Fordham Urban Law Journal

Volume 47
Number 4 *Symposium: Urban Intelligence and the Emerging City*
Article 1

2020

Governing Privacy in the Datafied City

Ira S. Rubinstein

Bilyana Petkova

GOVERNING PRIVACY IN THE DATAFIED CITY

Ira S. Rubinstein[*] *& Bilyana Petkova*[**]

ABSTRACT

Privacy — understood in terms of freedom from identification, surveillance, and profiling — is a precondition of the diversity and tolerance that define the urban experience. But with "smart" technologies eroding the anonymity of city sidewalks and streets, and turning them into surveilled spaces, are cities the first to get caught in the line of fire? Alternatively, are cities the final bastions of privacy? Will the interaction of tech companies and city governments lead cities worldwide to converge around the privatization of public spaces and monetization of data with little to no privacy protections? Or will we see different city identities take root based on local resistance and legal action?

This Article delves into these questions from a federalist and localist perspective. In contrast to other fields in which American cities lack the formal authority to govern, we show that cities still enjoy ample powers when it comes to privacy regulation. Fiscal concerns, rather than state or federal preemption, play a role in privacy regulation, and the question becomes one of how cities make

---

[*] Adjunct Professor of Law, New York University School of Law; Senior Fellow at the Information Law Institute and the Future of Privacy Forum.

[**] Assistant Professor, HBKU College of Law; Associate Scholar, Yale Information Society Project. We would like to thank everyone who generously commented on drafts presented at the Privacy Research Group, New York University School of Law; the Privacy Law Scholars Conference at Berkeley; the Georgetown Law Center Faculty Workshop; the 8th Annual State & Local Government Law Works-in-Progress Conference; and the *Fordham Urban Law Journal* Cooper-Walsh Colloquium on Urban Intelligence and the Emerging City. Particular thanks go to Julie Cohen, Nestor Davidson, Gabriel Nicholas, Paul Ohm, Marc Rotenberg, Aaron Shapiro, Katherine Strandburg, Olivier Sylvain, Mark Verstraete, and Salome Viljoen for reading and commenting on earlier drafts of the paper. We also thank our research assistants, Gabriel Ferrante and Sara Spaur, for excellent help with the project.

use of existing powers. Populous cosmopolitan cities, with a sizeable market share and significant political and cultural clout, are in particularly noteworthy positions to take advantage of agglomeration effects and drive hard deals when interacting with private firms. Nevertheless, there are currently no privacy frontrunners or privacy laggards; instead, cities engage in "privacy activism" and "data stewardship."

First, as privacy activists, U.S. cities use public interest litigation to defend their citizens' personal information in high profile political participation and consumer protection cases. Examples include legal challenges to the citizenship question in the 2020 Census and to instances of data breaches, including Facebook third-party data sharing practices and the Equifax data breach. We link the Census 2020 data wars to sanctuary cities' battles with the federal administration to demonstrate that political dissent and cities' social capital — diversity — are intrinsically linked to privacy. Regarding the string of data breach cases, cities expand their experimentation zone by litigating privacy interests against private parties.

Second, cities as data stewards use data to regulate their urban environment. As providers of municipal services, they collect, analyze and act on a broad range of data about local citizens or cut deals with tech companies to enhance transit, housing, utility, telecom, and environmental services by making them smart while requiring firms like Uber and Airbnb to share data with city officials. This relationship has proven contentious at times, but in both North American and European cities, open data and more cooperative forms of data sharing between the city, commercial actors, and the public have emerged, spearheaded by a transportation data trust in Seattle. This Article contrasts the Seattle approach with the governance and privacy deficiencies accompanying the privately-led Quayside smart city project in Toronto. Finally, this Article finds the data trust model of data sharing to hold promise, not least since the European rhetoric of exclusively city-owned data presented by Barcelona might prove difficult to realize in practice.

INTRODUCTION

What are the laws of privacy in urban settings? Legal scholars have begun discussing privacy in the narrow context of smart cities,[1] but the topic has yet to penetrate the federalism and localism debates. Our study of privacy in the city demonstrates that as new data-fueled business models emerge in the urban environment, analysis of the legal powers of the city may benefit from insights into the relationship not only among levels of government but also between the private and the public sector. Cities' power or powerlessness is not solely defined by federal and state preemption but might be influenced by a city's general fiscal autonomy (including dependence on federal and state grants), and the policies cities adopt when entering into partnerships with private corporations.

In contrast to other fields in which U.S. cities lack either the formal authority or actual capacity to govern,[2] the vast majority of cities retain ample legal powers over the collection and use of personal data

1. *See generally* Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581 (2015); Liesbet van Zoonen, *Privacy Concerns in Smart Cities*, 33 GOV'T INFO. Q. 472 (2016).

2. *See generally* GERALD FRUG & DAVID BARRON, CITY BOUND: HOW STATES STIFLE URBAN INNOVATION (2008); RICHARD SCHRAGGER, CITY POWER: URBAN GOVERNANCE IN A GLOBAL AGE (2016).

by city agencies.[3] Nevertheless, they often agree to relinquish powers by outsourcing control to tech companies in exchange for revenue or data, or in the hope of growing their technology sector in the name of innovation, jobs, and prosperity. For example, New York City might not fear state preemption when proposing to amend its administrative code to prohibit the sharing of location data with third parties.[4] However, the same city previously agreed to a deal whereby Sidewalk Labs — part of the Alphabet conglomerate and a sister company of Google — installed Wi-Fi kiosks in downtown Manhattan that used video cameras and Wi-Fi sensors to monitor the movements and activities of passersby with minimal protection of privacy interests.[5]

Privacy — on city sidewalks, streets, parks, plazas, and in public spaces generally — has emerged as an intrinsically urban value. Social scientists have long emphasized the anonymity of city life and connected it to the diverse social fabric and the freedom of choice that makes big cities appealing.[6] Diversity and tolerance are natural and desirable elements of the urban ethos. According to Jane Jacobs, privacy, as a precondition for both diversity and tolerance, is "precious in cities. It is indispensable."[7] Jacobs continues: "A good city street neighborhood achieves a marvel of balance between its people's determination to have essential privacy and their simultaneous wishes for differing degrees of contact, enjoyment or help from the people around."[8]

Intrinsic to city design are also public spaces, to which anonymity is inherent and which, as we show, are now increasingly being privatized. Public spaces have a long history as venues for political

---

3. *See generally* Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961 (2018).

4. *See* N.Y.C. Council Int. No. 1632 (2019), https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4069480&GUID=6FA8018C-84A4-4E71-93CE-D467AD53E9EA&Options=ID%7CText [https://perma.cc/M8NZ-XPQQ].

5. *See* Ava Kofman, *Are New York's Free LinkNYC Internet Kiosks Tracking Your Movements?*, INTERCEPT (Sept. 8, 2018), https://theintercept.com/2018/09/08/linknyc-free-wifi-kiosks/ [https://perma.cc/3EPT-23FT]; *see infra* Part III.

6. *See generally* JANE JACOBS, THE DEATH AND LIFE OF GREAT AMERICAN CITIES (1961); LYN LOFLAND, A WORLD OF STRANGERS: ORDER AND ACTION IN URBAN PUBLIC SPACE (1973); RICHARD SENNETT, BUILDING AND DWELLING: ETHICS FOR THE CITY (2018).

7. JACOBS, *supra* note 6, at 58.

8. *Id.* at 59; *see also* CHRISTENA NIPPERT-ENG, ISLANDS OF PRIVACY 2–3 (2010) (defining privacy as "selective concealment and disclosure" and as a daily activity of trying to "deny or grant varying amounts of access to our private matters to specific people in specific ways").

and ideological engagement.[9] As philosopher Michael Sandel points out, public spaces are "traditionally sites for the cultivation of a common citizenship, so that people from different walks of life encounter one another and so acquire enough of a shared . . . sense of a shared life that we can meaningfully think of one another as citizens in a common venture."[10]

In this Article, we ask whether technology is now changing the conventional wisdom about city life. As cities take on the role of technology testbeds, in ways never seen before, they become sites for ever more intrusive surveillance (in the conventional sense of monitoring behavior, or collecting and analyzing information to influence, manage, or direct behavior) and newer forms of what many refer to as "datafication," which is different from, and less familiar than, "digitization." The latter term refers to the use of computing devices to record, quantify, format, or store data as a series of digits. In contrast, "datafication" refers to "long-term storage in a format that is searchable, computationally manipulable, and [that] may be aggregated with information from other" sources.[11] Datafication thereby makes it possible for organizations to use data in ways that may have been unanticipated or even technologically infeasible at the time of collection, and are qualitatively different from the original purposes of the collection.

Cities are "data-rich environments"[12] because their large populations generate vast amounts of data as they interact with IoT devices and sensors in public spaces;[13] utilize city services that collect,

---

9. *See, e.g.*, DUNCAN MCLAREN & JULIAN AGYEMAN, SHARING CITIES: A CASE FOR TRULY SMART AND SUSTAINABLE CITIES 145 (2015) (characterizing public spaces in the city as "the crucible of democracy").

10. *The Reith Lectures: Michael Sandel, A New Citizenship, Markets and Morals*, BBC RADIO 4 (June 9, 2009) (downloaded using iTunes) *cited in* DUNCAN MCLAREN & JULIAN AGYEMAN, SHARING CITIES: A CASE FOR TRULY SMART AND SUSTAINABLE CITIES 145 (2015); *see also* LYN LOFLAND, THE PUBLIC REALM: EXPLORING THE CITY'S QUINTESSENTIAL SOCIAL TERRITORY 234–35 (1998) (identifying the practice of politics as one of several valuable uses of the public realm).

11. *See* Katherine Strandburg, *Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 11 (Julia Lane et al. eds., 2014).

12. Rubinstein, *supra* note 3, at 1964.

13. IoT (the "Internet of Things") refers to the information networks comprised of sensors and other technologies embedded in physical objects and linked via wired and wireless networks. *See* FUTURE OF PRIVACY FORUM, COMMENTS OF THE FUTURE OF PRIVACY FORUM ON CONNECTED SMART TECHNOLOGIES IN ADVANCE OF THE FTC "INTERNET OF THINGS" WORKSHOP 3 (2013), https://fpf.org/wp-content/uploads/FPF-Comments-Regarding-Internet-of-Things.pdf [https://perma.cc/UHW8-4DFJ].

analyze, and optimize personal data;[14] and encounter the special-purpose technologies deployed by law enforcement to maintain public safety and safeguard citizens against terrorist attacks.[15] This ubiquitous collection of data about all aspects of city living and the near-constant monitoring of public spaces erodes the anonymity of urban living. It also threatens the "marvel of balance"[16] between wanted and unwanted interaction with other people and government officials (especially local law enforcement), without which the diversity and tolerance of city life become unsustainable. Further, anonymity is but one aspect of privacy — the advent of big data has seen the emergence of broader concerns intertwined with privacy, such as lack of algorithmic fairness, accountability, and transparency. Questions inevitably arise as to how best to counteract these trends at the local level. Although we acknowledge the interconnection of the above contexts in which cities are data-rich environments, hereafter, we zoom in on civic uses of data in various cities.

