are leaders in developing privacy guidelines governing smart city technology, with both cities appointing Chief Privacy Officers and enacting laws that govern all municipal data collection.[60] In Seattle, the city will only use information as necessary to complete the "limit[ed] information use . . . purpose stated at the time of collection."[61] Seattle also provides that individuals may request that the city delete information collect from an individual, absent legitimate reason to retain the information.[62] When obtaining surveillance technology, any Seattle city department must obtain approval from the Seattle City

[57] City Auditor's Office, City of Atlanta, 17.06, Compliance Audit: ISO/IEC 27001 ISMS Precertification Audit Performed by Experis U.S., Inc. 10 (2018), http://www.atlaudit.org/uploads/3/9/5/8/39584481/2017_iso-iec_27001_isms_precertification_audit_-_january_2018.pdf.
[58] *Id.*
[59] *See* Lily Hay Newman, *The Ransomware that Hobbled Atlanta Will Strike Again*, Wired (Mar. 30, 2018), https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/.
[60] Ira Rubeinstein, *Privacy Localism*, 93 Wash. L. Rev. 1961, 1996 (2018), http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1853/93WLR1961.pdf.
[61] Saad Bashir, *About the Privacy Program: Using Your Information*, Seattle.gov, https://www.seattle.gov/tech/initiatives/privacy/about-the-privacy-program#usingyourinformation.
[62] Saad Bashir, *About the Privacy Program: Retention*, Seattle.gov, https://www.seattle.gov/tech/initiatives/privacy/about-the-privacy-program#retention.

Council.[63] Last year, both Oakland[64] and Santa Clara County, California[65] passed strong surveillance technology measures similar to Seattle. Similarly, New York City's Internet of Things privacy and transparency guidelines regulate the city's collection, use, disclosure, and retention of personal data. The privacy guidelines delineate that "IoT data should only be collected, transmitted, processed, and used for specified, explicit and legitimate purposes."[66] Despite having a good policy model, N.Y.C. Admin. Code Section 26-2101-5 requires home-sharing services to report monthly rental transactions to N.Y.C. Mayor's Office of Special Enforcement ("OSE"). As described in the previous section, a district court judge blocked this new law that would have expanded the city's ability to comb through Airbnb and other home-sharing platform's users' personal data and invade their expectation of privacy.

Data Disclosure Practices

Data should not be disclosed to private corporations without limitations set in place. Data disclosed to law enforcement agencies should also be limited for a specific purpose. A 2017 survey from the National League of Cities found that 79% of cities surveyed stated that they would be open to a partnership with a sharing economy company like Uber, Lyft, or Airbnb.[67] These partnerships would include arrangements to disclose data.

Several cities have different approaches to data dissemination. New York City's IoT privacy and transparency guidelines delineate that, "[b]efore any sensitive, private, or

[63] Seattle, Wash., Ordinance 125376 (Aug. 2, 2017) (codified at Seattle, Wash. Mun. Code § 14.18).
[64] Cyrus Farivar, *Oakland Passes "Strongest" Surveillance Oversight Law in US*, Ars Technica (May 3, 2018), https://arstechnica.com/tech-policy/2018/05/oakland-passes-strongest-surveillance-oversight-law-in-us.
[65] Kevin Forestieri, *Santa Clara County Cracks Down on Police Surveillance Technology: New Law Aims to Increase Transparency and Public Control over Police Tech*, Palo Alto Online (June 20, 2016), https://arstechnica.com/tech-policy/2018/05/oakland-passes-strongest-surveillance-oversight-law-in-us.
[66] Mayor's Off. of the Chief Tech. Officer, N.Y.C., *Guidelines for the Internet of Things: Privacy & Transparency*, https://iot.cityofnewyork.us/privacy-and-transparency.
[67] Nicole DuPuis & Brooks Rainwater, Nat'l League of Cities, Cities and the Innovation Economy: Perceptions of Local Leaders 2 (2017), https://www.nlc.org/sites/default/files/2017-11/NLC_CitiesInnovationEconomy_pages%5B1%5D.pdf.

