7

Smart Cities: Privacy, Transparency, and Community

*Kelsey Finch and Omer Tene**

INTRODUCTION

At the beginning of the 20th century, a group of Italian artists and poets called the Futurists sought to reshape the world around them to reflect a futuristic, technological aesthetic – transforming everything from cities, to train stations, to chess sets.[1] In the city of the future, they believed, technology would inspire and elevate the physical and mental world: "Trains would rocket across overhead rails, airplanes would dive from the sky to land on the roof, and skyscrapers would stretch their sinewed limbs into the heavens to feel the hot pulse of radio waves beating across the planet."[2]

But today's cities – and our train stations, self-driving cars, and chess sets – have moved far beyond artistic imagination. Today's cities are already pervaded by growing networks of connected technologies to generate actionable, often real-time data about themselves and their citizens. Relying on ubiquitous telecommunications technologies to provide connectivity to sensor networks and set actuation devices into operation, smart cities routinely collect information on cities' air quality, temperature, noise, street and pedestrian traffic, parking capacity, distribution of government services, emergency situations, and crowd sentiments, among other data points.[3]

While some of the data sought by smart cities and smart communities is focused on environmental or non-human factors (e.g., monitoring air pollution, or snowfall, or electrical outages), much of the data will also record and reflect the daily activities of the people living, working, and visiting the city (e.g., monitoring tourist foot traffic, or home energy usage, or homelessness). The more connected a city becomes, the more it will generate a steady stream of data from and about 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

* Kelsey Finch is Policy Counsel and Omer Tene is Senior Fellow at the Future of Privacy Forum. Tene is Vice President of Research and Education at the International Association of Privacy Professionals and Associate Professor at the College of Management School of Law, Rishon Lezion, Israel.

[1] *See* Adam Rothstein, *The Cities Science Fiction Built*, Motherboard (Apr. 20, 2015), https://motherboard.vice.com/read/the-cities-science-fiction-built; Italian Futurism, 1909–1944: Reconstructing the Universe (Vivian Greene, ed., 2014).

[2] Adam Rothstein, *The Cities Science Fiction Built*, Motherboard (Apr. 20, 2015), https://motherboard.vice.com/read/the-cities-science-fiction-built ("This artistic, but unbridled enthusiasm was the last century's first expression of wholesale tech optimism.").

[3] *See Shedding Light on Smart City Privacy*, The Future of Privacy Forum (Mar. 30, 2017), https://fpf.org/2017/03/30/smart-cities/.

more sustainable, more livable, and more equitable.[4] At the same time, connected smart city devices raise concerns about individuals' privacy, autonomy, freedom of choice, and potential discrimination by institutions. As we have previously described, "There is a real risk that, rather than standing as 'paragons of democracy, [smart cities] could turn into electronic panopticons in which everybody is constantly watched."[5] Moreover, municipal governments seeking to protect privacy while still implementing smart technologies must navigate highly variable regulatory regimes,[6] complex business relationships with technology vendors, and shifting societal – and community – norms around technology, surveillance, public safety, public resources, openness, efficiency, and equity.

Given these significant and yet competing benefits and risks, and the already rapid adoption of smart city technologies around the globe,[7] the question becomes: How can communities leverage the benefits of a data-rich society while minimizing threats to individuals' privacy and civil liberties?

Just as there are many methods and metrics to assess a smart city's livability, sustainability, or effectiveness,[8] so too there are different lenses through which cities can evaluate their privacy preparedness. In this article, we lay out three such perspectives, considering a smart city's privacy responsibilities in the context of its role as a data steward, as a data platform, and as a government authority. While there are likely many other lenses that could be used to capture a community's holistic privacy impacts, exploring these three widely tested perspectives can help municipalities better leverage existing privacy tools and safeguards and identify gaps in their existing frameworks. By considering the deployment of smart city technologies in these three lights, communities will be better prepared to reassure residents of smart cities that their rights will be respected and their data protected.

CITY AS DATA STEWARD

In many ways, smart communities are no different than other data-rich entities: they act as a data stewards, ensuring that data is always available, reliable, and useful to their organization. Data stewardship is well established in the information management field, denoting an individual or institution with control over the collection, handling, sharing, and analysis of data.[9] Increasingly, data governance in data-rich organizations concerns not only carrying out the day-to-day management of data assets, but also taking on fiduciary-like responsibilities to consider the

[4] *See, e.g., Smart Cities: International Case Studies*, Inter-Am. Dev. Bank, (2016), http://www.iadb.org/en/topics/emerging-and-sustainable-cities/international-case-studies-of-smart-cities,20271.html (last visited Mar. 31, 2017).

[5] Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 Fordham Urb. L.J. 1581, 1583 (2015), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2549&context=ulj.

[6] Including regulatory regimes and principles that create sometimes competing obligations to keep personal data private while also making the data held by government more transparent and accessible to the public. *See, e.g., Report of the Special Rapporteur on the Right to Privacy, Annex II*, Human Rights Council, U.N. Doc. A/HRC/31/64 (May 8, 2016) (by Joseph A. Cannataci).

[7] *See* Research & Markets, Global Smart Cities Market Insights, Opportunity Analysis, Market Shares and Forecast 2017–2023 (Jan. 2017).

[8] *See* ISO 37120:2014 Sustainable development in communities: City Indicators for Service Delivery and Quality of Life (2014), https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/37120_briefing_note.pdf.

[9] *See* Mark Moseley, *DAMA_DBOK Functional Framework*, The Data Mgmt. Ass'n. (Version 3.02, Sept. 10, 2008), https://www.dama.org/sites/default/files/download/DAMA-DMBOK_Functional_Framework_v3_02_20080910.pdf.

ethical and privacy impacts of particular data activities and to act with the best interests of individuals and society in mind.[10]

All organizations dealing with data must ensure that their data assets are appropriately secured, handled, and used. While privacy laws and commitments give organizations in both the private and public sectors clear motivations to protect personally identifying information (PII), non-personal data is oftentimes just as robustly safeguarded because of concerns for intellectual property and trade secrets. While this paper focuses on methods designed to protect PII, data governance and accountability mechanisms instituted throughout the data lifecycle often mitigate risks to both PII and non-PII.[11]

Companies, NGOs, and government agencies of all stripes are familiar to some extent with the variety of roles and responsibilities that accompany the day-to-day use and maintenance of data assets and that keep systems running smoothly: IT departments ensure that data is secure and uncorrupted, lawyers oversee compliance with privacy and other legal regimes, engineers architect new and better ways of developing data, researchers explore datasets for new insights, and business units and policy teams determine what data to collect and how to use it. In the municipal context, oftentimes it is a chief innovation officer (CIO), a chief technology officer (CTO), a chief data officer (CDO), or increasingly a chief privacy officer (CPO) who oversees this process and inculcates institutional norms around privacy and security.

Thus, the data steward model – and many of the data (and privacy) governance tools and terminology that accompany it – is already familiar to a wide set of IT, compliance, and privacy professionals in the private sector.[12] It is also familiar to career civil servants in public sector entities – especially data-intensive environments such as national security, healthcare and education.[13] As municipalities expand their technology and data capabilities, many of the professionals they hire will bring with them experience with data and privacy governance. Nevertheless, municipalities need to be forward-thinking and purposeful in planning, supervising, and controlling data management and use within – and between – their numerous departments, agencies, and public-private partnerships.

What tools and considerations, then, should smart cities take into account in their role as data stewards?

Privacy management. As data stewards, cities must devise privacy management programs to ensure that responsibility is established, accountability is maintained, and resources are allocated to successfully oversee, govern, and use individuals' data. Documenting and routinizing these principles and practices throughout the entire data lifecycle are critical to ensuring accountability.

[10] *See* Jan Whittington et al., *Push, Pull, and Spill: A Transdisciplinary Case Study in Municipal Open Government*, 30 (3) Berkeley Tech. L.J. 1989 (2015), http://btlj.org/data/articles2015/vol30/30_3/1899–1966%20Whittington.pdf; Jack Balkin & Jonathan Zittrin, *A Grand Bargain to Make Tech Companies Trustworthy*, The Atlantic (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/.

[11] We note, as well, that the line between PII and non-PII is often indistinct, and that data traditionally considered non-identifying may become PII in the future as look-up databases or technical systems emerge to link that data to individuals. *See* Jules Polonetsky, Omer Tene & Kelsey Finch, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 Santa Clara L. Rev. 593 (2016), http://digitalcommons.law.scu.edu/lawreview/vol56/iss3/3. Given these risks, instituting a variety of forward-thinking safeguards throughout the full data lifecycle is critical.

[12] *See, e.g.*, Moseley, *supra* note 9.

[13] *See, e.g.*, Susan Baird Kanaan & Justine M. Carr, *Health Data Stewardship: What, Why, Who, How*, Nat'l Comm. on Vital & Health Statistics, U.S. Dep't of Health & Human Svcs. (Sept. 2009), http://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/090930lt.pdf; *Data Governance and Stewardship*, Privacy Technical Assistance Ctr., U.S. Dep't of Educ. (Dec. 2011), http://ptac.ed.gov/sites/default/files/issue-brief-data-governance-and-stewardship.pdf.