Importantly, the comprehensive notion of data privacy that we adopt in this Article allows for the conceptualization of data privacy as a lever of both regulation and deregulation. Privacy is instrumentalized for the pursuit of traditional consumer protection and political participation goals that stretch beyond municipal boundaries, making cities participants in nation-wide debates of regulation and deregulation that reverberate across the country and may even have global implications. Rather than the enactment of new legislation, public interest litigation — as an instance of exercising existing city powers — plays a role in these cases. Simultaneously, privacy can also be instrumentalized by private actors — for example, in the sharing economy — that want to avoid regulation of any kind. With this in mind, we consider whether several cities, at the same moment in time, will reach different outcomes when faced with similar policy challenges or converge on

---

14. *See generally* STEPHEN GOLDSMITH & SUSAN CRAWFORD, THE RESPONSIVE CITY: ENGAGING COMMUNITIES THROUGH DATA-SMART GOVERNANCE (2014); STEPHEN GOLDSMITH & NEIL KLEIMAN, A NEW CITY O/S: THE POWER OF OPEN, COLLABORATIVE AND DISTRIBUTED GOVERNANCE (2017).

15. These include video security cameras, automatic license plate readers (ALPRs), shot detectors, body-worn cameras, and, most recently, facial recognition technology. *See generally* JAKE LAPERRUQUE, PROJECT ON GOV'T OVERSIGHT, FACING THE FUTURE OF SURVEILLANCE (2019), https://s3.amazonaws.com/docs.pogo.org/report/2019/Facing-the-Future-of-Surveillance_2019.pdf [https://perma.cc/HYY8-5LKV].

16. *See* JACOBS, *supra* note 6, at 59.

policies across the board. We question to what extent the level of privacy protection in the city is dependent on general federal constitutional and statutory frameworks. The Article offers tentative answers by discussing developments in a handful of U.S., Canadian, and European cities.

Given that privacy is a multifaceted concept, we find that the same cities may protect certain aspects of privacy in some areas while undermining it in others. For example, we see New York City litigating to ban the collection of citizenship data of its population,[17] yet also attempting to acquire from Airbnb, without subpoenas, the personal data of Airbnb hosts.[18] Thus, there are no privacy frontrunners or privacy laggards. Instead, we identify two main roles for data-rich cities: privacy activists and data stewards.

First, through data privacy activism, cities raise a voice in nation-wide political and consumer protection debates as in the Census 2020, Cambridge Analytica, and Equifax cases. As privacy activists, cities assume a role most closely aligned with a traditional public law institution acting to utilize innovation in the service of citizens.[19] Second, cities act as data stewards when they take steps to govern a new datafied urban space.[20] This role extends from pooling data among city agencies to improve the delivery of services, to managing data-sharing agreements with private actors in discrete contexts (such as ride- or bike-share data), to ceding control over data governance as an element of huge real estate development deals.[21] As privacy stewards, cities may reorient the very understanding of "public interest" from privacy protections to open data sharing practices and behave more like commercial actors. Privacy can give way to budgetary concerns exacerbated by federal and state disengagement from the provision of public services, immigration waves, and general urbanization trends. Our case studies suggest that data stewardship is best understood on a spectrum spanning both highly protective intracity data agreements and commercial giveaways, with "data collaboratives" (or "data trusts") occupying a middle ground. Thus, cities-as-data stewards attempt to regulate their urban environments through data, which may occur at the expense of

---

17. *See infra* Part II.

18. *See infra* Part III.

19. Privacy activism is not confined to litigation. It extends as well to legislative and regulatory activity. *See* Rubinstein, *supra* note 3, at 1966 (discussing innovative local surveillance ordinances).

20. Strandburg, *supra* note 11, at 10–11.

21. *See infra* Section III.B.iv.

privacy. Finally, we find that the privatization of public services is morphing into the privatization of public spaces, as data collected in communal areas are co-owned or co-opted by private companies.

This Article proceeds as follows: Part I situates urban data initiatives and related privacy issues in the context of federalism and localism. Part II examines the city as a privacy activist through the lens of the Census 2020 litigation and lawsuits against major corporations (such as Facebook and Equifax) in which city lawyers led consumer protection lawsuits on behalf of local residents but acted on a national stage. Part III then examines the city as a data steward using detailed case studies about the impact on the privacy of data-sharing agreements among city agencies and commercial agreements with urban innovation firms like Sidewalk Labs or sharing economy firms like Uber or Airbnb. Part III also contrasts instances of data governance arrangements in business-friendly environments, specifically comparing Toronto and Barcelona's efforts to preserve the public interest while embracing smart city concepts. The Article then concludes.

I. PLACING PRIVACY IN THE FEDERALISM AND LOCALISM DEBATES

This Part locates privacy and technology within a historical overview of theorizing cities from a legal vantage point: First, it shows how cities are slowly carved out space within American federalism and localism debates. Second, it engages with the most developed account of urban legal theory today — that of Professor Richard Schragger. In the privacy field, the model advanced by Schragger translates into an amalgam of urban privacy activism and data stewardship, as discussed below.[22] In other words, the model likely holds true even beyond the United States, with two caveats: when applied to big, cosmopolitan cities; and to the extent that such cities choose to avail themselves of agglomeration effects and existing legal powers.

A. From Federal to Local, Urban and Cosmopolitan Values

The study of big cities often falls in the cracks between federalism and localism. Amid insightful essays on "Our Federalism,"[23] "Our

22. *See infra* Parts II, III.

23. *See generally* Heather K. Gerken, *Our Federalism(s)*, 53 WM. & MARY L. REV. 1549 (2012).

Localism,"[24] and a carve-out for "Our Regionalism,"[25] a take on "Our Urbanism" is still missing. Federalism often centers on the relationship between the federal government and the states, while localism examines the relationship between states and localities. Granted, both scholarly work and constitutional doctrine recognize overlaps. Federalism and localism coincide with the values of decentralization: Dean Heather Gerken spells out the normative case for federalism as promoting "choice, competition, participation, experimentation, and the diffusion of power."[26] Professor Richard Briffault convincingly argues that what is true for federalism is even more true for localism, since:

> [T]he [Supreme] Court's conflation of federalism with "local" self-governance and accountability to local electorates is noteworthy, and many of the Court's federalism cases actually dealt with local governments. The Court's normative concerns with responsiveness to diverse needs in a heterogeneous society, innovation and experimentation, and citizen involvement in democratic processes apply even more to local governments than to states.[27]

Professor Schragger goes a step further by demonstrating that as large corporate interests drive state and federal policymakers to converge around a deregulatory agenda, cities — not states — have become the true "laboratories of democracy" in the United States, bulwarks of diversity, and engines of normative federalism.[28] Schragger persuasively argues that as economic activity in urban centers increases, cities' ability to experiment with redistributive and regulatory policies is on the rise.[29]

State and local autonomy have a long association with a conservative agenda, at least since the days of Jim Crow.[30] Especially in the aftermath of the 2016 U.S. presidential election, however, the

---

24. *See, e.g.*, Richard Briffault, *Our Localism: Part I — The Structure of Local Government Law*, 90 COLUM. L. REV. 1 (1990); Richard Briffault, *Our Localism: Part II — Localism and Legal Theory*, 90 COLUM. L. REV. 346 (1990).

25. *See generally* Jessica Bulman-Pozen, *Our Regionalism*, 166 U. PA. L. REV. 377 (2018).

26. Heather K. Gerken, *The Supreme Court 2009 Term — Foreword: Federalism All the Way Down*, 124 HARV. L. REV. 4, 8 (2010).

27. Richard Briffault, *The Challenge of the New Preemption*, 70 STAN. L. REV. 1995, 2018–19 (2018).

28. Richard Schragger, *Federalism, Metropolitanism, and the Problem of States*, 105 VA. L. REV. 1537, 1589–91 (2019).

29. *Id.* at 1597.

30. *See generally* Jack Balkin, *Federalism and the Conservative Ideology*, 459 URB. LAW. 3 (1987).

local has become the new stomping ground for progressives. American cities have formed a sort of bottom-up opposition in a host of policy domains, including campaign finance regulation,[31] "sanctuary" for immigrants,[32] environmental protection,[33] and anti-discrimination.[34] Federalism and localism scholars have long noted the trend, but what has gone under the radar is a new area of city initiatives: data privacy.

Should what is true for all localities and all cities in general — for example, their recently expanded capacity and willingness for regulatory experimentation — apply *a fortiori* to big cities that, thanks to a sizeable market share, are even better able to offer viable democratic experiments across a range of policies? The role of large U.S. cities in a federal or local constellation of actors is rarely studied separately.[35] No doubt, on these terms, New York City is no different from Tucson, Arizona. Professor Nestor Davidson persuasively shows that questions of legal autonomy across all localities are essential for depolarizing conflict and planting the seeds of legal doctrine, but emphasizes the variety of state constitutions that point to the difficulty of a one-size-fits-all approach.[36] There are a small number of major American cities with their own legal charters — Chicago, New York City, San Francisco, Seattle, and Washington, D.C. — that can be singled out because of their sheer size or cultural, technological, or political leadership. We focus our study on these

---

31. *See* Vivian Wang, *N.Y. Democrats Vowed to Get Big Money Out of Politics. Will Big Money Interfere?*, N.Y. TIMES (Nov. 22, 2018), https://www.nytimes.com/2018/11/22/nyregion/campaign-finance-reform-new-york.html [https://perma.cc/3NHR-FBPS] (referring to New York City's approved ballot proposal to lower contribution limits for city races and increase the city's matching funds for candidates).

32. *See generally* Christopher Lasch et al., *Understanding "Sanctuary Cities"*, 59 B.C. L. REV. 1703 (2018) (presenting a comprehensive overview of sanctuary policies on the state and city level).

33. *See generally* Sarah Holder, *One Year After Trump Left the Paris Agreement, Who's Still In?*, CITYLAB (June 1, 2018), https://www.citylab.com/environment/2018/06/one-year-after-trump-left-the-paris-agreement-whos-still-in/561674/ [https://perma.cc/3TCK-M9XY] (discussing funding initiatives for American cities' environmental pledge).

34. *Cities and Counties with Non-Discrimination Ordinances that Include Gender Identity*, HUM. RTS. CAMPAIGN, https://www.hrc.org/resources/cities-and-counties-with-non-discrimination-ordinances-that-include-gender [https://perma.cc/U5WP-EJAY] (last visited Dec. 23, 2019) (listing cities and counties that prohibit employment discrimination on the basis of gender identity by public and private employers).

35. Frug and Barron are the exceptions. *See supra* note 2.

36. *See generally* Nestor M. Davidson, *The Dilemma of Localism in an Era of Polarization*, 128 YALE L.J. 4 (2019).

cosmopolitan cities.[37] In seeking to understand the privacy aspects of "Our Urbanism," however, it also makes sense to add to the analysis a snapshot of medium-size and smaller cities located in the interior of the country.

Further, we attempt to place the U.S. developments within a global perspective by discussing a few foreign cities that have undertaken important smart city and data stewardship experiments — namely, Toronto and Barcelona.[38] The cosmopolitan ambitions of diverse and populous urban centers, like Canada's Toronto, are comparable to those of New York City. In contrast, Barcelona, Spain — a middle-sized city in Europe that struggles for a cosmopolitan flavor — provides an example of an alternative vision of the public sector's engagement with technology firms. Moreover, a federalist and localist framing remains apt for these cities since Toronto is embedded within a federal system, while Barcelona is a part of Spain's highly decentralized government.