confidential data is shared outside the originating City agency, the agency should ensure that [a] need cannot be met by using anonymized or aggregated data and that the appropriate protections are in place to preserve the confidentiality of the data."[68] Chicago's Array of Things ("AoT") Privacy Policy delineates that AoT sensors cannot capture sensitive PII; however, captured non-sensitive PII will not be publicly disclosed—but even for this data government employees, contractors, and researchers who can access the information are bound by confidentiality agreements.[69] Seattle states that it does not sell personal information to third-parties for marketing or commercial use.[70] Although Seattle does share collected data, it requires partners and vendors to follow the city's privacy requirements, which are consistent with federal and state laws regarding disclosure.[71]

Machine Learning and Algorithmic Fairness

With the rise of artificial intelligence and the increasing impact of computer-aided decision-making on individuals, EPIC established the Universal Guidelines for Artificial Intelligence,[72] endorsed by over 250 experts and 60 organizations in 40 countries.[73] The guidelines highlight the necessity of transparency, accuracy, and fairness for AI systems. Cities should adopt these universal guidelines when implementing AI technology to ensure algorithmic fairness.

---

[68] N.Y.C., *Guidelines for the Internet of Things: Privacy + Transparency*, https://iot.cityofnewyork.us/privacy-and-transparency.
[69] Array of Things, Array of Things Operating Policies (Aug. 15, 2016), https://arrayofthings.github.io/final-policies.html.
[70] Saad Bashir, *About the Privacy Program: Sharing Your Information*, Seattle.gov, https://www.seattle.gov/tech/initiatives/privacy/about-the-privacy-program#sharingyourinformation.
[71] City of Seattle, *Privacy Principles*, https://www.seattle.gov/Documents/Departments/InformationTechnology/City-of-Seattle-Privacy-Principles-FINAL.pdf.
[72] The Public Voice, *Universal Guidelines for Artificial Intelligence* (Oct. 23, 2018), https://thepublicvoice.org/ai-universal-guidelines.
[73] The Public Voice, *Universal Guidelines for Artificial Intelligence: Endorsement*, https://thepublicvoice.org/AI-universal-guidelines/endorsement.

New York City's IoT Data Management guidelines prescribe that all data sets "should be checked for geographic, social or system-driven bias (e.g., geographic differences in civic engagement) and other quality problems" and instructs that biasing factors be recorded and provided with the data set. If possible, bias should be corrected.[74] New York City, however, does not require that these algorithms be published and places the responsibility to address bias on the company.

Chicago applies an algorithm to predict gun violence in the city, but the algorithm is not publicly available. Chicago's "Strategic Subject List" uses an algorithm to rank the probability that an individual will be involved in a shooting, either as victim or perpetrator. A version of the list is available through its open data portal. The underlying algorithm assesses eight attributes:

> [The] number of times being the victim of a shooting incident, age during the latest arrest, number of times being the victim of aggravated battery or assault, number of prior arrests for violent offenses, gang affiliation, number of prior narcotic arrests, trend in recent criminal activity, and number of prior unlawful use of weapon arrests.[75]

The assigned risk scores associated with the algorithm, however, have been found to be at odds with the Chicago Policy Department's public statements and its effectiveness is far from clear.[76]

Transparency and Accountability

Cities must be transparent with their data collection and data disclosure practices and must be accountable for any infringement on the privacy interests of the individual.

---

[74] N.Y.C., *Guidelines for the Internet of Things: Data Management*, https://iot.cityofnewyork.us/data-management.
[75] Chicago, *Data Portal: Strategic Subject List* (Dec. 7, 2017), https://data.cityofchicago.org/Public-Safety/Strategic-Subject-List/4aki-r3np.
[76] Jeff Asher & Rob Arthur, *Inside the Algorithm That Tries to Predict Gun Violence in Chicago*, N.Y. Times (June 13, 2017), https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html.