The core of any privacy management program is establishing principles and practices that apply to collecting, viewing, storing, sharing, aggregating, analyzing, and using personal data. In order to strengthen public trust, some city leaders have used the process of developing core privacy principles as an opportunity to engage their communities. For example, as the City of Seattle developed its six citywide "Privacy Principles,"[14] the Seattle IT department created a Community Technology Advisory Board (CTAB), made up of local experts, business representatives, and academics from the University of Washington,[15] and invited their input, as well as that of local privacy advocacy groups.[16] The principles were ultimately adopted by City Council Resolution 31570,[17] and laid the foundation for a more in-depth, public-facing privacy policy detailing the city's privacy and security practices.[18]

Once their guiding principles are established, there are many models that city officials might turn to in building workable, auditable municipal privacy programs. In 2016, the Federal Office of Management and Budget (OMB) updated Circular A-130, the document governing the management of federal information resources.[19] Recognizing the impact of big data trends on government data management, the updated OMB Circular requires federal agencies to:

- Establish comprehensive, strategic, agency-wide privacy programs;
- Designate Senior Agency Officials for Privacy;
- Manage and train an effective privacy workforce;
- Conduct Privacy Impact Assessments (PIA);
- Apply NIST's Risk Management Framework to manage privacy risk throughout the information system development life cycle;
- Use Fair Information Practice Principles (FIPPs) when evaluating programs that affect privacy;
- Maintain inventories of personally identifiable information (PII); and
- Minimize the collection and usage of PII within agencies.[20]

Another leading example in the United States has emerged from the Federal Trade Commission's (FTC) body of privacy and security settlements. The FTC's model is likely to influence many of the technology vendors a city might partner with, who are expected to stay in line with their primary regulator's best practices or may be already under a settlement order themselves.[21] In broad strokes, the FTC has increasingly required settling companies to maintain a privacy program that:

[14] *See City of Seattle Privacy Principles*, City of Seattle (Mar. 2015), http://ctab.seattle.gov/wp-content/uploads/2015/03/Privacy-Principles-FINAL-RESOLUTION.pdf.

[15] *See CTAB Blog*, City of Seattle, http://ctab.seattle.gov/ (last visited Apr. 24, 2017).

[16] *See City of Seattle's Tech Board Restarts Privacy Committee*, Seattle Privacy Coal. (Sept. 27, 2016), https://www.seattleprivacy.org/city-of-seattles-tech-board-restarts-privacy-committee/.

[17] *See* Res. 31570, *A resolution adopting the City of Seattle Privacy Principles governing the City's operations, which will provide an ethical framework for dealing with current and future technologies that impact privacy, and setting timelines for future reporting on the development of a Privacy Statement and Privacy Toolkit for their implementation*, Seattle City Council (Mar. 3, 2015), http://clerk.seattle.gov/~legislativeItems/Resolutions/Resn_31570.pdf.

[18] *See Privacy*, City of Seattle, http://www.seattle.gov/tech/initiatives/privacy#x58255 (last visited Apr. 24, 2017).

[19] *See* Revision of OMB Circular A-130, "Managing Information as a Strategic Resource," FR Doc. 2016–17872 (July 28, 2016), https://obamawhitehouse.archives.gov/blog/2016/07/26/managing-federal-information-strategic-resource.

[20] *See* Circular No. A-130, *Managing Information as a Strategic Resource*, Appendix II, Office of Mgmt. & Budget, Exec. Office of the President (July 28, 2016), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[21] *See* Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.

- Is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) to protect the privacy and confidentiality of personal information;
- Is fully documented in writing;
- Contains privacy controls and procedures appropriate to the organization's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information;
- Designates an employee or employees to coordinate and be accountable for the privacy program;
- Conducts a privacy risk assessment identifying reasonably foreseeable, material risks, both internal and external, that could result in the organization's unauthorized collection, use, or disclosure of personal information – specifically including risks related to employee training and management and product design, development, and research;
- Implements reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, and regularly tests or monitors their effectiveness;
- Takes reasonable steps to select and retain service providers capable of maintaining appropriate security practices, and requires service providers to contractually implement appropriate safeguards; and
- Reevaluates and adjusts the privacy program in light of any new material risks, material changes in the organization's operations or business arrangements, or any other circumstances that might materially impact the effectiveness of the privacy program.[22]

International standards and regulations add clarity on the importance of robust privacy programs. The OECD's 1980 privacy guidelines, amended in 2013, dictate that data controllers should "Have in place a privacy management programme that:

- Gives effect to these Guidelines for all personal data under its control;
- Is tailored to the structure, scale, volume and sensitivity of its operations;
- Provides for appropriate safeguards based on privacy risk assessment;
- Is integrated into its governance structure and establishes internal oversight mechanisms;
- Includes plans for responding to inquiries and incidents; [and]
- Is updated in light of ongoing monitoring and periodic assessment."[23]

The new European General Data Protection Regulation (GDPR), which goes into force in May 2018, will also require the appointment of Data Protection Officers within organizations of all shapes and sizes, and the establishment of structured accountability programs.[24] Indeed, the Article 29 Working Party believes that "the DPO is a cornerstone of accountability."[25] DPOs are at a minimum tasked with monitoring their organizations' compliance with the GDPR; advising their organizations in the course of conducting data protection impact assessments (DPIAs); taking risk-based approaches to their data protection activities; and maintaining records of all of their organizations' data processing operations.[26] While uncertainty remains as to the precise

[22] *See id.* at 617.

[23] *See OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, The OECD Privacy Framework, 16 (July 11, 2013), https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

[24] *See* Regulation 2016/679, General Data Protection Regulation, art. 37, 2016 O.J. (L. 119) 1, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf; Art. 29 Data Protection Working Party, Guidelines on Data Protection Officers (Dec. 13, 2016), http://ec.europa.eu/information_society/newsroom/image/document/2016–51/wp243_en_40855.pdf.

[25] Art. 29 Working Party, *supra* note 24, at 4.

[26] *Id.* at 16–18.

contours of the DPO role within EU data protection practice, the International Association of Privacy Professionals (IAPP) estimates that at least 28,000 new DPO positions will be created in the coming years in Europe alone in response to the GDPR.[27]

Privacy oversight. Designating a governance lead (such as a Chief Privacy Officer, a DPO or a Senior Agency Official for Privacy[28]) who oversees privacy responsibilities can create an authoritative hub where dedicated experts navigate relevant laws and regulations, advise other officials and departments, create documentation and policies, look for and remediate violations, and educate the public workforce on privacy policies and practices. As data stewards, smart cities should clearly establish governance structures and oversight mechanisms for granting access to data, analytics, and tracking technologies.

In addition to designating a privacy lead, smart cities should consider the value of establishing a privacy committee made up of a range of stakeholders, including members of the public. Such working groups are common within the privacy profession, and often stress interdisciplinary representation within the working groups to improve outcomes, make programs more inclusive, and generate buy-in throughout an organization.[29] Seattle's Community Technical Advisory Board is formalized in the Seattle Municipal Code,[30] and in January 2016 the Oakland City Council created and defined the duties of a formal Privacy Advisory Commission, tasked with (among other things): providing advice and technical assistance on privacy best practices for surveillance equipment and citizen data, providing annual reports and recommendations on the city's use of surveillance equipment, conducting public hearings, drafting reports, and making findings and recommendations to the city council.[31]

While only Seattle and Oakland have established formal citywide privacy advisory boards at this date, specific agencies within local government have also turned to their communities for input – local libraries, for instance, have long been on the forefront of progressive citizen-engaged privacy policymaking.[32] And the original Array of Things installation in Chicago, a partnership between the City of Chicago, the University of Chicago, and the Argonne National Laboratory, has convened independent governance boards responsible for overseeing the privacy and security practices of its distributed sensor arrays and data processing activities.[33]

Privacy Risk Management. Robust data governance requires identifying, assessing, and ultimately mitigating privacy risks. While many organizations have their own internal risk management structures, privacy-specific frameworks are less systematic and, given the largely subjective nature of privacy harms, more difficult to quantify.[34] One instructive risk management framework for municipal officials to consider is a recent effort by the US National Institute

[27] *See* Warwick Ashford, *GDPR Will Require 28,000 DPOs in Europe and US, Study Shows*, Computer Weekly (Apr. 20, 2016), http://www.computerweekly.com/news/450283253/GDPR-will-require-28000-DPOs-in-Europe-study-shows.

[28] *See* Office of Mgmt. & Budget, *supra* note 20.

[29] *See* IAPP-EY Annual Privacy Governance Report 7 (2015), https://webforms.ey.com/Publication/vwLUAssets/EY_-_IAPP_ey_privacy_governance_report_2015/$FILE/EY-IAPP-ey-privacy-governance-report-2015.pdf.

[30] Seattle Community Technology Advisory Board (CTAB) – Membership and duties, Seattle Municipal Code 3.23.060, https://www.municode.com/library/wa/seattle/codes/municipal_code?nodeId=TIT3AD_SUBTITLE_IIDEOF_CH3.23SEINTEDE_3.23.060SECOTEADBOCTEMDU (last visited Apr. 24, 2017).

[31] *Privacy Advisory Commission*, City of Oakland, http://www2.oaklandnet.com/government/o/CityAdministration/d/PrivacyAdvisoryCommission/index.htm (last visited Apr. 24, 2017).

[32] *See, e.g.*, San Francisco Pub. Library Tech. & Privacy Advisory Comm., Summary Report: Radio Frequency Identification and the San Francisco Public Library (Oct. 2005), http://sfpl.org/pdf/about/commission/RFID-and-SFPL-summary-report-oct2005.pdf.

[33] *See* Array of Things Operating Policies (Aug. 15, 2016), https://arrayofthings.github.io/final-policies.html.