The capacity of big cities for experimentation is arguably stronger than that of smaller cities since, as Schragger points out, agglomeration effects limit the fear of capital flight.[39] He challenges the view of competitive federalists who explain urban ethos with simple convergence around a single deregulatory agenda: in the latter view, cities competing to attract businesses and skilled workers will offer different deregulatory bundles lest capital and skilled labor decide to "vote with their feet" and go elsewhere due to more favorable conditions.[40] Instead of sorting, Schragger posits agglomeration as central to urban policy initiatives. In his model,

---

37. *See infra* Parts II, III. For the first foray of the notion of a global city in the academic debate, see generally SASKIA SASSEN, THE GLOBAL CITY (1991). Defining cosmopolitanism is not an easy task. *See, e.g.*, KWAME APPIAH, COSMOPOLITANISM: ETHICS IN A WORLD OF STRANGERS (2007); ULRICH BECK, COSMOPOLITAN VISION (2006). In the context of our study, the cosmopolitan can be broadly linked to city communities of diverse, often immigrant populations that in spite of racial, religious, or other differences try to arrive at a common understanding of the good life, including on the place of technology, innovation, and privacy in it. In a similar vein, Jeremy Waldron suggests that the "cosmopolitan" can be understood as an attitude, lifestyle, and a way of constructing an identity for oneself that is different from devotion or immersion in a particular culture. *See generally* Jeremy Waldron, *What Is Cosmopolitan?*, 8 J. POL. PHIL. 227 (2002). A related idea is cosmopolitan citizenship and the construction of a community based on shared values. *See* Sandel, *supra* note 10, at 145.

38. *See infra* Section III.B.iv, Part IV.

39. Schragger, *supra* note 28, at 1557.

40. *See generally* Charles M. Tiebout, *A Pure Theory of Local Expenditures*, 64 J. POL. ECON. 416 (1956). Although the phrase has been ascribed to Tiebout, he never actually used that wording in his work.

what matters for businesses and skilled workers is access to the right places with the right people — agglomeration results in restricted capital and labor mobility, unlocking, in turn, the potential for democratic experiments on the local level. [41]

We observe that in the technology arena, Schragger's model may shed more light on urban data initiatives in bigger rather than middle-sized cities. For example, in Louisville, Kentucky, despite the city advancing legal changes at Google's behest to facilitate the installation of Google's high-speed internet service, the company recently pulled out of the medium-sized city.[42] Conversely, despite protests and a pending privacy lawsuit, Sidewalk Labs continued to move ahead on its Quayside smart city project in the larger city of Toronto until the economic uncertainty resulting from the COVID-19 pandemic led the firm to withdraw from the project.[43] However, the sphere for experimentation that agglomeration opens up for cities is circumscribed by both federal and state law factors such as a general lack of constitutional status for U.S. cities and the very broad ability of states to preempt local laws and policy initiatives.[44] Schragger strongly emphasizes the lasting shift from rural to urban in American demographics that has yet to be encapsulated in law and power distribution.[45] Recently, academic discussions of both federalists and localists zoom in on aggressive new preemption measures enacted in the United States primarily by red states that target blue cities' regulatory experiments.[46] In the data privacy field, however, U.S. cities have fared somewhat better and have successfully regulated both city agency data collection and the

---

41. Schragger, *supra* note 28, at 1549–50.

42. Chris Welch, *Google Fiber Is Leaving Louisville in Humiliating Setback*, VERGE (Feb. 7, 2019), https://www.theverge.com/2019/2/7/18215743/google-fiber-leaving-louisville-service-ending [https://perma.cc/G9N9-BCJD].

43. *See infra* note 312 and accompanying text.

44. *See* RICHARD BRIFFAULT & LAURIE REYNOLDS, CASES AND MATERIALS ON STATE AND LOCAL GOVERNMENT LAW 289–90, 327–28 (8th ed. 2016) (unpacking the U.S. Supreme Court's doctrine that cities are creatures of their states). For a Canadian equivalent — treating cities as creatures of their provinces — see the 1997 decision of the Ontario Superior Court in East York v. Ontario (Att'y Gen.) (1997), 34 O.R. 3d 789 (Can. Ont. Gen. Div.)

45. Richard Schragger, *The Attack on American Cities*, 96 TEX. L. REV. 1163, 1166–68 (2018) (arguing that the equal representation of states in the Senate privileges less populous rural areas over densely populated cities, and so do gerrymandering and state and congressional districting).

46. *Id.*; *see also* Kenneth A. Stahl, *Preemption, Federalism, and Local Democracy*, 44 FORDHAM URB. L.J. 133, 136–37 (2017). *See generally* Davidson, *supra* note 36.

purchase and use of surveillance technologies.[47] In fact, cities possess the legal power to do so, and relevant state laws do not preempt them due to what one of the co-authors has described elsewhere as the Fair Information Practice Principles' (FIPPs) gap (meaning that the federal Privacy Act and its state analogs only apply to data collection and use by federal and state agencies, but not by local ones) and the public surveillance gap (meaning that federal surveillance law typically does not limit surveillance in public spaces and city surveillance ordinances have filled in this gap).[48]

Privacy regulation of the commercial sector is more complicated as the sectoral approach to privacy in U.S. law would mean that localities would need to navigate around federal law governing entire sectors such as credit, healthcare, and finance.[49] Commercial privacy regulation is attempted by a few states — notably in California through the newly enacted California Consumer Privacy Act (CCPA), which went into force in 2020.[50] The statute is expected to be influential well beyond Californian borders[51] and is already being discussed in congressional hearings that consider proposals for a U.S. federal consumer privacy bill.[52] The CCPA explicitly preempts "all rules, regulations, codes, ordinances, and other laws" adopted at the local level "regarding the collection and sale of consumers' personal information by a business."[53] Thus, local commercial privacy regulation represents another potential gap for local privacy law but a harder one to fill by cities — instead, several U.S. cities have attempted a case-by-case quasi-regulation of the private sector through initiating lawsuits against private companies that mishandle

47. *See* Rubinstein, *supra* note 3, at 2035.

48. *Id.* at 1974–79.

49. *See* Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2011); Gramm–Leach–Bliley Act (GLBA), 15 U.S.C. § 6803 (2012); Health Insurance Portability and Accountability Act Regulations (HIPAA), 45 C.F.R. pt. 164 (2012).

50. California Consumer Privacy Act (CCPA), CAL. CIV. CODE § 1798.175 (2019).

51. Many other U.S. states have introduced bills regulating commercial (consumer) privacy — in 2019 alone, 25 states and Puerto Rico introduced or filed such bills. *See* Anupam Chander et al., *Catalyzing Privacy Law* 30 (Univ. of Colo. Law Sch., Working Paper No. 19-25, 2019), https://ssrn.com/abstract=3433922 [https://perma.cc/D9TQ-UGE5] (arguing that many of the state bills closely resemble the CCPA).

52. *See GDPR and CCPA: Opt-ins, Consumer Control, and the Impact on Commerce and Innovation Before the S. Comm. on the Judiciary*, 116th Cong. (2019), https://www.judiciary.senate.gov/meetings/gdpr-and-ccpa-opt-ins-consumer-control-and-the-impact-on-competition-and-innovation [https://perma.cc/6A35-YKCU].

53. CAL. CIV. CODE § 1789.180.

data under state and city consumer protection laws. Despite the controversy in federalist debates over what constitutes the "local,"[54] in order to be regulated effectively (in subsidiarity parlance),[55] the credit and finance sectors arguably need national (and perhaps even an international threshold) regulation. In both Spain and Canada, unlike in the United States, a comprehensive statutory framework already regulates commercial privacy at the European level in the European Union (the General Data Protection Regulation (GDPR))[56] and the federal level in Canada (the Personal Information Protection and Electronic Documents Act (PIPEDA)).[57]

In sum, U.S. cities' legal powers in the field of privacy are substantial within a few narrow areas. However, in the mismatch between cosmopolitan and other cities' rising economic and societal importance and constrains on their legal and fiscal autonomy — a discrepancy lamented at least since Gerald Frug published his seminal work *City Making*[58] — preemption is but one aspect on the scale of city power versus powerlessness. Granted, major blue cities in large, blue states in the United States might be seen as the bulwarks of progressive federalism.[59] This is because the preemption of regulation on the state level, although it does occur,[60] is far less disruptive than the overreaching preemption enacted by red states against blue localities that stretches to punitive measures.[61] However,

---

54. Briffault, *supra* note 27, at 2020–21 (showing, for example, that gun violence has a local dimension insofar as it impacts local services such as hospitals or that through the management of waste disposal, local governments become sensitized about nonbiodegradable products addressing the "ostensibly nonlocal problem of climate change").

55. For the most articulate legal incarnation of the principle of subsidiarity, see Consolidated Version of the Treaty on the Functioning of the European Union art. 5, Oct. 26, 2012, 2012 O.J. (C326) 1; *see also* Yishai Blanc, *Federalism, Subsidiarity, and the Role of Local Governments in the Age of Global Multilevel Governance*, 37 FORDHAM URB. L.J. 509, 531–32 (2010).

56. General Data Protection Regulation, 2016/679, 2016 O.J. (L 119).

57. Personal Information Protection and Electronic Documents Act, S.C. 2000, ch. 5 (Can.).

58. *See generally* GERALD FRUG, CITY MAKING: BUILDING COMMUNITIES WITHOUT BUILDING WALLS (2001).

59. Heather K. Gerken, *A New Progressive Federalism*, DEMOCRACY 38 (2012).

60. *See* Schragger, *supra* note 28, at 1566.

61. RICHARD BRIFFAULT ET AL., AM. CONSTITUTION SOC'Y FOR LAW & POLICY, THE TROUBLING TURN IN STATE PREEMPTION: THE ASSAULT ON PROGRESSIVE CITIES AND HOW CITIES CAN RESPOND 1 (2017), https://www.acslaw.org/wp-content/uploads/2017/09/ACS_Issue_Brief_-_Preemption_0.pdf [https://perma.cc/HH8Y-E84A] ("States have adopted statutes that threaten to withhold funding and expose cities to private liability in preemption conflicts as well as enacted laws that seek to impose personal civil penalties — and in some instances,

these major blue cities might also face disempowerment based on fiscal constraints.

B. Cosmopolitan Ambitions versus (Fiscal) Autonomy

In terms of economic power, not only are cosmopolitan cities responsible for a significant percentage of revenue and taxes in their respective states and the national economy as a whole, but their gross metropolitan product may exceed that of many states.[62] That said, perhaps as a result of municipal giveaways to railroad interests and overspending on other forms of infrastructure in the past, many U.S. states have circumscribed metropolitan revenue-raising even in their largest cities. Dillon's rule — the doctrine restricting local governments' law-making authority only to explicit grants of such power by the state — emerged in the United States and spread throughout Canada amidst various fiscal concerns.[63] Further, progressive reformers of the past century sought to "limit the capacity for [city] governments to take on debt by entrenching debt limitations into state constitutions."[64] The European context is somewhat comparable: European Union-wide austerity measures following the European debt crisis in 2009 led Spain to reverse its prior Keynesian approach resulting in cutbacks on local fiscal autonomy and the enactment of legal measures aimed at general recentralization after 2010.[65] Although most U.S. states have long since replaced Dillon's rule with a broader mandate for local autonomy under home rule,[66] and Canadian cities emancipated themselves around 2005 to obtain

---

even potential criminal liability — on mayors, city council members, police chiefs and other local officials who defy state legislation.").

62. *See* U.S. CONF. OF MAYORS & COUNCIL ON METRO ECONS, U.S. METRO ECONOMIES: ECONOMIC GROWTH AND FULL EMPLOYMENT, ANNUAL GMP REPORT (2018); Schragger, *supra* note 45, at 1168 ("Cities and their wider metropolitan areas now contain the bulk of the American population and are the primary economic drivers of their states, their regions, and the nation.").

63. *See* Ron Levi & Mariana Valverde, *Freedom of the City: Canadian Cities and the Quest for Governmental Status*, 44 OSGOODE HALL L.J. 410, 415–16 (2006) (detailing the origins and spread of Dillon's rule to Canada).