In 2017, New York City unanimously passed a bill to establish a task force to examine the city's "automated decision systems" and to issue a report of its findings in December 2019.[77] The task force, however, cannot perform proper oversight because it must rely on voluntary disclosures from agencies.[78] The bill also does not address how the city can exercise power over the companies who create these automated decision systems. The final bill deviated from the original draft language that ambitiously proposed that whenever a city agency would use algorithms to make decisions, the source code must be available to the public and the algorithm's simulation must use data submitted by New Yorkers.[79] The city resisted an attempt at algorithmic transparency in favor of protecting alleged proprietary information.[80]

Several smart cities require that all public data sets be available and accessible to the public on a single web portal. Having open data portals make it easier for the public to gain information about cities and scrutinize the activities of the government. Cities such as Chicago,[81] San Francisco,[82] and New York City[83] have open data laws. New York City also releases an annual report highlighting various open datasets and explains why specific open data reports were removed from the NYC Open Data portal.[84]

---

[77] Press Release, N.Y.C., Mayor de Blasio Announces First-in-Nation Task Force to Examine Automated Decision Systems Used by the City (May 16, 2018), https://www1.nyc.gov/office-of-the-mayor/news/251-18/mayor-de-blasio-first-in-nation-task-force-examine-automated-decision-systems-used-by.
[78] *See* Julia Powles, *New York City's Bold, Flawed Attempt to Make Algorithms Accountable*, New Yorker (Dec. 20, 2017), https://www.newyorker.com/tech/annals-of-technology/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable.
[79] *Id.*
[80] *Id.*
[81] Chicago, Ill., Open Data Exec. Order No. 2012-2 (2012).
[82] S.F., Cal., Ordinance 285-13 (Jan. 25, 2014) (Codified at S.F., Cal., Admin. Code §§ 22D.1, 22D.2, and 22D.3).
[83] N.Y.C., N.Y., Local Law 11-2012 (Mar. 7, 2012) (Codified at N.Y.C., N.Y., Admin. Code § 23-503).
[84] *See* N.Y.C. Open Data, *Laws and Reports*, https://opendata.cityofnewyork.us/open-data-law.

Citizen Engagement

To implement effective smart city initiatives, cities must consult with residents prior to the implementation of any initiative and take constructive criticism seriously. For instance, Oakland passed Ordinance No. 13349 prescribing that public input and opinion should be considered by the Privacy Advisory Commission before funding, purchasing, acquiring, or using surveillance technology.[85]

Residents should also have rights over their personal data and information inferred or predicted from the collection of their data. Amsterdam, for example, has a number of efforts to increase understanding and put control of data back in residents' hands. The Amsterdam Economic Board launched a campaign called "Tada!" where a universal label is placed on something to indicate that this technology, product, or event incorporates six principles of a manifesto that highlight concepts of inclusion, transparency, and ethical data use.[86] Amsterdam and other partners launched DECODE as an experimental project to give people the power to take control of their personal data by developing alternatives to manage and share data while taking account of privacy protections.[87]

IV. Conclusion

The vast collection of data allows cities the opportunity to be data stewards when designing privacy norms and standards for new technology. Cities bear the responsibility to protect the privacy interests of their residents and to include their residents in the decision-making process. The City of New York took an important step toward protecting privacy by enacting Local Laws 245 and 247. Now, the newly-created Mayor's Office of Information Privacy has the opportunity to make that step meaningful. The Citywide Privacy Protection

[85] Oakland, Cal., Ordinance 13,349 (Jan. 19, 2016).
[86] *See* Tada, https://tada.city/en/home-en.
[87] *See* DECODE, https://decodeproject.eu.

Policies must be written with the risks of data breach and the potential for bias in automated decision-making in mind. Further, the Office must incorporate minimization of data collection, de-identification of aggregated data, limitations on retention, restrictions on use, and controls over disclosure. Lastly, the Office should require frequent reporting, offer meaningful opportunities for redress, and continuously reassess the policies to keep current with advances in technology.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Jeramie D. Scott
Jeramie D. Scott
EPIC Senior Counsel

/s/ Enid Zhou
Enid Zhou
EPIC Open Government Counsel

/s/ Ellen Coogan
Ellen Coogan
EPIC Domestic Surveillance Fellow

/s/ Daniel de Zayas
Daniel de Zayas
EPIC Clerk