[34] *See* NIST Internal Report (NISTIR) 8062, Privacy Risk Management for Federal Information Systems 1 (Jan. 4, 2017), http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf ("Although existing tools such as the Fair Information Practice Principles (FIPPs) and privacy impact assessments (PIAs) provide a foundation for taking

of Standards and Technology (NIST) to develop a comprehensive system for "Privacy Risk Management for Federal Information Systems."[35] NIST explicitly modeled this effort on its successful cybersecurity risk management framework (RMF) and accompanied the development of a privacy risk model with a foundation for "the establishment of a common vocabulary to facilitate better understanding of – and communication about – privacy risks and the effective implementation of privacy principles in federal information systems."[36]

A recurring challenge for smart communities in deploying risk mitigation strategies is that reducing privacy risk often entails impairing data utility, thus inhibiting potentially beneficial uses of data. For smart communities and other organizations, considering the *risks* of a project is merely one part of a balanced value equation; decision-makers must also take into count the project's *benefits* in order to make a final determination about whether to proceed.[37] In another article, we suggested that in addition to conducting a Privacy Impact Analysis (PIA), therefore, decision-makers need to conduct a Data Benefit Analysis (DBA), putting a project's benefits and risks on an equal footing.[38] This is especially true as cities, researchers, companies, and even citizens engage in the sort of big data analyses that promise tremendous – and often unexpected – benefits, but which also introduce new privacy and civil liberties concerns associated with large-scale data collection and analysis. On the one hand, if a city can provide free internet access for thousands of un- or underserved individuals, for example, it may be legitimate to deploy such a service even though not all of its privacy risks can be completely eliminated.[39] On the other hand, where smart city benefits are small or remote, larger privacy risks would not be justified.[40]

These assessments should take into account variables such as the nature of the prospective risk or benefit, the identity of the impacted subject(s), and the likelihood of success. These assessments should consider and document specific impacts to individuals, communities, organizations, and society at large, in part to help determine whether risks and benefits are accruing fairly and equitably across these populations.[41] Cities must also negotiate the difficult reality that social and cultural priorities and sensitivities may vary widely among their constituent communities, and ensure that all interested members of the public can legitimately have their voices heard on the potential impacts of civic projects.[42]

Vendor management. Public-private partnerships have also emerged as a leading driver for smart city developments. Rather than simply outsourcing technical work to service providers, cities are increasingly co-organizing, co-operating, co-funding, and co-branding data intensive projects with private enterprises.[43] In such high profile relationships, cities (and vendors) must

privacy into consideration, they have not yet provided a method for federal agencies to measure privacy impacts on a consistent and repeatable basis.").

[35] *Id.*

[36] *Id.* at 3.

[37] Jules Polonetsky, Omer Tene & Joseph Jerome, Benefit-Risk Analysis for Big Data Projects 1 (Sept. 2014), https://fpf.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf [hereinafter "DBA"].

[38] *Id.*

[39] *See, e.g.*, Eillie Anzilotti, *To Court a Skeptical Public, New York Sends Wi-Fi Ambassadors*, CityLab (Aug. 12, 2016), http://www.citylab.com/navigator/2016/08/to-court-a-skeptical-public-new-york-sends-wi-fi-ambassadors/495623/.

[40] *See* DBA, *supra* note 37, at 4.

[41] *Id.* at 9.

[42] *Id.* at 7 ("For example, the relative value of a health or national security benefit may differ from society to society. Some societies may place a high value on individual benefits, while others give greater weight to community values.").

[43] *See* Inter-Sessional Panel on "Smart Cities and Infrastructure" and "Foresight for Digital Development," U.N. Conference on Trade & Dev. (Jan. 11–13, 2016), http://unctad.org/meetings/en/Presentation/CSTD_2015_ppt07_Bufi_en.pdf; *PPP for Cities Case Studies Quick Facts and PPP Learned Lessons*, Specialist Centre on PPP in Smart and Sustainable Cities (Nov. 17, 2016), http://www.pppcities.org/wp-content/uploads/2016/11/7.-PPP-for-Cities.pdf.

do their due diligence and clearly delineate each party's responsibilities (and capacities) for managing, using, sharing, securing, or destroying data; for communicating with the public about privacy; and for supervising other contractors or subcontractors.

Even when initiating projects on their own, smart cities rely extensively on vendors, particularly in deploying, maintaining, and analyzing emerging data tools and technologies (including procuring Internet of Things devices, maintaining sensor networks, and publishing open data to platforms). As scholars have noted, "Vendors have different capabilities and incentives than a municipal government; they may be more or less capable of keeping data secure, and are not likely to be as responsive to residents as their city government ... [and] stakeholders will ultimately hold cities responsible as stewards and expect them to uphold constituent values."[44]

An instructive example of how the dynamics between public sector agencies and technology vendors can lead to gaps in individual privacy protection was presented in a study by the Center for Law and Information Policy at Fordham Law School. In the study, researchers analyzed contracts between US public schools and cloud computing service providers and found that "only 25% of districts inform parents of their use of cloud services, 20% of districts fail to have policies governing the use of online services, and a sizeable plurality of districts have rampant gaps in their contract documentation, including missing privacy policies."[45] Their findings showed that vendors often produced commercial boilerplate contracts that did not adequately address the student data context[46]; that school districts lacked knowledgeable privacy officers and staff; and that each party to a transaction expected that the other would raise any relevant privacy and security concerns.[47] These findings – and the fierce public backlash that ensued – should serve as a warning sign for other smart community services, which leverage private sector vendor technologies and business models but could create or exacerbate privacy risks.

Standard contract terms, such as data use limitations, data ownership, data security policies, confidentiality statements, and commitments not to reidentify data are crucial tools for ensuring individuals' privacy in multilayered smart city ecosystems. Given that the technologies and data analysis and management tools required for smart city operations typically are sold or managed by third-party service providers, it is essential that city leaders carefully select, engage, and supervise their vendors. It is also essential that privacy and security obligations flow with the data, binding subcontractors to equivalent protections throughout the data lifecycle. City leaders must continue to regularly monitor, assess, and audit whether service providers and other partners continue to adhere to contracts and agreed-upon practices.

Another reason that city leaders must be forward thinking in selecting and contracting with their service providers is that – unlike dispersed public schools – cities are "market makers, not market takers."[48] Cities wield significant purchasing power, and by requiring commitments around privacy and security in their deals with vendors they can effectively set nationwide industry standards. Best practices and standard contractual clauses at the largest companies can then have a trickle-down effect. This is particularly true as cities turn to start-ups and smaller

[44] *See* Whittington et al., *supra* note 10, at 1947.

[45] *See* Joel Reidenberg et al., *Privacy and Cloud Computing in Public Schools*, Fordham Ctr. On L. and Info. Policy (Dec. 12, 2013), http://www.immagic.com/eLibrary/ARCHIVES/GENERAL/FRDHM_US/F131213R.pdf.

[46] For example, including terms that would violate the Federal Educational Rights and Privacy Act, the Protection of Pupil Rights Amendment, and the Children's Online Privacy Protection Act. *See id*. at 35.

[47] *Id*.

[48] *See* Whittington et al., *supra* note 10, at 1954.

organizations for their technology services, which may not have the same institutional expertise with privacy and security as large enterprise vendors.[49]

Data research and ethical reviews. Smart cities are becoming storehouses of hugely valuable information for public and private researchers. But appropriating civic data that was originally collected for another purpose without citizens' knowledge or consent raises significant privacy concerns – and weighty ethical and technical questions.

Traditionally, privacy laws have envisioned researchers utilizing de-identification to unleash the value of data while protecting privacy.[50] In recent years, however, advances in reidentification science and the increasing availability of external datasets with potentially revealing elements have led scientists and policymakers to doubt the reliability of de-identification measures to appropriately reduce the risk of an individual being reidentified from a dataset.[51] A robust scholarly debate continues unabated to this day between data scientists, researchers, lawyers, and regulators over whether and to what extent data can be scientifically or legally considered de-identified.[52]

Nevertheless, even as the debate continues to rage, communities leveraging citizens' data for additional, secondary purposes, including conducting scientific research or business analytics, must do so while respecting individuals' privacy. If consent to use data in a particular manner is not feasible to obtain, or de-identification unduly degrades the data or offers inadequate guarantees, urban data stewards must evaluate and document risk benefit assessments as part of a structured ethical review process.

In the United States, federal and federally supported institutions conducting human subject research have been governed by the Common Rule since 1991, which is itself grounded in the principles articulated by the *Belmont Report* of the 1970s. Under the Common Rule guidelines, researchers who are studying human subjects seek the informed consent of their subjects or, where that is not feasible, obtain the approval of an institutional review board composed of trained experts from diverse backgrounds who are charged with balancing the risks to individuals against the benefits of a research project. To the extent that cities accept federal funding, they are also directly subject to the Common Rule.

At the same time, the sort of big data research and analysis that municipalities and even corporate institutions increasingly are interested in have challenged existing legal and ethical frameworks, including the Common Rule. For example, the Common Rule defines a human subject as "a living individual about whom an investigator ... conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information."[53] In the age of data-focused research, however, it is unclear whether research of large datasets collected from public or semi-public sources even constitutes human subject research, as it often requires no interaction with individuals or involves data that has been de-identified or

[49] *See, e.g.*, *80+ Startups Making Cities Smarter Across Traffic, Waste, Energy, Water Usage, and More*, CB Insights (Jan. 24, 2017), https://www.cbinsights.com/blog/iot-smart-cities-market-map-company-list/; Jason Shueh, *How Startups Are Transforming the Smart City Movement*, GovTech (Sept. 1, 2015), http://www.govtech.com/How-Startups-Are-Transforming-the-Smart-City-Movement.html; Ben Miller, *3 Reasons Some Local Governments Are Eschewing Big Tech Vendors for Startups*, GovTech (Oct. 27, 2016), http://www.govtech.com/civic/3-Reasons-Some-Local-Governments-are-Eschewing-Big-Tech-Vendors-for-Startups.html.

[50] *See, e.g.*, Paul Schwartz & Dan Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 NYU L. Rev. 1814 (2011).

[51] *See* Ira Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Wash. L. Rev. 703 (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2646185.

[52] *See id.*

[53] 45 C.F.R. 46.102(f).

that was in the public domain.[54] The size and scope of the data that researchers can now access – often involving the mining of massive datasets that can be years old and gathered from around the world – also tends to render traditional "informed consent" mechanisms ineffective.[55] Furthermore, as research projects are initiated beyond traditional academic institutions, new ethical review processes and principles will continue to develop.[56] City officials who wish to enable data research should be aware of the robust and ongoing discussions within the research community about how to responsibly and ethically use data in the pursuit of knowledge.