64. Schragger, *supra* note 28.

65. Carmen Navarro & Esther Pano, *Spanish Local Government and the Austerity Plan: In the Eye of the Perfect Storm*, *in* LOCAL PUBLIC SERVICES IN TIMES OF AUSTERITY ACROSS MEDITERRANEAN EUROPE 100 (Andrea Lippi & Theodore Tsekos eds., 2019) (discussing a correlation between recentralization and austerity in the aftermath of the Euro-crisis in Spain).

66. Briffault, *supra* note 27, at 2011 (describing the home rule as the commitment to local law-making capacity, codified in the constitutions and statutes of the vast majority of states).

certain concessions of autonomy from their provinces,[67] remnants of Dillon's Rule persist in North America in terms of fiscal restraints on local governments. New York, for example, limits the amount raised by taxes on real estate in New York City in any fiscal year to 2.5% of the average full valuation.[68] Similarly, the pendulum has swung back in Spain, where in 2019, the center-left Prime Minister proposed substantial increases in public spending for the region of Catalonia (where Barcelona is located). However, the measure was not approved as Catalonians saw it as an insufficient grant of fiscal autonomy.[69]

Cities worldwide are experiencing similar problems. A central issue is described as "offloading" — an abdication of responsibility on the side of state or federal/central governments from the provision of urban infrastructure coupled with the reduction in federal or state grants for urban centers.[70] Cities are expected to fill in the gap while demands for infrastructure updates and the need for new services are constantly on the rise due to rapid population growth and immigration. In addition to challenges in the availability of affordable housing, poverty levels, traffic congestion, and other transit problems, cities now face new challenges brought by the digital revolution, such as closing the digital divide and boosting urban information infrastructure. Privacy considerations are intrinsically linked to the agglomeration of data, including personally identifiable data, on the local level. Local governments amass data not only as a result of providing the usual municipal services to local citizens (transportation, housing, sanitation, education and libraries, health and social services, and public safety) but also due to their growing embrace of data-driven products and services. Cities worldwide attempt to transform themselves by taking advantage of data analytics, social engagement, and big data.[71] The digital revolution has led to urban investments in information technology (IT) infrastructure as never before with the dual goals of enhancing and improving municipal services (especially social services and

67. Levi & Valverde, *supra* note 63, at 415–30.

68. Schragger, *supra* note 45, at 1179.

69. Omar G. Encarnación, *Will Spain Become a Victim of the Catalan Separatists?*, N.Y. TIMES (Feb. 25, 2019), https://www.nytimes.com/2019/02/25/opinion/spain-catalonia-election.html [https://perma.cc/APB3-UHLV].

70. *See generally* Levi & Valverde, *supra* note 63.

71. *See generally* GOLDSMITH & KLEIMAN, *supra* note 14.

policing)[72] and ensuring greater access to technology through broadband initiatives and investments in the local technology workforce.[73] Local financial dependence on private investment to create and maintain such infrastructure results in a special symbiosis with businesses that arguably delineates the outer boundaries of regulatory experimentation on the city level. Local governments can seek to circumvent debt and taxing limitations in many ways, including through licensing and fees. Related to privacy, we see that some cities require data (including personally identifiable information) instead of fees for licensing data-intense services such as ride- or home-share companies like Uber and Airbnb.[74] It is difficult to find direct causation between low levels of fiscal autonomy and attempts for "data regulation" instead of direct taxation. It is safe to say, however, that cities worldwide are facing general legal and fiscal constraints relative to their elevated societal and economic status and new responsibilities. Such constraints may dictate decisions cities take to enter into legal arrangements that are favorable to private companies but damaging to privacy.

Even so, cities are left with plenty of legal ammunition in the privacy field. As in the case of land use planning in the United States, the question is not whether a city has power, but how it chooses to exercise its extensive power. As cities experiment with data-driven services, they are not forced into making concessions to tech giants but may do so simply by agreeing to commercial terms that outsource public functions or disfavor privacy as a matter of choice. One example is New York City's obtaining "free" (i.e., ad-funded) technology and telecommunications services for local citizens in the aforementioned "LinkNYC" deal with Sidewalk Labs,[75] or requiring non-anonymized data from Airbnb to enforce city housing regulations without imposing tax burdens.[76] Another is Toronto's decision to outsource the development and management of a parcel on its waterfront to Sidewalk Labs without fully addressing the privacy implications of the deal despite the existence, in Canada, of solid federal and provincial privacy laws that Toronto could have

---

72. *See* Rubinstein, *supra* note 3, at 1964–65. *See generally* ANDREW FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017).

73. *See generally infra* Part III.

74. See *infra* Sections III.B.i–ii.

75. *See infra* Section III.B.i.

76. *See infra* Section III.B.ii.

used as leverage in their negotiations.[77] This decision was in keeping with Toronto's initial disregard of the long-term impact of the deal on the city's autonomy vis-à-vis a powerful tech company. Such data deals are cut without sufficient deliberation about whether local residents truly wish to exchange privacy and public control over public places for the promise of improved efficiency and greater convenience.[78]

The symbiosis between city governments and tech companies is mirroring, on the subnational level, the important transformation of law and legal standards that Julie Cohen compellingly traces on the supra-national level.[79] As both businesses and governmental institutions transition from industrial to data-intense, informational capitalist models, U.S. cities exemplify that transition: they function as a hybrid between a public institution seeking to act in the public interest and a business corporation seeking to maximize profits. Interestingly, this trend — that we coin as "data stewardship" — co-exists with cities' public litigation efforts that promote privacy — a trend that we call "privacy activism." Public lawyers typically defend their governmental clients when litigation is initiated against them. Yet, as pointed out by the City Attorney of San Francisco,[80] lawyers in a city's law department can also act as civil plaintiffs invoking federal, state, and city law in the public interest. Data activism is an example of just how cities make use of existing powers to expand their sphere of policy experimentation.

---

77. See *infra* Section III.B.iv.

78. *See* Susan Crawford, *Beware of Google's Intentions*, WIRED (Feb. 1, 2018), https://www.wired.com/story/sidewalk-labs-toronto-google-risks/ [https://perma.cc/GB9S-5D4X] (stating that "it is not clear whether Toronto will gain any useful insights from its partnership with Google. Meanwhile, Google will be gaining insights about urban life including energy use, transit effectiveness, climate mitigation strategies, and social service delivery patterns — that it will then be able to resell to cities around the world. Including, perhaps, Toronto itself.").

79. *See generally* JULIE COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019). *See also* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

80. JILL HABIG ET AL., LOCAL ACTION, NATIONAL IMPACT: A PRACTICAL GUIDE TO AFFIRMATIVE LITIGATION FOR LOCAL GOVERNMENTS 4 (2019), https://www.sfcityattorney.org/wp-content/uploads/2019/04/A-Practical-Guide-to-Affirmative-Litigation-FINAL-4.13.19-1.pdf?fbclid=IwAR3QB-jbCANH4rTK5jGE36vFgqEZOEnhPBrk237Z_1nBnkGAcmTx_932bLA [https://perma.cc/NX5V-J4DP].

II. THE CITY AS PRIVACY ACTIVIST

Some of the big, cosmopolitan cities we examine have been active in trying to safeguard privacy-as-political participation in an issue with national ramifications: the 2020 Census citizenship litigation. Others have initiated lawsuits against major firms like Facebook and Equifax for privacy violations affecting local residents. This Part examines cities as privacy activists in both sets of cases.

A. Data Wars: Privacy and Political Participation

Data is power. By trying to protect the personal information of their immigrant populations, states and cities are trying to safeguard local autonomy and ensure political participation. As Professor Ilya Somin remarks: "State and local governments have extensive information about hundreds of millions of people that the federal government could abuse in many ways."[81] Such abuse of data could stifle federalism's institutional structure for allowing minorities to take part in governance, what Heather Gerken has called "the loyal opposition."[82] Urban power measured in political representation and the disbursement of state and federal funds depends on cities' population size. But urban population size often correlates with diversity. In terms of demographics, global cities like New York, San Francisco, Chicago, Seattle, and Washington, D.C. are homes to very diverse populations, many of whom are immigrants such that lack of privacy about their legal status may result in severe consequences including deportation proceedings.[83] Urban power can, therefore, be indirectly connected to policies favoring the preservation of the data privacy of these vulnerable populations.

In May 2017, President Trump established the (now defunct) Presidential Advisory Commission on Election Integrity.[84] The Commission was supposed to collect a large pool of voter's personal

---

81. Ilya Somin, *Making Federalism Great Again: How the Trump Administration's Attack on Sanctuary Cities Unintentionally Strengthened Judicial Protection for State Autonomy*, 97 TEX. L. REV. 1248, 1283 (2019) [hereinafter Somin, *Making Federalism Great Again*].

82. Heather K. Gerken, *The Loyal Opposition*, 123 YALE L.J. 1958, 1960 (2014).

83. *See generally* Anil Kahan, *The Fourth Amendment and Privacy Implications of Interior Immigration Enforcement*, 41 U.C. DAVIS L. REV. 1137 (2008).

84. Charles Steward III, *Trump's Controversial Election Integrity's Commission Is Gone. Here's What Comes Next*, WASH. POST (Jan. 4, 2018), https://www.washingtonpost.com/news/monkey-cage/wp/2018/01/04/trumps-controversial-election-integrity-commission-is-gone-heres-what-comes-next/ [https://perma.cc/TE8E-75AX].

data from election officials in states, including names, addresses, dates of birth, political affiliations, voter histories, criminal records, military status, and partial social security numbers.[85] The government's purported justification — to fight voter fraud via access to state voter registration databases — was seen by many as an ill-masked attempt to restrict voting rights.[86] Forty-four states, including many Republican-led state governments, and the District of Columbia, invoked privacy, among other reasons, to reject some or all of the government's demands.[87] Many of the opposing states filed lawsuits, and civil society organizations also initiated legal actions on privacy grounds under federal law.[88] Finally, the government decided to discontinue the existence of the Commission, citing state resistance and its choice to not "engage in endless legal battles" — battles that commentators indicated the administration probably expected to lose.[89] The Election Integrity Commission episode throws in sharp relief the connection between data and power on the one hand, and privacy and local autonomy on the other.

More recently, the Trump Administration's crackdown on immigration has been countered by local efforts to oppose the federal government's deportation of undocumented immigrants.[90] In turn, the federal government has fought back not only by directly challenging sanctuary cities but also by leveraging new data wars that threaten to curtail local autonomy significantly.[91] We argue that the Census 2020 litigation, in which states and cities were the first to file a case against the Department of Commerce's decision to insert a

---

85. *Id.*; *see also* Letter from Kris W. Kobach, Vice Chair, Presidential Advisory Comm'n on Election Integrity, to Hon. Matt Dunlap, Sec'y of State (June 28, 2017), http://i2.cdn.turner.com/cnn/2017/images/06/30/peic.letter.to.maine%5b2%5d.pdf [https://perma.cc/ENZ2-WZHA].

86. *Fresh Air: Trump's Election Integrity Commission Could Have A 'Chilling Effect' On Voting Rights*, NAT'L PUB. RADIO (May 17, 2017), https://www.npr.org/2017/05/17/528769195/trumps-election-integrity-commission-could-have-a-chilling-effect-on-voting-righ [https://perma.cc/MT43-8QSN].

87. Ilya Somin, *Demise of Trump Voter Fraud Commission Is a Victory for Federalism*, VOLOKH CONSPIRACY (Jan. 4, 2018), https://reason.com/2018/01/04/demise-of-trump-voter-fraud-commission-i/ [https://perma.cc/382Y-MZKM].