Irrespective of the precise scope of the Common Rule, municipalities conducting data research must consider ethical review processes and benefit-risk analyses as critical parts of privacy and civil liberties protections, particularly when sensitive data or vulnerable populations are concerned. Part of the difficult calculus of data-based research is determining when the risks of using personal information in a particular way so strongly outweigh the benefits that a project becomes unethical and should not be allowed to proceed – or, conversely, when individuals must assume some risk for the greater good. Without robust ethical review processes to help researchers, data stewards, and publishers answer these questions, valuable data research results could become locked away or research projects never even started for fear of public backlash or regulatory action."[57] Cities that seek to conduct research or to enable research by others must address these difficult challenges, and should engage with researchers and ethicists to develop new approaches to ethical review and big data research.[58]

As communities begin to actively push their data out into the hands of researchers, citizens, businesses, and other civic constituencies, however, they move beyond the routine tools of enterprise data management. When they act as platforms for data inputs and outputs, smart cities must rely on additional tools to strike the right balance between protecting privacy and enabling data use for the public good.

CITY AS PLATFORM

Historically, communities have been governed by "nineteenth and twentieth-century ideas of civic organization and social norms … revolv[ing] around representative governance and centrally directed bureaucracies overseen by experts using strict, formal rules of procedure."[59] Municipal data management has followed similar trends: data was often lost in siloed, incompatible systems, inaccessible to other agencies, let alone the public. Even where data was made public, it was often buried in labyrinthine city websites, in non-searchable or cross-linkable formats.[60]

[54] Omer Tene & Jules Polonetsky, Beyond IRBs: Ethical Guidelines for Big Data Research 1 (Dec. 2015), https://bigdata.fpf.org/wp-content/uploads/2015/12/Tene-Polonetsky-Beyond-IRBs-Ethical-Guidelines-for-Data-Research1.pdf.

[55] *See id.*

[56] *See generally* Conference Proceedings: Beyond IRBs: Ethical Guidelines for Big Data Research, Future of Privacy Forum (Dec. 10, 2015), https://fpf.org/wp-content/uploads/2017/01/Beyond-IRBs-Conference-Proceedings_12–20-16.pdf.

[57] *See* Jules Polonetsky, Omer Tene & Joseph Jerome, *Beyond the Common Rule: Ethical Structures for Data Research in Non-Academic Settings*, 13 Colo. Tech. L.J. 333, 336 (2015), http://ctlj.colorado.edu/wp-content/uploads/2015/08/Polonetsky-Tene-final.pdf.

[58] *See* Matthew Zook et al., *Ten Simple Rules for Responsible Big Data Research*, PLoS Comput. Bio. 13 (2017), http://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1005399.

[59] David Bollier, *The City as Platform: How Digital Networks Are Changing Urban Life and Governance*, The Aspen Institute Commc'ns & Soc'y Program (2016), http://csreports.aspeninstitute.org/documents/CityAsPlatform.pdf.

[60] *See id.* at 8.

Today, however, technological progress is helping municipalities make a revolutionary shift. By mediating interactions between communities and their citizens, smart city technologies, apps, and datasets are helping cities position themselves not as fixed, distant decision-makers, but as vital, central platforms that support the efforts of citizens, businesses, and other organizations to play a direct role in community operations.[61] Rather than relying on "separate islands of software that don't communicate," cities are centralizing and interconnecting "all the digital functionality the city needs to serve internal operating requirements and to engage with citizens."[62] In the process, they are becoming massive data and computing platforms, controlling what can and cannot be done with data, whether data will flow in and out of the city, and how privacy and security protections will be embedded throughout its physical and digital infrastructure.

In an era in which "code is law,"[63] municipalities should embrace their roles as digital platforms and the opportunity to set norms and standards around privacy for emerging technologies. Smart cities sit at the convergence of every major technology trend: the Internet of Things, cloud computing, mobile connectivity, big data, crowdsourcing, artificial intelligence, algorithmic decision-making, and more. Just as the Apple iTunes and the Google Play platforms mediate interactions between consumers and apps,[64] municipalities are creating platforms to mediate interactions between citizens and the civic environment. Similarly to commercial platforms, too, cities have an opportunity to write their own terms of service and to embed privacy and security protections throughout their physical and digital infrastructures.

Given the political gridlock and the pace of technological advancement today, privacy policy is seldom written by lawmakers in Washington, DC, or faraway state capitols, but rather is being embedded into the deals that cities are striking with technology and analytics providers. Cities already deploy sensor networks to monitor air pollution and reduce asthma rates; they support smartphone apps to optimize bus routes (or 911 services, or snow removal, remedying potholes, or any number of things); they develop facial recognition and algorithms to make policing more efficient; they provide free (but often ad-supported) public Wi-Fi; they send drones to monitor road congestion; and they rely on citywide electric grids to self-report usage and maintenance needs.[65]

Many cities are already absorbing data from the urban environment – including existing infrastructure and systems, sensor networks, social media feeds, user-generated app data, and more – and then centralizing and repackaging it in accessible, usable interfaces for developers, civic hackers, researchers, businesses, other cities, and citizens to take advantage of.[66] Providing a city's many constituents with access to data from and about their lives promotes a more engaged polity. Importantly, it also helps prepares citizens to consider their own data footprint and how "the technologies that seamlessly connect individuals to their environments change how they interact with the city and how the city interacts with the world at large."[67]

[61] *See id.*

[62] *See* Barbara Thornton, *City-As-A-Platform: Applying Platform Thinking to Cities*, Platform Strategy (http://platformed.info/city-as-a-platform-applying-platform-thinking-to-cities/ (last visited Apr. 24, 2017).

[63] Lawrence Lessig, *Code Is Law: On Liberty in Cyberspace*, Harvard Magazine (Jan. 1, 2000), http://harvardmagazine.com/2000/01/code-is-law-html.

[64] *See* Adrian Fong, *The Role of App Intermediaries in Protecting Data Privacy*, 25 Int'l J. L. & Info Tech. 85 (2017), doi: 10.1093/ijlit/eax002.

[65] *See Shedding Light on Smart City Privacy*, The Future of Privacy Forum (Mar. 30, 2017), https://fpf.org/2017/03/30/smart-cities/.

[66] *See, e.g.*, Rob van der Meulen, *Developing Open-Data Governance in Smart Cities*, Gartner (June 21, 2016), https://www.gartner.com/smarterwithgartner/developing-open-data-governance-in-smart-cities/ ("CitySDK, a project by the European Commission, and the Smart Nation API coLab from Singapore are two examples already in progress.").

[67] Matt Jones, *The City Is a Battlesuit for Surviving the Future*, Io9 (Sept. 20, 2009), https://io9.gizmodo.com/5362912/the-city-is-a-battlesuit-for-surviving-the-future.

Another significant, technology-driven aspect of this policy shift is that many of these efforts rely on novel combinations of municipal data, consumer data, and corporate data. For example, the City of Los Angeles entered into a data-sharing partnership with Waze, the smartphone app that tracks traffic in real time, in which "Data flows upward from motorists to Waze about traffic accidents, police traps, potholes, etc., and the City shares with Waze its data about construction projects, big events and other things that may affect traffic."[68] Where partnerships with private companies are not established, local regulatory authorities may instead require data sharing by law. In New York, San Francisco, and Sao Paolo, for example, local governments have revised rules or brought bills requiring Uber to share granular data about individual trips for such purposes as guiding urban planning, regulating driver fatigue, or reducing traffic congestion.[69]

Thus, smart cities will increasingly find themselves situated as intermediaries in an ecosystem of complex data and analytics flows. Given cities' unique regulatory, market, and social positioning, they will become important gatekeepers, dictating when, how, and for what purposes civic data may flow from one entity to another. What tools and considerations, then, should smart cities take into account in their role as platform?

Data mapping. Before cities can begin mediating the complex flows of municipal data to and from individuals and other entities, city officials need to understand what data they are collecting and how it is used throughout the entire smart city ecosystem. While this task can be daunting for an entity with the size and complexity of a municipality, a central component of a successful privacy and security program is knowing what data is collected, how sensitive it is, how identifiable it is, where it is stored, who has access to it, when and how it might be disposed of, and what it is or will be used for. When the city is acting as a platform for sharing data, the complexity of mapping data increases – as do the consequences should a city fail to understand the legal, economic, and social impacts of citizens' data spilling out without clear oversight.[70]

In particular, although these categories remain hotly debated, it is important to classify data as personally identifiable, pseudonymous, or de-identified.[71] Whether data can be used to identify or single out an individual within the city will have major legal implications and will determine under what conditions and for what purposes data may be used. This sort of identifiability classification is increasingly popular as part of open data schemas,[72] even as cities should be aware that there is significant debate within privacy and data science communities over when and how to regard data as "de-identified" or "anonymous."[73]

Urban datascapes raise difficult questions about data ownership. Who owns civic data – the individual who generates the data? The technology system provider? The municipality that contracted for the technology system? The public? Cities and those in privity with them need to navigate these complex waters, while keeping abreast of related issues such as what capacity parties have to secure data systems (e.g., a small public school may lack the expertise of a global

[68] David Bollier, *The City as Platform*, Bollier.org (Feb. 19, 2016), http://bollier.org/blog/city-platform.

[69] *See* Assembly Bill A6661, 2017–2018 (NY), https://www.nysenate.gov/legislation/bills/2017/A6661; *Regulating Individual Transportation in Sao Paolo: What Is at Stake?*, InternetLab (Jan. 12, 2016), http://www.internetlab.org.br/en/opinion/regulating-individual-transportation-in-sao-paulo-what-is-at-stake/; Joe Fitzgerald Rodriguez, *SF Wants Access to Uber and Lyft to Tackle Traffic Congestion*, SF Examiner (Mar. 31, 2017), http://www.sfexaminer.com/sf-wants-access-uber-lyft-data-tackle-traffic-congestion/; Lauren Smith, *NYC Taxi & Limousine Commission Proposal Requiring Drop-Off Location Data Raises Privacy Concerns*, Future of Privacy Forum (Dec. 30, 2016), https://fpf.org/2016/12/30/privacy-implications-collecting-hire-vehicle-drop-off-location-data/.

[70] *See* Whittington et al., *supra* note 10.

[71] *See* Jules Polonetsky, Omer Tene & Kelsey Finch, *supra* note 11.