88. The first case filed by a civil society organization was a suit brought in Washington, D.C. by the Electronic Privacy Information Center (EPIC). *See EPIC v. Presidential Election Commission*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/litigation/voter/epic-v-commission/ [https://perma.cc/25Y6-BW3J] (last visited Jan. 25, 2020).

89. Somin, *supra* note 87, at 2.

90. *See* Somin, *Making Federalism Great Again*, *supra* note 81, at 1247–48.

91. *See infra* Section II.A.i.

citizenship question in the 2020 census, is best understood against the backdrop of the administration's attempts to discipline sanctuary jurisdictions.

i. The Census 2020 Citizenship Question Through the Prism of Sanctuary Cities

In 2017, California declared itself "a sanctuary state." As a part of its sanctuary policies, the state enacted Senate Bill 54, restricting the range of information state and local governments are allowed to share with federal immigration enforcers,[92] and Assembly Bill 450, prohibiting employers from voluntarily allowing a federal immigration enforcement agent to enter "nonpublic" areas of their workplaces or to access, review, or obtain employees' records.[93] In response, the Trump Administration sought to aggressively enforce 8 U.S.C. Section 1373, a federal law mandating that a federal, state, or local government entity or official may not prohibit, or in any way restrict, any government entity or official from sending to, or receiving from, the (former) Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.[94] Section 1373 predates the Trump Administration by decades and has been the subject of prior federalism challenges by some of the jurisdictions involved in the citizenship imbroglio.[95] The novelty of the Trump Administration's effort is to legally tie federal enforcement to punitive measures, thereby turning Section 1373 into a grant condition for federal funding of local governments.[96] The Trump Administration also evoked Section 1373 to challenge the legality of California's sanctuary laws; litigation is ongoing.[97] The case has been framed as one about

92. CAL. GOV'T CODE §§ 7284.6(a)(1)(C)–(D) (2018).

93. CAL. GOV'T CODE §§ 7285.1–2 (2018).

94. 8 U.S.C. § 1373(a) (1996).

95. *See* City of New York v. United States, 505 U.S. 144, 157 (1992) (the City relied on *Printz v. United States*, 521 U.S. 898, 907 (1997), but the Tenth Circuit distinguished the cases). In an earlier case, *Sturgeon v. Brathon*, 95 Cal. Rptr. 3d 718 (2009), California litigated against Section 1373. *See also* Bill Ong Hing, *Immigration Sanctuary Policies: Constitutional and Representative of Good Policing and Good Policy*, 2 U.C. IRVINE L. REV. 247, 263 (2012).

96. *See* Exec. Order No. 13,768, 82 Fed. Reg. 8799 (Jan. 25, 2017); *see also* Somin, *Making Federalism Great Again*, *supra* note 81, at 1248.

97. *See* United States v. California, 314 F. Supp. 3d 1077, 1101 (E.D. Cal. 2018) (interpreting Section 1373 narrowly to avoid conflict with California's Senate Bill 54).

local enforcement of immigration law and federalism.[98] However, these issues closely intersect with privacy, given that the challenged laws attempt to safeguard the personal information of California's immigrant population. Many California cities (including San Francisco) have sided with the state sanctuary policies based on a narrower interpretation of Section 1373.[99]

Several of the cities examined in this Article (New York City, Seattle, San Francisco, and Chicago) have litigated on their own or joined a coalition of states against the government's mandate of cooperation in deporting illegal immigrants as a condition of receiving federal grants to localities.[100] The Census 2020 litigation, in which many sanctuary cities have taken part, is not directly about federalism, much like the sanctuary cities' litigation is not directly about the protection of personal information. No matter the legal framing, however, the context of the litigation in the Census 2020 cases reveals a pattern: for local autonomy to exist, the privacy of national minorities who make up the majority in big urban centers needs to be preserved.

ii. The Census 2020 Litigation in Focus[101]

The U.S. Constitution explicitly mandates the government to conduct a census every ten years.[102] The federal government collects census data on all persons residing in the United States, regardless of their legal status, to apportion state representatives to the House of Representatives, to draw political districts and allocate power to them, as well as to allocate hundreds of billions of dollars in federal, state, and local funds.[103] Simultaneously, census data is used for

98. *See* Somin, *Making Federalism Great Again*, *supra* note 81, at 1252 (arguing that Section 1373 might violate the Tenth Amendment, which has been interpreted, according to established precedents that go back to *Printz*, to bar federal "commandeering" of state and local governments).

99. Steinle v. City & County of San Francisco, 230 F. Supp. 3d 994, 1006 (N.D. Cal. 2017).

100. Somin, *Making Federalism Great Again*, *supra* note 81, at 1259–60.

101. This Section builds on Marc Rotenberg & Bilyana Petkova, *U.S. Supreme Court Blocks Citizenship Question on 2020 US Census, Trump Issues Executive Order to Collect Citizenship Data*, 5 EUR. DATA PROTECTION L. REV. 453 (2019).

102. U.S. CONST. amend. XIV, § 2.

103. *See Counting for Dollars 2020: The Role of the Decennial Census in the Geographic Distribution of Federal Funds*, GEO. WASH. INST. PUB. POL'Y (Feb. 10, 2020), https://gwipp.gwu.edu/counting-dollars-2020-role-decennial-census-geographic-distribution-federal-funds [https://perma.cc/F2Q3-V8RK].

demographic purposes and has habitually included respondents' race, sex, age, and whether they own or rent a home.[104]

> Since 1960, the decennial census questionnaire distributed to all households . . . has excluded a question on citizenship . . . . The Census Bureau has stated that to ask this question increases the difficulty of counting already "hard-to-count" groups — particularly non-citizens and Hispanics — whose members would be less willing to participate for fear that their data could be used against them.[105]

In March 2018, Secretary of Commerce Wilbur Ross announced that he would add the citizenship question to the Census for 2020 to assist the Department of Justice (DOJ) in enforcing the Voting Rights Act (VRA).[106] Various plaintiffs challenged the decision in court.[107] The plaintiffs included a coalition of 15 states and a number of cities and counties as well as non-governmental organizations that support immigrants.[108] They raised two challenges: first, that the decision violated the Administrative Procedure Act (APA), which prohibits federal agencies from acting in an arbitrary manner; second, that the decision violated the Due Process Clause of the Fifth Amendment because it was motivated in part by invidious discrimination against immigrant communities of color.[109]

---

104. *See* Beth Jarosz & Paola Scommegna, *Why Are They Asking That? What Everyone Needs to Know About 2020 Census Questions*, POPULATION REFERENCE BUREAU (Aug. 13, 2019), https://www.prb.org/why-are-they-asking-that-what-everyone-needs-to-know-about-2020-census-questions/ [https://perma.cc/5FU9-XPYR]; Issie Lapowsky, *The Challenges of America's First Online Census*, WIRED (Feb. 6, 2019 12:07 PM), https://www.wired.com/story/us-census-2020-goes-digital/ [https://perma.cc/6XVW-L6EM]; Kim Parker et al., *Chapter 1: Race and Multiracial Americans in the U.S. Census*, PEW RES. CTR. (June 11, 2015), https://www.pewsocialtrends.org/2015/06/11/chapter-1-race-and-multiracial-americans-in-the-u-s-census/ [https://perma.cc/DG5C-KYMX].

105. Bilyana Petkova, *Citizenship Data Wars*, INT'L J. CONST. L. BLOG (July 24, 2019), http://www.iconnectblog.com/2019/07/citizenship-data-wars [https://perma.cc/2PWC-RWXA].

106. Salvador Rizzo, *The Four Pinocchio Claim at the Center of the Census Citizenship Question*, WASH. POST (Apr. 22, 2019, 3:00 AM), https://www.washingtonpost.com/politics/2019/04/22/four-pinocchio-claim-center-census-citizenship-question/ [https://perma.cc/GA9P-8MZW].

107. *See id.*

108. Hansi Lo Wong, *15 States Say Unauthorized Immigrants Should Continue to Count for Seats in Congress*, NAT'L. PUB. RADIO (Sept. 6, 2019 8:45 PM), https://www.npr.org/2019/09/06/754685703/15-states-say-unauthorized-immigrants-should-continue-to-count-for-seats-in-cong [https://perma.cc/8ZYQ-KTHT].

109. New York v. U.S. Dep't of Commerce, 315 F. Supp. 3d 766, 773 (S.D.N.Y. 2018).

Writing for the district court, Judge Furman sided with the plaintiffs, finding that an undercount would translate into a loss of political power and funds for states and localities.[110] The court also found that, in states with large migrant populations (like California and New York), an undercount might result in both the loss of a congressional seat[111] and dilution of the political power of certain cities within their states.[112] In addition, since national census data is also used for a range of municipal purposes, the court accepted as an injury, in fact, New York City's and Chicago's argument for a diversion of resources to counteract the potentially harmful effects of data distortion that inserting a citizenship question to the census might cause.[113] Finally, the court found that the government's stated rationale for restoring the citizenship question — to promote enforcement of the VRA — was pretextual and thus violated the APA.[114] But, the court rejected the claim that the Secretary of Commerce was motivated by invidious discrimination in violation of the equal protection component of the Due Process Clause.[115] The government then appealed the decision directly to the Supreme Court.[116]

In a long and divided opinion authored by Chief Justice Roberts, the Court left in place the injunction blocking the citizenship question from the 2020 Census.[117] Chief Justice Roberts was satisfied with the evidence showing that the reluctance of noncitizen households' to answer the citizenship question would depress census data.[118] This, in

---

110. Somin, *Making Federalism Great Again*, *supra* note 81, at 1248.

111. Emily Badger, *A Census Question That Could Change How Power Is Divided in America*, N.Y. TIMES (July 31, 2018), https://www.nytimes.com/2018/07/31/upshot/Census-question-citizenship-power.html [https://perma.cc/7XEH-66DQ]. In California, the decision not to litigate was possibly motivated by an interstate split between sanctuary and non-sanctuary cities. *See generally* Rose Cuison Villazor & Prateepan Gulasekaram, *The New Sanctuary and Anti-Sanctuary Movements*, 52 U.C. DAVIS L. REV. 549 (2018).

112. As the court explained, this problem arises for cities that are home to a disproportionate share of their states' noncitizen populations. *U.S. Dep't of Commerce*, 315 F. Supp. 3d at 789; New York v. U.S. Dep't of Commerce, 351 F. Supp. 3d 502, 595 (S.D.N.Y. 2019). New York City, for example, "contains approximately forty-three percent of the total state population, but approximately seventy-one percent of the state's noncitizen population." *U.S. Dep't of Commerce*, 351 F. Supp. 3d at 595.

113. *U.S. Dep't of Commerce*, 351 F. Supp. 3d at 603.

114. *Id.* at 635.

115. *Id.* at 671.