[72] *See, e.g.*, *Data Classification Policy*, Office of the Chief Tech. Officer (Mar. 30, 2011), https://octo.dc.gov/sites/default/files/dc/sites/octo/publication/attachments/DataClassificationPolicy.pdf.

[73] *See* Part III below ("Open Data").

technology firm); who should be liable in the event of a data breach; what extra-legal privacy or security commitments entities have made; what data can or may cross territorial borders; and under what circumstances a particular party might be compelled to turn data over to a third party (e.g., a company holding citizen data may provide data to law enforcement subject to a subpoena or warrant, and a municipality may provide it to an individual subject to a freedom of information request).

Privacy notices. Every city, no matter how sizable its smart technology stores, should also establish – and make publicly available – a comprehensive privacy policy. These policies help all community stakeholders understand how and why data will be collected and used throughout the city, encouraging accountability and building public trust. While the science of effective disclosures continues to develop,[74] privacy policies remain a foundational tool for businesses and government organizations.

These public-facing policies should describe urban data practices, including, but not limited to, the following key provisions:

- How data is collected, stored, used, secured, shared, and disclosed
- For what purposes data is collected and used
- Which data sets are owned by which stakeholders, and what data rights and protections accompany them
- Which data sets are private or require individuals' consent before being used
- Which data sets can be shared with the city or with authorized third parties
- How de-identified data can be shared
- What options, if any, individuals have to access, correct, or request the deletion of their personal data
- If personal data will be used for automated decision-making, meaningful information about the logic involved and the significance and envisaged consequences of such processing for the individual
- How data holders will respond to law enforcement requests for data
- The identity and the contact details of the data controller
- Whether data will be used for research
- The period for which personal data will be stored

Cities can and should experiment with additional features such as layered notices, just-in-time notifications, and explanatory illustrations and data visualizations, as well as ensure that privacy policies are consistent, easy to understand, and accessible to all members of the public, including individuals with disabilities. Determining *where* and *how* to place notices in public spaces can be challenging. For example, in many places around the world, CCTV cameras are accompanied by a printed card with the legal authority, a statement that the camera is in operation, and contact details for obtaining additional details about the data processing.[75] Once cities begin expanding to distributed devices and sensors, however, notice will become even more difficult – should citizens look for a license plate on a drone overhead? Should there be a sign at the entrance to every subway station with mobile location analytics systems? Should cities

[74] *See, e.g.*, Lorrie Cranor, *Reflections on the FTC's Disclosure Evaluation Workshop*, Fed. Trade Comm'n (Nov. 30, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/11/reflections-ftcs-disclosure-evaluation-workshop.

[75] *See Data Protection and CCTV*, Data Protection Comm'r (Ireland), https://www.dataprotection.ie/docs/Data-Protection-CCTV/m/242.htm (last visited Apr. 24, 2017).

provide an app that will pop up notices about active data collection?[76] With a vast array of devices and sensors hovering around the cityscape, the public sphere can quickly become cluttered with an incomprehensible cacophony of privacy notices.

In addition to the challenge of balancing comprehensive disclosures against *readable* disclosures, smart city officials have sometimes struggled to draft disclosures that are temporally appropriate. That is, sometimes privacy policies describe not just the city's current technological and data collection capabilities, but also those that it hopes to roll out in the future (sometimes seeking to look years forward).[77] While cities should be commended for thinking about and making public the potential privacy impact of their new technologies and services suitably far in advance, making such disclosures in a privacy policy – without additional discussion – can muddy the water.

Much like their corporate counterparts, city attorneys that are not sure precisely how a new feature will work in practice often find themselves drafting privacy policies with the broadest possible terms, providing flexibility for when the city does finally roll out an ambitious project. Until the feature *is* available, however, such broad, permissive policies may give citizens, communities, and consumer and privacy advocates (and anyone else who reads the privacy policy)[78] cause for concern. Confusion and mistrust are only likely to compound when city officials (understandably) cannot describe any concrete privacy controls for as yet inactive features.

This is not to say that cities should withhold information about prospective privacy-impacting technologies or services; after all, constant updates to a privacy policy every time a new feature comes online may also fail to satisfy (or adequately notify) citizens and advocates. Rather, cities should aspire to publish privacy policies that are current and timely, but also to supplement them with additional transparency mechanisms.

Transparency. In a smart city, privacy policies are necessary but not sufficient for informing citizens about how data is collected and used. Municipalities must strive to be truly *transparent* to the public they serve. This requires engaging with communities and stakeholders early and often, seeking creative ways to alert citizens to data-driven activities, and increasing data literacy throughout the city's population.

When cities literally act as data platforms, they gain additional leverage to promote transparency throughout the smart city data ecosystem. Through their terms of service or contractual dealings, cities may condition other parties' access to civic data on maintaining appropriate transparency mechanisms. Consider, for example, the critical role played by the Apple iTunes and Google Play platforms, which require apps to provide privacy policies and link to them from

[76] *See, e.g.*, Art. 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (Sept. 16, 2014), http://www.dataprotection.ro/servlet/ViewDocument?id=1088; Art. 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones (June 16, 2015), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf; *Opening remarks of FTC Chairwoman Edith Ramirez, Privacy and the IoT: Navigating Policy Issues*, Int'l. Consumer Electronics Show (Jan. 6, 2015), https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf.

[77] For example, early versions of the privacy policy for LinkNYC, which offered free public Wi-Fi through sidewalk kiosks, contained language about camera and facial recognition for months before the cameras were turned on. *See* Brady Dale, *Meet the Brave Souls Who Read LinkNYC's Two Different Privacy Policies*, Observer (July 28, 2016), http://observer.com/2016/07/linknyc-intersection-sidewalk-labls-alphabet-google-privacy/.

[78] *Cf.* Aleecia McDonald & Lorrie Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A J. of L. and Policy for the Info. Soc'y 543 (2008), http://hdl.handle.net/1811/72839.

within the platforms themselves.[79] App platforms also tackle more sensitive data collection by requiring and prompting users with just-in-time notifications about particular data uses, such as location tracking or access to address book contacts.

Cities can also leverage their unique control over both physical and digital spaces to deploy multifarious messages about how civic data is collected and used. City officials should proactively and preemptively assess in what manner to provide information about data collection and use for every initiative that involves citizens' PII. Some uses may be appropriately disclosed via municipal publications or announcements, while other, more sensitive uses may require specific, on-site public disclosures or signage. The physical environment for cities' connected devices also provides creative opportunities, such as lights or noises, to indicate when data is being collected. Some devices will be more obvious than others; for example, a streetlight triggered by a motion detector likely does not need a more specific notification. A streetlight passively sensing a nearby smartphone's MAC signal, on the other hand, would raise a more significant concern.[80]

Cities can also invest in digital literacy and education campaigns, to help citizens understand and take advantage of technological offerings more generally while bridging the digital divide.

Purpose specification and data minimization. Finally, when designing systems to collect or use personal data, smart cities should specify the purpose of data collection and ensure data minimization to avoid collecting beyond what is necessary for those purposes. In situations where notice and choice may not be practical, or where data may leave the city's specific control and enter an unregulated ecosystem, narrowing collection and use of personal data in accordance with these principles will safeguard individuals' privacy and bar indiscriminate surveillance. At the same time, these principles should not be rigidly applied to hinder the ability of smart cities to improve and develop innovative new services. Smart cities should consider looking to the Federal Privacy Act of 1974 as a model for addressing the privacy impact of government databases.

City officials must also keep in mind their influence as custodians of a data and technology intermediary, where data practices, permissions, and assumptions written into a city's code can become *de facto* laws.[81] By controlling the pipeline of civic data and restricting the types and classes of data going into and out of their data platforms (whether internal or public-facing), cities will have tremendous power to set privacy-protective standards, norms, and technologies in place to enforce – or, conversely, to undercut – the principles of purpose specification and data minimization. This requires cities not only to implement these principles, but to enforce them and monitor data recipients and systems for compliance. At the same time, however, cities should be cognizant of their own limitations: data that enters city hands may be *more* susceptible to being made public via freedom of information requests or open data mandates.

[79] *See, e.g.*, *Google API Terms of Service*, Google Developers (Dec. 5, 2014), https://developers.google.com/terms/; *Terms and Conditions*, Apple Developer, https://developer.apple.com/terms/ (last visited Apr. 24, 2017); *FPF Mobile Apps Study*, Future of Privacy Forum (Aug. 2016), https://fpf.org/wp-content/uploads/2016/08/2016-FPF-Mobile-Apps-Study_final.pdf (showing upward trend of privacy policies in app stores).

[80] *See, e.g.*, *Mobile Location Analytics Opt-Out*, Smart-Places, https://smart-places.org/ (last visited Apr. 24, 2017); *Wi-Fi Location Analytics*, Info. Comm'r's Office (U.K.) (Feb. 16, 2016), https://ico.org.uk/media/1560691/wi-fi-location-analytics-guidance.pdf; U.S. v. InMobi Pte Ltd., Case No.: 3:16-cv-3474 (N.D. Cal. 2016), https://www.ftc.gov/system/files/documents/cases/160622inmobicmpt.pdf; *WiFi Tracking Technology in Shops and on Public Roads by Bluetrace: Investigation by the Dutch Data Protection Authority*, Autoriteit Persoonsgegevens (Oct. 2015), https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_bluetrace_investigation.pdf.

[81] *See* Martjin de Waal, *The City as an Interactive Platform*, The Mobile City (Oct. 9, 2009), http://themobilecity.nl/2009/10/09/593/.

Collecting data without an intent to use it in specific ways, or storing it after it has served its purpose, is risky behavior for any organization, but cities especially hold the keys to highly sensitive data, often from vulnerable populations.[82] The New York City municipal ID program, for example, was designed to help undocumented immigrants integrate into the city's residential fabric. Upon the election of President Trump and a policy shift by the federal government towards actively tracking and deporting undocumented immigrants, New York City officials have struggled over what to do to protect their database: challenge in court any attempt by the federal data to access it? Destroy it?[83] When cities choose to collect personal and sensitive data, they must consider how that information could be reused by others. It is common privacy gospel that if sensitive data cannot be adequately safeguarded, it should not be collected in the first place.