116. U.S. Dep't. of Commerce v. New York, 139 S. Ct. 2551, 2565 (2019).

117. *See generally id.*

118. *Id.* at 2565–66.

turn, would result in a number of injuries — diminishment of political representation, loss of federal funds, overall degradation of census data, and diversion of resources — satisfying the "injury in fact" standing requirement.[119] However, the Chief Justice concluded that the Secretary of Commerce was within his discretion to weigh the benefits of completeness and accuracy of census data in favor of completeness and against the recommendation of the Census Bureau.[120] Contrary to what the district court found, uncertainty about the reasons behind underreporting was not unjustified, and the Secretary of Commerce's policymaking discretion did not need to be subordinated to the technocratic expertise of the Bureau. In other words, the Chief Justice found that inserting a citizenship question in the census was a policy choice within the range of reasonable options before the Secretary of Commerce.[121] Despite this partial reversal of the District Court's judgment, the Chief Justice finally affirmed Judge Furman's opinion by stating that there was a "significant mismatch between the decision the Secretary made and the rationale he provided."[122]

If the Trump Administration succeeds in its anti-sanctuary measures, it will assert broad power to impose new conditions on federal grants to state and local governments, thereby suppressing political dissent in these jurisdictions. It is worth questioning the Administration's attempt to achieve the same goal — disempowering its state and city political opponents — by waging data wars. Approximately two weeks after the Supreme Court decision in the census case, President Trump issued an Executive Order establishing "an interagency working group with a goal of making available to the Department administrative records showing citizenship data for 100 percent of the population."[123] The new rationale for this extensive data collection is the identification of those who are eligible for public benefits. The Executive Order continues, "data identifying citizens will help the Federal Government generate a more reliable count of the unauthorized alien population in the country."[124] A subsequent statement describes a recent "massive influx of illegal immigrants at our southern border," states that "hundreds of thousands of aliens who entered the country illegally have been released into the interior

119. *Id.* at 2565.
120. *Id.* at 2570–71.
121. *Id.* at 2565.
122. *Id.* at 2575.
123. Exec. Order 13,880, 84 Fed. Reg. 33,821 (July 16, 2019).
124. *Id.*

of the United States pending the outcome of their removal proceeding," and warns that "more than 1 million illegal aliens who have been issued final removal orders from immigration judges . . . remain at-large in the United States."[125]

There is a limited constitutional right to information privacy in the United States,[126] and privacy injuries are often insufficient to show standing, let alone sustain a substantive claim.[127] The unresolved constitutional crossover between privacy and antidiscrimination law has a long pedigree that goes back to at least *Roe v. Wade*[128] and *Lawrence v. Texas*.[129] Moreover, although the substantive due process might have been eschewed for extracting a right to bodily privacy in *Griswold v. Connecticut* due to its Lochner-era connotations,[130] due process has resurfaced in relation to information privacy and anti-discrimination concerns in the context of big data.[131] As Justice Breyer wrote in his concurring opinion on the citizenship question, studies by the Census Bureau found that "Hispanics were significantly more likely than were non-Hispanics to stop answering at the point they reached the citizenship question."[132]

In substance, the Census 2020 litigation is about making available the personal information of vulnerable immigrant populations concentrated in big urban centers to the federal government. The gap in constitutional protection led the justices to decide the case only on administrative law grounds under the APA. That said, the lower court ruling and the Roberts opinion emphasized that the violation of the APA alone was substantial, given the statutory protection of core constitutional and democratic values of accountability.[133] President Trump's Executive Order appears to contemplate the collection of personal data concerning citizenship status for statistical purposes, and the use of citizenship data for determinations about public

---

125. *Id.*

126. *See, e.g.*, Fred H. Cate & Beth E. Cate, *The Supreme Court and Information Privacy*, 2 INT'L DATA PRIVACY L. 255, 258 (2012).

127. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 807–08 (6th ed. 2017).

128. 410 U.S. 113 (1973).

129. 539 U.S. 588 (2003).

130. *See* 381 U.S. 479, 488 (1965); Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 744–45 (1989).

131. Jason Schultz & Kate Crawford, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 99–100 (2014).

132. U.S. Dep't. of Commerce v. New York, 139 S. Ct. 2551, 2588 (2019).

133. *Id.* at 2575; New York v. United States Dep't of Commerce, 333 F. Supp. 3d 282, 291 (S.D.N.Y. 2018).

benefits and possible deportation.[134] It, therefore, seems possible that the census case may return to the Supreme Court to determine again whether the decision to collect data about citizenship is a renewed "contrivance,"[135] similar to those evoking election fraud and the enforcement of the VRA.[136]

B. City Attorneys General as Data Privacy Enforcers

Cities have litigated against the federal government to preserve the personal information of city dwellers and safeguard diversity, local autonomy, and political participation. They have also fought to protect the public interest against private parties that violate the privacy of their residents. Although state attorneys general (AGs) have a proven track record in privacy enforcement,[137] city AGs are emerging now as new players at the forefront of consumer privacy enforcement. States have their own versions of the Federal Trade Commission Act (FTCA),[138] as well as other privacy and consumer protection laws that city AGs can invoke in court either directly or under municipal law. Often, a state's mini-FTCA and related privacy statutes are worded more broadly than their federal counterparts. In addition, the FTC has no immediate fining authority (unless a firm violates the terms of a consent decree), whereas state law permits city AGs to directly claim (not insignificant) civil penalties.[139]

The cases discussed below are among the first instances in which city AGs use state consumer protection legislation for privacy protection. Importantly, such suits can proceed even if the violating

---

134. On the same day that the President issued the Executive Order, *The New York Times* reported that Immigration and Customs Enforcement would renew "[n]ationwide raids to arrest thousands of members of undocumented families." Caitlin Dickerson & Zolan Kanno-Youngs, *Thousands Are Targeted as ICE Prepares to Raid Undocumented Migrant Families*, N.Y. TIMES (July 11, 2019), https://www.nytimes.com/2019/07/11/us/politics/ice-families-deport.html [https://perma.cc/93LK-2FPB]. According to the *Times*, the "operation, backed by President Trump, had been postponed, partly because of resistance among officials at his own immigration agency." *Id.*

135. Rotenberg & Petkova, *supra* note 101, at 457.

136. *See supra* Section II.A.

137. *See* Bilyana Petkova, *The Safeguards of Privacy Federalism*, 20 LEWIS & CLARK L. REV. 595, 619–23 (2016). *See generally* Danielle K. Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016). In the case of Washington, D.C., the state and city attorney are the same.

138. 15 U.S.C. § 45 (2012) (prohibiting unfair or deceptive practices in or affecting commerce).

139. *Id.*

conduct of an online platform or data broker has not taken place beyond the limits of a city's litigation jurisdiction.

i. District of Columbia v. Facebook

Facebook has a decade-long track record of privacy failures, but the recent Cambridge Analytica scandal tops them all.[140] As widely reported in the press,[141] Facebook allowed a researcher, Alexander Kogan, to contact Facebook users about downloading a personality quiz application. Around 270,000 users responded. The application collected not only their data but also harvested the information of all their friends, giving access to the profiles of an estimated 50–70 million people.[142] Kogan then sold this information to a company called Cambridge Analytica, a political data firm that offered to identify the preferences of voters based on their personality traits, friend networks, and Facebook "likes" to influence their behavior with targeted election advertisements.[143] President Trump's 2016 election campaign thereafter hired Cambridge Analytica to gain access to these voter profiles,[144] as did the Brexit campaign.[145] The ensuing scandal gained notoriety precisely because of the number of people affected and the fact that they were voters with political interests, and not merely shoppers with consumer interests. As a result, the public outcry in the Cambridge Analytica scandal has been loud and persistent.

In 2018, the Federal Trade Commission (FTC) launched an investigation of the matter premised on Facebook's violation of a

---

140. *See* James Sanders & Dan Patterson, *Facebook Data Privacy Scandal: A Cheat Sheet*, TECHREPUBLIC (July 24, 2019, 8:52 AM), https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/ [https://perma.cc/9LBX-BFQR].

141. *See* Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/4TH7-A86Q].

142. *See* Sanders & Patterson, *supra* note 140 (reporting the figure was later revised up to "87 million profiles").

143. *See* Granville, *supra* note 141.

144. Paul Lewis & Paul Hilder, *Leaked: Cambridge Analytica's Blueprint for Trump Victory*, GUARDIAN (Mar. 23, 2018), https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory [https://perma.cc/HXJ4-QVFB].

145. Sue Halpern, *Why the U.K. Condemned Facebook for Fueling Fake News*, NEW YORKER (Feb. 22, 2019), https://www.newyorker.com/tech/annals-of-technology/why-the-uk-condemned-facebook-for-fuelling-fake-news [https://perma.cc/GH99-ZKXZ].

2012 consent decree involving data sharing with third-party applications. Under the consent decree, Facebook agreed, among other stipulations, to give users clear and conspicuous notice and to obtain "affirmative express consent" before sharing their data with third parties.[146] Facebook failed to meet this requirement in allowing Kogan to harvest an enormous trove of data and share it with Cambridge Analytica.[147] In July 2019, the FTC imposed a record $5 billion fine against Facebook for violating the 2012 consent decree along with new measures to ensure accountability and transparency.[148] European privacy officials also imposed fines under the then-in-force Data Protection Directive.[149] Despite these actions, civil society organizations like the Electronic Information Privacy Center (EPIC) insisted that privacy regulators must do more to change Facebook's predatory business practices — in particular, arguing that the FTC either failed to follow up on its consent orders or did not do so fast enough.[150] FTC largely leaves tech companies' privacy violations unpunished, revealing a potential enforcement gap. It is this gap that State, and now City, Attorneys are seemingly stepping in to fill.

---

146. David C. Vladeck, *Facebook, Cambridge Analytica, and the Regulator's Dilemma: Clueless or Venal?*, HARV. L. REV. BLOG (Apr. 4, 2018), https://blog.harvardlawreview.org/facebook-cambridge-analytica-and-the-regulators-dilemma-clueless-or-venal/ [https://perma.cc/X496-ZLS5].

147. *Id.*

148. *See FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMMISSION (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/E7B7-BLLA].

149. *See Facebook Fined £500,000 for Cambridge Analytica Scandal*, BBC NEWS (Oct. 25, 2018), https://www.bbc.com/news/technology-45976300 [https://perma.cc/P97T-ALPX]. Much more severe fines could have been pursued under the General Data Protection Regulation (GDPR) that entered into force in May 2018. *See* Ira Rubinstein & Bilyana Petkova, *The International Impact of the GDPR, in* COMMENTARY ON THE GDPR 8 (Marc Cole & Franziska Boehm eds., forthcoming 2020).

150. Under a Freedom of Information Act (FOIA) request, EPIC revealed that since the FTC issued the 2012 Consent Order against Facebook there were 26,000 pending consumer complaints against Facebook on file and not a single legal action. *See EPIC FOIA-FTC Confirms Number of Pending Facebook Complaints, Doubling Every Two Years*, ELECTRONIC PRIVACY INFO. CTR. (Apr. 3, 2019), https://epic.org/2019/04/epic-foia---ftc-confirms-numbe.html [https://perma.cc/3VKJ-43NY]. EPIC is seeking to block the automatic approval of the settlement. *See* Natasha Singer, *Privacy Group Files Legal Challenge to Facebook's $5 Billion F.T.C. Settlement*, N.Y. TIMES (July 26, 2019), https://www.nytimes.com/2019/07/26/technology/facebook-ftc-epic-privacy.html [https://perma.cc/6D59-YJSE].

As a city-state jurisdiction, the position of Washington, D.C., is unique within the United States. In 2018, before the FTC acted, Washington, D.C. Attorney General Karl Racine filed a complaint under the District's Consumer Protection Procedures' Act (CPPA).[151] Racine alleged that Facebook did not meet consumers' reasonable expectations of privacy, including that of more than 340,000 D.C. residents, when it failed to protect their data in the Cambridge Analytica matter. Substantively, the allegations of misrepresentation and lack of reasonable oversight of third-parties' applications in the Racine complaint matched those later raised by the FTC.[152] However, Racine's claim that Facebook needed to notify its users of the unintended use of their data by Cambridge Analytica likely goes a notch further. In terms of remedies, much would depend on what constitutes a single violation under the CPPA. Although the AG had not specified amounts, D.C.'s consumer protection law provides for treble damages or $1500 per violation (whichever is greater), in addition to injunctive relief, punitive damages, and attorney's fees.[153] The AG found the new settlement with Facebook reached by the FTC unsatisfactory and has proceeded further with this litigation. In spite of Facebook's dispute over the D.C. court's jurisdiction, so far, the claim has been allowed to proceed. The D.C. Superior Court asserted that it had jurisdiction since Facebook engaged in continuous and systemic business activities with D.C. residents, acquiring substantial revenue from consumers in the District.[154] Setting aside the question of whether the municipal tier is the right level of regulation when it comes to ensuring privacy protections in the private sector, the example of this case of public interest city litigation, and the one that follows shows that cities are currently flexing their muscle as privacy activists to fill in a perceived regulatory gap.

---

151. Complaint, District of Columbia v. Facebook, Inc., 2018 CA 008715 B (D.C. Super. Ct. 2018).

152. Complaint at 6–7, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. July 24, 2019).

153. *See* Consumer Protection Procedures Act (CPPA), D.C. CODE §§ 28–3905 (2014).

154. *See* Andrew Harris & Daniel Stoller, *Facebook Must Proceed with Privacy Breach Lawsuit*, BLOOMBERG (June 2, 2019), https://www.bloomberg.com/news/articles/2019-06-02/facebook-must-proceed-with-privacy-breach-suit-d-c-judge-rules [https://perma.cc/ULL3-NM26].

ii. San Francisco and Chicago versus Equifax

Last but not least, in the string of litigation that portrays cities as participants in nation-wide debates, are the data breach cases filed by the City Attorneys of San Francisco[155] and Chicago[156] against Equifax. The firm is among the three largest U.S. credit reporting agencies, and its business consists of amassing extensive personal records, which it sells to third-parties for a range of uses where an individual's creditworthiness determines his or her eligibility for various products and services (for example, consumer credit, insurance, cellphone service, student loans, home purchases, car leases, and so on).[157] Equifax collects and maintains data of 820 million customers worldwide.[158] In 2016 alone, the company reported annual revenue of more than $3.1 billion.[159]

In 2017, Equifax suffered a major data breach that compromised the personal information of more than 145 million Americans.[160] Both the FTC and the CFPB could have pursued civil penalties for the breach under the Fair Credit Reporting Act (FCRA) and could have immediately pursued civil penalties calculated by experts of up to $48,000 per violation.[161] However, the FTC instead chose to rely on the FTCA, even though the statute does not grant the Commission any immediate fining authority.[162] Almost two years later, Equifax

---

155. *See generally* Complaint, People v. Equifax, Inc., No. CGC 17-56129 (Cal. App. Dep't Super Ct.) (filed Sept. 26, 2017).

156. *See generally* City of Chicago v. Equifax, Inc., No. 1:18-cv-01470 (N.D. Ga. May 22, 2018).

157. *See* Stacy Cowley, *Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement*, N.Y. TIMES (July 22, 2019), https://www.nytimes.com/2019/07/22/business/equifax-settlement.html [https://perma.cc/49HC-7XM9].

158. *See* Tara Siegel Bernard et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html [https://perma.cc/5S39-QHTF].

159. *See* EQUIFAX, 2016 ANNUAL REPORT: THE POWER OF INSIGHTS 2 (2016), https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2016-annual-report.pdf [https://perma.cc/5DLA-GNGK].

160. Cowley, *supra* note 157.

161. 15 U.S.C. § 1681s (2012); Thomas M. Cull, *An Overview of Damages Recoverable Under the Fair Credit Reporting Act*, NAT'L L. REV. (Feb. 8, 2019), https://www.natlawreview.com/article/overview-damages-recoverable-under-fair-credit-reporting-act [https://perma.cc/U9EW-WJ28]; Interview with David Vladeck, Former Dir., Fed. Trade Comm'n, in Washington, D.C. (March 23, 2019).

162. *See* 15 U.S.C. § 4 (2012); *see also* Chris Jay Hoofnagle et al., *The FTC Can Rise to the Privacy Challenge, but not Without Help from Congress*, BROOKINGS INST. (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-c

agreed to a settlement that included a still hefty penalty of $575–700 million.[163]

In terms of injunctive relief, Equifax agreed to a set of extensive measures, including the establishment of a detailed security program over the course of 20 years and reports to the FTC of data incidents, as well as biennial security assessments by a third party.[164] The monetary and injunctive relief was granted based on three legal grounds raised by the FTC. First, the FTC asserted Equifax's failure to apply reasonable measures to secure data in the knowledge of security vulnerabilities.[165] Without showing concrete examples, the Commission pointed out that as a result, the breach led to "a substantial injury" to consumers.[166] Second, the company misrepresented its security and privacy policies, misleading consumers about its products. Finally, the company failed to meet its obligations under federal law requiring financial institutions to develop a comprehensive written information security program.[167]

Although the FTC began investigating the Equifax breach in the fall of 2017,[168] it did not reach a final settlement until the summer of 2019. Within a few months of the breach, however, the San Francisco City Attorney filed the first legal action for privacy breach in the country by a governmental actor.[169] This action raised several claims: first, that the company failed to implement reasonable security measures in violation of the California Customer Records Act

---

hallenge-but-not-without-help-from-congress/ [https://perma.cc/L23R-428Q] ("The FTC generally cannot issue a fine for Section 5 violations initially — fines can only be issued for violations of consent decrees[.]").

163. Press Release, Federal Trade Commission, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related [https://perma.cc/JYL4-XF23] (noting that the payment was divided between the offices of 48 AGs, the District of Columbia and Puerto Rico, the CFPB, and a fund that compensates consumers).

164. *Id.*

165. Complaint at 12–15, Fed. Trade Comm'n v. Equifax Inc., No. 1:190mi-99999-UNA (N.D. Ga. July 22, 2019).

166. *Id.* at 19.

167. *Id.* at 21.

168. Russell Brandom, *The FTC Is Looking into the Equifax Breach*, VERGE (Sept. 14, 2017), https://www.theverge.com/2017/9/14/16306872/equifax-breach-ftc-probe-lawsuit-vulnerability [https://perma.cc/MCH6-VQ7L].

169. Complaint, Herrara v. Equifax, No. CGC-17-561529 (Cal. Super. Ct. Sept. 26, 2017).

(CRA),[170] and that this failure compromised the data of approximately 44% of the U.S. population, including 15 million Californian residents; second, that Equifax exacerbated the risk of identity theft and fraud faced by Californian consumers by delaying notification of the breach until six weeks after the discovery of the breach, in violation of California's breach notification law, which requires expedient notification if personal information is unencrypted or reasonably believed to have been acquired by an unauthorized person.[171]

The City Attorney based San Francisco's standing on California's Business and Professional Code, which gives the city the right to enter a suit on behalf of local residents when a company is allegedly conducting "unlawful, unfair and fraudulent" business practices within the city.[172] The city met the "injury in fact" standard because California residents suffered financial harm from the Equifax breach even though the complaint did not cite any particular injured party.[173] The city sought civil penalties of $2500 for each violation, restitution to Californians who used Equifax's services, and injunctive relief.[174]

Chicago filed a suit against Equifax under the city's Consumer Fraud, Unfair Competition, or Deceptive Practices Ordinance.[175] The city asserted jurisdiction since the company was conducting unfair and deceptive practices while doing business in Chicago, and the conduct of Equifax resulted in compromising the personal information of 5.4 million residents of Illinois, including an uncounted number of people who resided in Chicago.[176] The Chicago Corporate Counsel raised four claims: First, that Equifax fell short of its public promises to make the protection of personal data its "top priority."[177] Second, it failed to implement security industry best practices (for example, encryption, deployment of available fixes, and patches in the knowledge of security vulnerabilities).[178] Third, it failed to provide timely and full notice of the breach to Chicago residents (in

170. *Id.* at 13.

171. *Id.* at 18. Delays are possible in case of criminal investigations, but Equifax's delay did not result from the request of a law enforcement agency in that context. CAL. CIV. CODE §§ 1798.82(a)–(b) (2020).

172. CAL. BUS. & PROF. CODE § 17200 (1993).

173. Complaint, *supra* note 169, at 19.

174. *Id.*

175. Complaint, Chicago v. Equifax, No. 2017-CH-13047 (Ill. Cir. Ct. Sept. 28, 2017).

176. *Id.* at 2–4.

177. *Id.* at 11.

178. *Id.* at 6–10.

violation of the Illinois Personal Information Privacy Act (PIPA)).[179] And fourth, that Equifax engaged in further unfair and deceptive practices after the breach.[180]

As in the San Francisco case and that of the federal agencies, Chicago claimed that the Equifax data breach caused potential harm to Chicago residents by exposing them to the risk of identity theft and financial fraud but did not give examples of particular victims and occasions of harm.[181] The Chicago complaint went slightly beyond the San Francisco and federal complaints because Chicago also raised claims of emotional harm to local residents based on lost time, fear, and anxiety.[182]

The participation of various cities in privacy enforcement actions seeking to protect the public interest reveals certain patterns. First, the cases that they chose to litigate are usually high-profile ones — both the Cambridge Analytica incident and the Equifax breach are prime examples of high-profile cases with significant nation-wide, and even global, impact. Second, the city attorneys (sometimes in concert with the state AGs) are usually the first governmental actor to start litigation, serving as an alarm bell for federal enforcement agencies. Unlike in other expertise-heavy data breach cases where the state AGs participate at the end stages of litigation, leaving the FTC to invest resources into an investigation and then sharing the settlement,[183] in the cases we discuss city law offices are first movers in litigating.

Although legally speaking, all cases fall within the same title — privacy consumer protection — thematically, they can be divided into two types. In the electoral context, the Cambridge Analytica suit, much like in the context of political representation and local autonomy, the Census 2020 litigation tries to preserve democratic

---

179. *See id.* at 12–13; *see also* Personal Information Protection Act, 815 ILL. COMP. STAT. 530/5 (2006). This PIPA violation was an "unlawful practice" that gave the Corporate Counsel authority to sue under the city ordinance. Complaint, *supra* note 169, at 12.

180. Although Chicago had the option of bringing some of the claims under the city ordinance alone, it chose not to do so since the local privacy ordinance would not have justified the notice requirement under PIPA. Telephone Interview, Office of the Chicago Attorney General (Apr. 19, 2019).

181. The Chicago City AG used emphatic language: "Chicago is not required to demonstrate harm to its residents to enforce the Ordinance." *See* Complaint, *supra* note 175, at 13.

182. *See id.* at 14–15.

183. Interview with David Vladeck, *supra* note 161.

values.[184] The Equifax cases, in turn, are aimed at improving consumer protection standards in data-intense sectors[185] and are based on a broad interpretation of harm that might have triggered or reaffirmed such an interpretation on the federal level.[186] Further, unlike in other areas of law where cities abruptly clash with states trying to preempt city ordinances along party lines,[187] data privacy

---

184. Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today — and How to Change the Game*, BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/2SJD-4TY2].

185. Los Angeles also filed a suit against Uber in another major data breach case with a national dimension, and so did Chicago, followed by Illinois. *See* David Cohen et al., *U.S. City Suits: The Next Frontier of Data Breach Actions*, N.Y.L.J. (Feb. 21, 2018), https://www.law.com/newyorklawjournal/2018/02/21/city-suits-the-next-frontier-of-data-breach-actions/ [https://perma.cc/H6R9-MC72] (discussing how in the state of Illinois settled, but the office of the Chicago AG decided to continue litigating in the Uber litigation). Data breach litigation on the city level has also emerged against more traditional industries that are becoming increasingly data-intense. *See generally* Complaint, Chicago v. Marriott, No. 2019-CH-00948 (N.D. Ill. Feb. 14, 2019).