CITY AS GOVERNMENT

Even the most technologically advanced city in the world[84] is still ultimately a political entity, accountable to the needs and desires of its constituents. Unlike private sector data stewards or platforms, cities cannot pick and choose which populations to serve, and every misstep can have huge and lasting impacts on the urban life of citizens. The technologists' desire to "move fast and break things" is dangerous when real lives and the public interest are at stake.

In their more traditional role as a local governmental entity, cities must navigate their obligations to ensure the safe, efficient, and equitable administration of city services; to govern transparently; and to protect the civil liberties of city residents. Often, these goals need to be balanced against each other, as for example, transparency mandated by freedom of information laws may run up against individuals' privacy rights. Complicating this, cities must account for the competing public values and preferences of their highly diverse constituents: some citizens broadly support the use of body-worn cameras by police for improving accountability and public safety, for example, while others distrust and reject this measure for increasing government surveillance of vulnerable populations.[85]

Furthermore, municipalities' reliance on data-driven decision-making raises concerns that "technocratic governance" could supplant citizen-centered political processes.[86] Municipalities that are overeager to deploy technologically oriented solutions may inadvertently find themselves prioritizing some citizens over others.[87] The City of Boston, for example, developed a smartphone app that would use the phone's accelerometer and GPS data to automatically report

[82] *See, e.g.*, Deepti Hajela & Jennifer Peltz, *New York City Could Destroy Immigrant ID Card Data After Donald Trump Win*, The Denver Post (Nov. 15, 2016), http://www.denverpost.com/2016/11/15/new-york-city-destroy-immigrant-id-card-data/.

[83] *See* Liz Robbins, *New York City Should Keep ID Data for Now, Judge Rules*, N.Y. Times (Dec. 21, 2016), https://www.nytimes.com/2016/12/21/nyregion/new-york-city-should-keep-id-data-for-now-judge-rules.html.

[84] According to one recent study, Tokyo. IESE Cities in Motion Index 25 (2016), http://www.iese.edu/research/pdfs/ST-0396-E.pdf/.

[85] *See* Harvard Law Review, *Considering Police Body Cameras*, 128 Harv. L. Rev. 1794 (Apr. 10, 2015), http://harvardlawreview.org/2015/04/considering-police-body-cameras/.

[86] *See* Rob Kitchin, *The Real-Time City? Big Data and Smart Urbanism*, 79 GeoJournal 1–14 (2014), https://pdfs.semanticscholar.org/6e73/7a0e5ef29303760a565ba5e9d98510ab0976.pdf.

[87] *See* Jathan Sadowski & Frank Pasquale, *The Spectrum of Control: A Social Theory of the Smart City*, 20 First Monday (2015), http://firstmonday.org/article/view/5903/4660 ("To take some obvious examples: should new forms of surveillance focus first on drug busts, or evidence of white-collar crime, or unfair labor practices by employers? . . . Do the cameras and sensors in restaurants focus on preventing employee theft of food, stopping food poisoning, and/or catching safety violations?").

potholes to the city's Public Works Department as users drove around town.[88] Before launching the app, however, the city and the app developers realized that variances in smartphone ownership could foster inequities in road improvement. The populations that were most likely to own a smart phone – the young and the wealthy – were at risk of diverting city services away from poor and elderly neighborhoods.[89] Instead, the city modified their rollout plans, "first handing the app out to city-road inspectors, who service all parts of the city equally, relying on the public for only additional supporting data."[90]

Municipalities must ever be conscious of how the deployment of data-collecting technologies will shift the balance of power maintained between citizens and the city. What tools and considerations, then, should smart cities take into account to protect individual privacy in their role as local government?

Open data. Many federal, state, and municipal governments have committed to making their data available to city partners, businesses, and citizens alike through Open Data projects and portals.[91] Open data efforts characterize themselves as providing the social, economic, and democratic values that cities often seek to embody[92]: they are about "living up to the potential of our information, about looking at comprehensive information management and making determinations that fall in the public interest," "unlock[ing] troves of valuable data – that taxpayers have already paid for," and establishing "a system of transparency, public participation, and collaboration."[93] As a practical matter, too, governments are uniquely situated to give back to their communities due to the quantity and centrality of the government's data collection, as well as the fact that most government data is public data by law.[94]

In the spirit of civic innovation and reform, many cities are not only making their databases public, they are increasingly doing so by default. The City of Louisville has a standing executive order for all data to be open,[95] for example, and the mayor and city council of the City of Palo Alto have also recently decreed data to be open by default.[96] The City of Seattle, which finds itself attempting to balance a stringent public records law against a robust civic tech ethos, has decreed that data will be made "open by preference."[97] Indeed, all levels of government are encouraging open data: in 2013, "President Obama signed an executive order that made open and machine-readable data the new default for government information,"[98] and the federal data.

[88] *See* Exec. Office of the President, Big Risks, Big Opportunities: the Intersections of Big Data and Civil Rights (May 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf; John D. Sutter, *Street Bump App Detects Potholes, Tells City Officials*, CNN (Feb. 16, 2012), http://edition.cnn.com/2012/02/16/tech/street-bump-app-detects-potholes-tells-city-officials/index.html.

[89] *See* Kelsey Finch & Omer Tene, *supra* note 5, at 1604.

[90] *Id.*

[91] *See* Roberto Montano & Prianka Srinivasan, *The GovLab Index: Open Data*, GovLab (Oct. 6, 2016), http://thegovlab.org/govlab-index-on-open-data-2016-edition/.

[92] *See, e.g.*, Jane Jacobs, The Death and Life of Great American Cities (1961) ("Cities have the capability of providing something for everybody, only because, and only when, they are created by everybody.").

[93] *See Open Government* Initiative, The White House, https://obamawhitehouse.archives.gov/open (last visited Apr. 24, 2017), *Why Open Data?*, Open Data Handbook, http://opendatahandbook.org/guide/en/why-open-data/ (last visited Apr. 24, 2017).

[94] *See id.*

[95] Mayor of Louisville, Executive Order No. 1, Series 2013, *An Executive Order Creating an Open Data Plan* (Oct. 11, 2013), https://louisvilleky.gov/government/mayor-greg-fischer/read-open-data-executive-order.

[96] City of Palo Alto, *Proclamation of the Council Proclaiming the City of Palo Alto as Open [Data] by Default* (Feb. 10, 2014), http://www.cityofpaloalto.org/civicax/filebank/documents/38803.

[97] Office of the Mayor, City of Seattle, Executive Order 2016–01 (Feb. 27, 2016), http://murray.seattle.gov/wp-content/uploads/2016/02/2.26-EO.pdf.

[98] *See Open Government Initiative*, The White House, https://obamawhitehouse.archives.gov/open (last visited Apr. 24, 2017).

gov catalog contains 5,610 datasets from nineteen contributing city governments, 1,392 datasets from seven county governments, and 9,619 datasets from twenty-one state governments.[99]

City leaders must also carefully evaluate local public records laws[100] to ensure that individuals' personal data is not inadvertently made public by open programs. The breadth of any relevant Freedom of Information Act or similar laws should also be considered in determining what personal information a city can or should collect. While freedom of information laws uniformly include exceptions to protect individuals from the "unwarranted invasion of personal privacy,"[101] they predate the advent of big data and smart city technologies. Consequently, cities – and governments more broadly – have struggled to adapt to the realities of modern de-identification and reidentification science in determining what constitutes protected personal information. In 2013, for example, the New York Taxi and Limousine Commission collected "pickup and drop off times, locations, fare and tip amounts, as well as anonymized (hashed) versions of the taxi's license and medallion numbers" for every taxi ride in the city.[102] The data was obtained via a freedom of information request and subsequently made public, at which point industrious data scientists began reidentifying trips made by particular celebrities (including exact fare and tipping data), as well as, more salaciously, detailing the travels of everyone who took a taxi to or from Larry Flynt's Hustler Club, "pinpointing certain individuals with a high probability."[103]

Open and accessible public data benefits citizens by helping cities uphold their promises towards efficient and transparent governance, but also poses a significant risk to individual privacy. One of the greatest risks of opening government datasets to the public is the possibility that individuals may be reidentified or singled out from those datasets, revealing data about them that would otherwise not be public knowledge and could be embarrassing, damaging or even life threatening.[104] Recent advances in smart city technologies, reidentification science, data marketplaces, and big data analytics raise those reidentification risks.[105]

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, *real-time* data about the city's – and its citizens' – activities available to anyone in the world. Databases of calls to emergency services – for 911, or fire departments, or civil complaints about building codes, restaurants, and even civil rights violations – are all obvious risks for the leakage of sensitive data. Data sets that are more bureaucratic may fail to raise the same privacy red flags, while still leaving individuals just as exposed. In 2017, for example, a parent who was examining expenditure files on the Chicago Public Schools website discovered that deep within the tens of thousands of rows of vendor payment data were some 4,500 files that identified students with Individualized Educational Programs – revealing in plain text the students' names, identification

[99] *Data Catalog*, Data.gov, https://catalog.data.gov/ (last visited Jan. 3, 2017).

[100] *See, e.g.*, *State Freedom of Information Laws*, Nat'l Freedom of Info. Coal., http://www.nfoic.org/state-freedom-of-information-laws (last visited Apr. 24, 2017).

[101] *See, e.g.*, *Exemption 6*, Dep't of Justice Guide to the Freedom of Info. Act, https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption6_0.pdf (last visited Apr. 24, 2017).

[102] Anthony Tockar, *Riding with the Stars: Passenger Privacy in the NYC Taxicab Database*, Neustar Research (Sept. 15, 2014), https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/.

[103] *Id.*

[104] *Report of the Special Rapporteur on the Right to Privacy, Annex II*, Human Rights Council, U.N. Doc. A/HRC/31/64 (May 8, 2016) (by Joseph A. Cannataci); Ben Green et al., Open Data Privacy Playbook (Feb. 2017), https://cyber.harvard.edu/publications/2017/02/opendataprivacyplaybook.

[105] *See, e.g.*, Arvind Narayanan & Edward Felten, No Silver Bullet: De-Identification Still Doesn't Work (July 9, 2014), http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf.

numbers, the type of special education services that were being provided for them, how much those services cost, the names of therapists, and how often students met with the specialists.[106]

Governments and scholars have only recently begun to tackle the difficult question of publishing and de-identifying record-level government data.[107] In 2016, the National Institute of Standards and Technologies released a guide to de-identifying government datasets,[108] and de-identification expert Dr. Khaled El Emam published an "Open Data De-Identification Protocol."[109] The City of San Francisco also published the first iteration of an "Open Data Release Toolkit," which walks city officials through the process of classifying data's appropriateness for public output, identifying direct and indirect identifiers, applying de-identification techniques, and balancing the residual risks to individual privacy against the potential benefit and utility of the data.[110] The City of Seattle is currently producing an "Open Data Risk Assessment," which in collaboration with a community advisory board and local academics, examines the city's open data program, organizational structure, and data handling practices and identifies privacy risks and mitigation strategies.[111]

De-identification may be the single most difficult tool for cities to implement, and yet also one of the most important if data continues to be made open.[112] In addition to risk assessments, cities should consider alternatives to the "release and forget" model that most open data portals use.[113] Where possible, cities may condition access to data on the signing of a data use agreement (for example, prohibit attempted reidentification, linking to other data, or redistribution of the data), or set up a data enclave where researchers can run queries on de-identified information without ever acquiring it directly.[114]

Communications and engagement strategies. As smart city residents begin to interact with new technologies and data-driven services in their environment, misunderstandings around what data is collected and fears about how it may be used could risk the viability of valuable urban projects.

Smart city leaders should develop proactive strategies that anticipate potential privacy concerns and seek to address them in public. Materials that are easy for the public to access and understand should be available from the outset of a program to explain the purposes and societal benefits of using data in a particular way, as well as the range of safeguards available to mitigate residual privacy risks. Citizens should be given opportunities to comment publicly on the

[106] *See* 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/ (further database details on file with authors); Cassie Creswell, *How a Parent Discovered a Huge Breach by Chicago Public Schools – of Private School Students with Special Needs*, Parent Coal. for Student Privacy (Mar. 5, 2017), https://www.studentprivacymatters.org/how-a-parent-discovered-a-huge-breach-by-chicago-public-schools-of-private-school-students-with-special-needs/.

[107] *Cf.* The U.S. Census Bureau, which has been producing aggregated statistics and engaging with cutting-edge statistical disclosure control science for decades. *Statistical Disclosure Control*, U.S. Census Bureau, https://www.census.gov/srd/sdc/ (last visited Apr. 24, 2017).

[108] Simson Garfinkel, NIST Special Publication 800–188, 57 (2nd Draft): De-Identifying Government Datasets (Dec. 2016), http://csrc.nist.gov/publications/drafts/800–188/sp800_188_draft2.pdf.

[109] Khaled El Emam, *A De-Identification Protocol for Open Data*, Privacy Tech (May 16, 2016), https://iapp.org/news/a/a-de-identification-protocol-for-open-data/.

[110] Erica Finkle, DataSF: Open Data Release Toolkit, https://drive.google.com/file/d/0B0jc1tmJAlTcR0RMV01PM2NyNDA/view (last visited Apr. 24, 2016).

[111] *See* Green et al., *supra* note 105, at 57.

[112] *See* Garfinkel, *supra* note 108.

[113] *See* Simson Garfinkel, NISTIR 8053: De-Identification of Personal Information 14 (Oct. 2015), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.

[114] *Id.*

development and deployment of smart city technologies, particularly where data will be collected in new or different ways. Where possible, cities should also consider including citizens in the development process through user research, hackathons, and other participatory design events, which will give them an opportunity for deeper and more collaborative engagement than a public comment period alone. These responses, together with a proactive and responsive communications strategy, can help explain urban data strategy to alleviate public concerns.

One instructive example is the City of Chicago's "Array of Things" project. In partnership with the University of Chicago and the Argonne National Laboratory, the city wanted to deploy "a network of interactive, modular sensor boxes around Chicago to collect real-time data on the city's environment, infrastructure, and activity for research and public use."[115] Given the breadth and novelty of this urban sensing network, concerns about privacy loomed large.[116]

In addition to taking technical measures to minimize any personally identifying data being captured by the sensors, and instituting a variety of governance tools, the Array of Things also developed a sophisticated civic engagement plan. Its goals were fourfold: to "educate Chicagoans about the Array of Things project, process, the potential of the research, and the sensors' capacities; inform future generations of the Array of Things sensors; understand what the people want out of the Internet of Things & these neighborhood data; and collect resident feedback on privacy and governance policies for Array of Things."[117] The project team partnered with local community organizations to engage and educate Chicagoans, provided several easily accessible in-person and digital mechanisms for individuals to comment on its draft privacy policy, and developed a curriculum for a local high school to educate students on the Array of Things, developing their technology skills and engaging them with their city's real-time data flows.[118] The result was a more sophisticated privacy policy, an engaged and informed populace, and a positive model for cities around the world.

In contrast, the implications of failure to communicate effectively and timely can be stark, as demonstrated by the quick rise and even quicker demise of education technology vendor inBloom. Only a year after its public launch, the high-profile educational nonprofit inBloom folded in the face of sustained parent, press, and regulatory pressure about student privacy.[119] inBloom, in fact had more sophisticated privacy and security processes than many of the public schools whose data it sought to warehouse "so that school officials and teachers could use it to learn about their students and how to more effectively teach them and improve their performance in school."[120] Yet the organization largely failed to communicate proactively and respond to concerns about privacy, assuming that the value proposition of its data tools was self-evident. In doing so, it lost sight of the need to involve parents in the creation and implementation of the project and failed to prepare its partners – school districts and states – to talk about privacy and new technologies at a time when student data analytics were new to many stakeholders (including students, parents, and teachers). The results of failing to engage and communicate

[115] *What Is the Array of Things*, Array of Things, https://arrayofthings.github.io (last visited Apr. 24, 2017).

[116] *See* Amina Elahi, *City Needs More Detail in Array of Things Privacy Policy, Experts Say*, Chicago Tribune (June 20, 2016), http://www.chicagotribune.com/g00/bluesky/originals/ct-expert-array-of-things-privacy-policy-bsi-20160621-story.html.

[117] *Array of Things Civic Engagement*, Smart Chicago, http://www.smartchicagocollaborative.org/work/ecosystem/array-of-things-civic-engagement/ (Apr. 24, 2017).

[118] *Id.*

[119] *See* Natasha Singer, *InBloom Student Data Repository to Close*, N.Y. Times (Apr. 21, 2014), http://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close/.

[120] *See* Dan Solove, *Why Did inBloom Die? A Hard Lesson About Education Privacy*, LinkedIn (Apr. 29, 2014), https://www.linkedin.com/pulse/20140429042326-2259773-why-did-inbloom-die-a-hard-lesson-about-education-privacy.

with citizens were a $100 million failed project, a skeptical and distrusting populace, and a wave of legislation permanently restricting the sharing of student data.[121]

Surveillance and individual control. While ubiquitous and persistent monitoring technologies are increasingly available to cities – including CCTV and body-worn cameras, stingrays, facial recognition, and automated license plate readers – the important goals of security and efficiency should not open the door to unlimited surveillance of urban residents.[122] A recent study by the Georgetown Law Center on Privacy and Technology suggests that half of all US residents are in a police facial recognition database, but that the systems are typically unregulated and hidden from the public.[123] Troublingly, the report notes that "of 52 agencies, only four (less than 10%) have a publicly available use policy. And only one agency, the San Diego Association of Governments, received legislative approval for its policy," and that "only nine of 52 agencies (17%)" had an intent to log and audit officers' face recognition searches for improper use."[124] Further, the report underscores racial disparities built into the facial recognition technologies, which both "include a disproportionate number of African Americans" and "may be less accurate on black people."[125] The lack of transparency, lack of strict oversight, sensitivity of the data, and power imbalance inherent in surveillance programs significantly threatens civil liberties and undercuts public trust in all other civic technology programs. The report, along with further testimony before the House Committee on Oversight and Government Reform, also implicates the enhanced risk to privacy and transparency when local government joins forces with federal agencies – in this case, allowing the FBI access to state DMV photo databases through contractual memoranda with state governments.[126]

Wherever possible, cities should strive to give citizens detailed information and legitimate choices about how their data is collected and used. In some situations, however, cities may be faced with technologies and data services that make it impractical or infeasible to offer citizens traditional notices or choices. If citizens could opt out of automated tolling enforcement, or security cameras, or court records, important public safety and accountability goals could not be met.[127] If cities needed to inform citizens of every instance in which their smartphones' mobile identifiers were collected by a city-run Wi-Fi connection,[128] individuals would constantly be bombarded by information and grow unreceptive even to important notices. Nevertheless, cities should sometimes be prepared to trade off perfect data for individual privacy, in order to build trust. While citywide smart grids will not be as efficient without 100 percent participation, and many citizens may be perfectly happy to share their utility information for lower costs overall,

[121] *See* Brenda Leong & Amelia Vance, *inBloom: Analyzing the Past to Navigate the Future*, Data & Soc'y (Feb. 2, 2017), https://points.datasociety.net/inbloom-analyzing-the-past-to-navigate-the-future-77e24634bc34.

[122] *See* U.S. v. Jones, 132 S.Ct. 945 (2012) (J. Sotomayor, concurring).

[123] Clare Garvie, Alvaro Bedoya & Jonathan Frankle, The Perpetual Line-Up (Oct. 216), https://www.perpetuallineup.org/.

[124] *Id.*

[125] *Id.*

[126] *See Law Enforcement's Policies on Facial Recognition Technology: Hearing Before the H. Comm. on Oversight and Gov't Reform*, 115th Cong. (2016), https://oversight.house.gov/hearing/law-enforcements-use-facial-recognition-technology/.

[127] Paradoxically, in order to maintain such opt-outs the government would need to maintain a database of individuals who did not want to be tracked in order to effectuate those choices.

[128] *See, e.g.*, Steven Irvine, *Wifi Data Trial – Understanding London Underground Customer Journeys*, Transport for London Digital Blog (Nov. 23, 2016), https://blog.tfl.gov.uk/2016/11/23/wifi-data-trial-understanding-london-underground-customer-journeys/.

cities have nevertheless found ways to offer free and easy opt-outs for those citizens who do not wish to participate.[129]

If cities cannot notify citizens about a specific data collection in advance or at the time of collection, they should consider alternatives to safeguard individual privacy and bar indeterminate surveillance. If notice or choice is not provided in a particular instance, cities should:

- Conduct a privacy impact assessment and document in writing why notice or choice was not provided[130] (and revisit the decision on a regular basis),
- Implement processes to aggregate or de-identify data as soon as possible,[131]
- Seek the input and approval of an independent ethical review board,
- Provide individuals with information about how their data was used within a reasonable period of time after it had been collected,[132] and/or
- Minimize data to only what is necessary for a particular purpose.

Indeed, given that citizens may have no reasonable alternatives to opt out of municipal information systems, smart cities should seek to minimize data collection, or otherwise restrict the use and retention of personal data. As we have discussed previously, "one of the fundamental principles of informational privacy is to prevent the creation of secret databases."[133]

In addition to broader, public access to open government datasets that provide aggregate data on city and citizen activities, *individual* access rights are critical drivers for establishing trust and support in smart city technologies. They can ensure that smart city surveillance is not adversarial and secretive by empowering users to see for themselves what information has been collected about them. Where cities rely on algorithms to make substantive decisions with individual impacts, they should make efforts to reveal which databases they maintain and what criteria are used in their decision-making processes. If individuals cannot understand how and why civic institutions use their data, individual access rights may ring hollow.

Equity, fairness, and antidiscrimination. City leaders increasingly rely on big data analytics and algorithms to make cities, e-government, and public services faster, safer, and more efficient.

[129] *See, e.g.*, U.S. Energy Info. Admin., Smart Grid Legislative and Regulatory Policies and Case Studies (Dec. 2011), https://www.eia.gov/analysis/studies/electricity/pdf/smartggrid.pdf; Cassarah Brown, *States Get Smart: Encouraging and Regulating Smart Grid Technologies*, Nat'l Conference of State Legislatures (July 2013), http://www.ncsl.org/research/energy/regulating-and-encouraging-smart-grid-technologies.aspx (listing states with legislative action creating smart grid opt-outs); Nancy King & Pernille Jessen, *For Privacy's Sake: Consumer Opt-Outs for Smart Meters*, 30 Computer L. & Security Rev. 530 (2014), http://ir.library.oregonstate.edu/xmlui/bitstream/handle/1957/55599/KingNancyBusinessForPrivacy'sSake.pdf; jsessionid=9D15BA5022E662CA12B15F1FAC292B49?sequence=1.

[130] For example, the FBI's Privacy Impact Assessments often include this question: "Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not." *See, e.g.*, Privacy Impact Assessment for the FIRST (Firearms Information, Registration & Shooter Tracking) Application, Fed. Bureau of Investigation, Dep't of Justice (July 2013), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/first.

[131] *See, e.g.*, Info. Comm'r's Office (U.K.), *supra* note 79 (recommending data from Wi-Fi analytics be aggregated or have identifiable elements removed as soon as possible); Autoriteit Persoonsgegevens, *supra* note 79 (suggesting that Wi-Fi tracking within shops would be "less intrusive if the personal data processed will be made anonymous as soon as possible, or at least within 24 hours.").

[132] *See, e.g.*, Lukasz Olejnik, *Switzerland's New Surveillance Law*, Security, Privacy, & Tech Inquiries (Sept. 26, 2016), https://blog.lukaszolejnik.com/switzerlands-new-surveillance-law/.

[133] *See* Kelsey Finch & Omer Tene, *supra* note 5, at 1613 ("From its inception, information privacy law has been modeled to alleviate this concern, which arose in the Watergate period in the United States and the Communist era in Eastern Europe when secret databases were used to curtail individual freedoms.").

It is important that smart cities also use these tools to make their environments fairer, and not unfairly distribute resources or inadvertently discriminate against certain groups, including not only historic minorities, but also any group of individuals with a smaller digital footprint, who may otherwise be left out of data-driven analytics.[134] City leaders will need to be particularly forward-thinking as they consider the societal impact of revolutionary new technologies that may have conflicting impacts on different populations: automated vehicles, for example, promise to bring new freedom and mobility to the elderly and people with disabilities, and to rededicate urban spaces to people, rather than parking, but at the same time may eat up thousands of driving jobs.[135]

As municipal governments begin to gain real-time awareness of the people and activities within the city, that information feeds into policies with "profound social, political and ethical effects: introducing new forms of social regulation, control and governance; extending surveillance and eroding privacy; and enabling predictive profiling, social sorting and behavioural nudging."[136] With increasingly robust data and analytics, cities will be more equipped than ever to subtly "nudge" their citizens to modify their behavior in subtle, low-cost interventions – hopefully, for the common good.[137] For example, when the Center for Economic Opportunity in New York City implemented its $aveNYC initiative, it relied on behavioral economics to nudge low-income households to opening savings accounts, tying the accounts to financial incentives in the form of a 50 percent savings match, with results showing that "half of the program's participants reported no history of savings, 80% saved for at least one year to receive the match and 75% continued to save thereafter."[138] City leaders must be careful to nudge individual behavior in ethical ways, rather than in ways that will constrain individual behavior, or profile and discriminate against a certain class of people.

As cities increasingly rely on data to automate their decision-making, they must be careful to think holistically about why and how data is being used: bad data can lead to bad policies, even (or especially) in "smart" systems. Predictive policing and predictive sentencing, for example, have repeatedly been undercut by studies revealing racial bias in both their inputs (historic arrest and recidivism data, respectively) and their outputs, leading to institutional racial profiling.[139]

As we have discussed previously, big data and increased data flows may both exacerbate and alleviate governmental discrimination, whether intentional or inadvertent. Given this, it is more important than ever that cities engage citizens early and often in designing such systems, and

[134] *See* Exec. Office of the President, Big Risks, Big Opportunities: the Intersections of Big Data and Civil Rights (May 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf; John D. Sutter, *Street Bump App Detects Potholes, Tells City Officials*, CNN (Feb. 16, 2012), http://edition.cnn.com/2012/02/16/tech/street-bump-app-detects-potholes-tells-city-officials/index.html.

[135] *See* Jackie Ashley, *The Driverless Car Revolution Isn't Just about Technology: It's about Society Too*, The Guardian (Jan. 1, 2017), https://www.theguardian.com/commentisfree/2017/jan/01/driverless-cars-boon-bane-coming-down-fast-lane.

[136] *See* Rob Kitchin, *Getting Smarter About Smart Cities: Improving Data Privacy and Data Security*, Data Protection Unit, Department of the Taoiseach (Jan. 2016), http://www.taoiseach.gov.ie/eng/Publications/Publications_2016/Smart_Cities_Report_January_2016.pdf.

[137] Monika Glowacki, *Nudging Cities: Innovating with Behavioral Science*, Data-Smart City Solutions (May 17, 2016), http://datasmart.ash.harvard.edu/news/article/nudging-cities-innovating-with-behavioral-science-833 ("At the 15th Convening of the Project on Municipal Innovation, mayoral chiefs of staff and leaders in the field discussed how behavioral science can be used as a tool to improve public policy.").

[138] *Id.*

[139] *See* Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; Kelsey Finch & Omer Tene, *supra* note 5, at 1602–1603.

provide individuals who may be adversely impacted be informed of the criteria used in the decision-making processes, if not necessarily the raw data or code behind the determination.

Municipalities must be constantly vigilant to ensure they are serving *all* of their citizens, however difficult it may be to strike a balance between smart city beneficiaries and smart city casualties.

CONCLUSION

As Jane Jacobs said half a century ago, "Cities have the capability of providing something for everybody, only because, and only when, they are created by everybody."[140] The goal of local governments, technology developers, and community organizations should be to empower and engage citizens – to ensure that the cities of the future *are* created by everybody. And while many technological innovations are emerging first in urban spaces, they hold the potential to transform communities of all shapes and sizes.

Smart and data-driven technologies launch new conversations – and new ways to converse – between community leaders and community residents, creating room for the cultural growth and democratic impulses that have caused modern cities to flourish. Through open data programs, hackathons, participatory governance, and innovative community engagement processes, local governments are giving individuals new ways to interact with themselves, each other, and the world around them. When individuals have more control of their own data for their own purposes, a culture of data-driven decision-making, civic participation, and empowerment takes hold.

At the same time, if citizens do not trust that their data will be protected or do not see the benefits of new technologies, they could begin to fear the smart city's sensors and services as tools of discipline and surveillance, rather than cherish them as vehicles for transparency and innovation. City officials will need to learn how to make thoughtful decisions about providing appropriate notices, choices, and security measures to protect citizens' data, and to compete on accountability and transparency as much as on technological advancement. They will need to act as data stewards, diligently and faithfully protecting the personal data that the city and its partners collect. They should embrace their roles as platforms for data and technology, setting the bar high for privacy and security practices. And they must always strive to govern both their citizens and their citizens' data legally, fairly, and ethically.

If city leaders, technology providers, community organizations, and other stakeholders work together to address core privacy issues and principles, they will be able to leverage the benefits of a data-rich society while minimizing threats to individual privacy and civil liberties.

[140] Jane Jacobs, The Death and Life of Great American Cities 238 (1961).