186. Notwithstanding the Supreme Court's ruling in *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (2016), there is a substantial circuit split on the harm standard in U.S. Courts of Appeals. *See* Rahul Mukhi & Tanner Mathison, *Supreme Court Declines to Review Standing in the Data Breach Context Despite Ongoing Circuit Split*, CLEARY GOTTLIEB: CLEARY CYBERSECURITY & PRIVACY WATCH (Mar. 7, 2018), https://www.clearycyberwatch.com/2018/03/supreme-court-declines-review-standing-data-breach-context-despite-ongoing-circuit-split/ [https://perma.cc/V6F7-WKEH] ("[T]he D.C., Third, Sixth, Seventh, Ninth, and Eleventh Circuits hold[] that data theft, with the attendant risk of future identify theft fraud, is by itself sufficient for Article III standing, and the Second, Fourth, and Eighth Circuits hold[], in contrast, that such allegations are not sufficient on their own to satisfy Article III's injury requirements." (internal citations omitted)). A number of courts have held that data breach alone is sufficient for establishing standing by satisfying "the injury in fact" threshold under Article III of the U.S. Constitution, while others have focused on the actual misuse of the data as a threshold requirement. *See generally Spokeo, Inc.*, 136 S. Ct. 1540; Luke Martin, *Resolving the Circuit Split on Article III Standing for Data Breach Suits*, COLUM. BUS. L. REV. (Aug. 13, 2019), https://journals.library.columbia.edu/index.php/CBLR/announcement/view/181 [https://perma.cc/C6TY-K8Z2] (citing Mukhi & Mathison, *supra* note 186). The FTC has never adopted a firm stance on the matter. Jonathan S. Kolodner et al., *Latest FTC Data Privacy Settlement May Signal More Direct Approach to Regulating Data Security*, CLEARY GOTTLIEB: CLEARY CYBERSECURITY & PRIVACY WATCH (Nov. 20, 2019), https://www.clearycyberwatch.com/2019/11/latest-ftc-data-privacy-settlement-may-signal-more-direct-approach-to-regulating-data-security/ [https://perma.cc/SEQ6-HQJD]. Since harm can prove intractable in privacy claims, the broader interpretation of that threshold espoused by state and city AGs under state and municipal legislation might help inform both the federal bench and the FTC in asserting a firm standard.

187. *See* Briffault, *supra* note 27, at 1997–98; Davidson, *supra* note 36, at 959–60. Sarah Swan explains there is generally limited state pushback against local litigation in terms of the prevalence of issues that are not polarizing and attract condemnation

litigation shows a harmonious city-state relationship of well-resourced, big cities working shoulder-to-shoulder with their states. That dynamic might be exemplary of what Schragger dubs as "our federalism's anti-urbanism" or the tendency of U.S.-state based federalism to disfavor decentralization to sub-state governments, and to exert any real-life influence, often cities need to be in synchrony with their states.[188] In this sense, large, cosmopolitan cities' privacy activism in the United States is emerging within progressive states, and opposition seems more likely to come from a conservative federal administration.[189] At least when it comes to enforcement, there seems to be no horizontal city coordination because, unlike with state attorneys general, [190] city attorneys general do not share a venue for collective action.

Certainly, city litigation with data privacy implications fits neatly into the wider partisan dynamics where local actors serve as checks on federal power through the institutional venue of federalism.[191] As the office of the City Attorney of Chicago remarked:

> It would be correct to say . . . that a number of our present initiatives (including but not limited to in the data privacy arena) are driven by a concern that at present the federal government is not taking sufficient action to protect the health, safety, and interests of Chicago residents.[192]

---

across party lines. *See generally* Sarah L. Swan, *Preempting Plaintiff Cities*, 45 FORDHAM URB. L.J. 1241 (2018). Although some litigation efforts like the recent cases about removing Confederate monuments can also be inflammatory, the examples we bring of local privacy litigation against private companies fit Swan's findings. *Id.* at 1284.

188. Richard C. Schragger, *The Attach on American Cities*, 96 TEX. L. REV. 1163, 1184 (2018). In 2018, Chicago introduced its own, far-reaching consumer privacy ordinance that has, however, since stalled. *See generally* Chi. City Council O2018-3240, 2018 Sess. (Chi. 2019) (amendment failed to pass).

189. *See, e.g.*, Cristiano Lima & John Hendel, *California Democrats to Congress: Don't Bulldoze Our Privacy Law*, POLITICO (Feb. 21, 2019, 5:07 AM), https://www.politico.com/story/2019/02/21/congress-data-privacy-california-1185943 [https://perma.cc/45R6-HJ8B] (describing state efforts to fend off federal preemption of the CCPA); Nilay Patel, *Facebook's $5 Billion FTC Fine Is an Embarrassing Joke*, VERGE (July 12, 2019), https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke [https://perma.cc/REG4-7XK3] (criticizing lenient federal enforcement of privacy regulations).

190. *See generally About NAAG*, NAT. ASS'N ATT'YS GEN., https://www.naag.org/naag/about_naag.php [https://perma.cc/3B7T-AV4X] (last visited Feb. 21, 2020).

191. *See* Gerken, *supra* note 82, at 1959; *see also* Jessica Bulman-Pozen, *Partisan Federalism*, 127 HARV. L. REV. 1077, 1096 (2014).

192. Interview with David Vladeck, *supra* note 161.

However, attitudes toward Silicon Valley and concomitant privacy issues vary both across and within party lines, demonstrating the nuances of partisan federalism in this field.[193] Further, unlike with state and city attorneys general, FTC's settlements do not go to the Commission's coffers, but directly to the Federal Treasury. Coupled with the revenue-raising restraints cities face as outlined above, this is possibly creating a depoliticized, purely financial incentive for prosecutors on both the state and the city level to bring actions. Chicago is not dropping its charges at the moment of writing in the wake of the FTC settlement with Equifax,[194] while San Francisco has yet to announce its decision on the matter.[195] The trend shows the crossing of public interest litigation with profit-seeking on the side of city actors.

III. THE CITY AS DATA STEWARD

At every level of government — federal, state, and local — government agencies amass personal data and must manage their data assets in the public interest. Cities collect and utilize an extensive range of personal and sensitive data and do so with relatively few encumbrances from superior levels of government. When they act explicitly as data stewards, cities not only carry out day-to-day management tasks but also take on "fiduciary-like responsibilities to consider the ethical and privacy impacts of particular data activities and to act with the best interests of individuals and society in mind."[196] According to Kelsey Finch and

---

193. For example, a draft federal bill introduced by Democratic Senator Markey may prevent state and city prosecutors from brining legal actions once the FTC has entered a consent order:

> If the Commission institutes an action with respect to a violation of this Act or a regulation promulgated under this Act, a State may not, during the pendency of that action, institute an action under subsection (a) against any defendant named in the complaint in the action instituted by the Commission based on the same set of facts giving rise to the violation with respect to which the Commission instituted the action.

Privacy Bill of Rights Act, S. 1214, 116th Cong. § 16(e) (2019).

194. E-mail from Office of the Chi. Attorney Gen. (July 22, 2019) (on file with author).

195. Dominic Fracassa, *Equifax Agrees to Pay $600 Million for 2017 Data Breach*, S.F. CHRON. (July 22, 2019), https://www.sfchronicle.com/bayarea/article/Equifax-agrees-to-pay-600-million-for-2017-data-14112539.php [https://perma.cc/445P-J8GB].

196. Kelsey Finch & Omer Tene, *Smart Cities: Privacy, Transparency and Community*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 126–27 (Evan Selinger et al. eds., 2018).

Omer Tene, data stewardship consists of a familiar set of data governance and accountability mechanisms.[197] Its five components include first, "privacy management programs establishing principles and practices that apply to collecting, viewing, storing, sharing, aggregating, analyzing, and using personal data."[198] Second, an oversight mechanism for such programs, which minimally requires appointing a designated privacy lead.[199] Third, privacy risk management, which may entail conducting Privacy Impact Assessments as well as a benefit-risk analysis for big data projects that promise tremendous benefits but that also "introduce new privacy and civil liberties concerns associated with large-scale data collection and analysis."[200] Fourth, vendor management — because so many smart city developments depend on public-private partnerships.[201] Fifth, an ethical review processes akin to the rules for conducting human subject research whenever cities allow public or private researchers access to big data.[202] This is especially true if the research involves secondary purposes (i.e., "appropriating civic data that was originally collected for another purpose without citizens' knowledge or consent").[203]

Cities do not always achieve this ideal of data stewardship. As the case studies below demonstrate, cities must fully embrace their role as data stewards when they process data incidental to delivering city services and share it among city agencies under the terms of interagency data sharing agreements or local privacy regulations. They face greater challenges in protecting data and serving the public interest when they interact with powerful commercial actors motivated by private interests. Nor are the privacy measures cities adopt in commercial interactions uniform across all cases. Privacy measures adopted range from arms-length agreements in which cities bargain away privacy rights in exchange for private firms offering discounted or "free" services such as broadband;[204] to ill-conceived regulations forcing sharing economy firms to hand over customer data (which have sparked lawsuits by regulated firms positioning

197. *Id.* at 127.
198. *Id.* at 128.
199. *See id.* at 130.
200. *Id.* at 130–31.
201. *See id.* at 182–84 (describing vendor management in terms of clearly delineating responsibilities of cities and vendors for privacy management, public communication, and supervision of other contractors and subcontractors).
202. *See id.* at 133–34.
203. *See id.* at 133.
204. *See infra* note 239.

themselves as protecting their customers' privacy interests against the city government);[205] to more collaborative forms of data sharing in which cities and technology platforms experiment with open data or data trusts;[206] and, finally, to more complex and protracted engagements such as the Toronto Quayside project, where government, the private sector, and local citizenry are contesting the very soul of the smart city.[207]

A. Managing City Data

A recent trend in urban governance is the delivery of more efficient and effective services via data integration and analysis, a trend that extends to traditional social services.[208] Many families receive services and benefits from multiple public and private programs. Yet, all too often, caseworkers working with the same families are not even aware of one another in part because they maintain their data in siloed databases. Data integration and analysis not only allows caseworkers to coordinate services for clients but also to do a better job of matching individual clients with existing services and improve policy decisions and program development more generally.[209] Integrated social service programs entirely depend on the collection, sharing, and repurposing of highly personal data.[210] They, therefore, require very tight controls over data access, use, disclosure, and retention to avoid gross privacy violations. Proponents of data-driven solutions have viewed privacy rules as a nuisance akin to bureaucracy[211] or acknowledged that local government has responsibility for privacy and security protections but

---

205. *See* Rick Schmitt, *The Sharing Economy: Can the Law Keep Pace with Innovation?*, STAN. LAW. (May 31, 2017), https://law.stanford.edu/stanford-lawyer/articles/the-sharing-economy-can-the-law-keep-pace-with-innovation/ [https://perma.cc/WJC5-4QJK].

206. *See* Jane Croft, *Data Trusts Raise Questions on Privacy and Governance*, FIN. TIMES (Sept. 12, 2019), https://www.ft.com/content/a683b8e4-a3ef-11e9-a282-2df48f366f7d [https://perma.cc/V6Q6-MUTG].

207. Leyland Cecco, *'Surveillance Capitalism': Critic Urges Toronto to Abandon Smart City Project*, GUARDIAN (June 6, 2019), https://www.theguardian.com/cities/2019/jun/06/toronto-smart-city-google-project-privacy-concerns [https://perma.cc/TDX2-L893].

208. *See generally* GOLDSMITH & KLEIMAN, *supra* note 14.

209. *See id.* at 109–49.

210. *See id.*

211. *See, e.g.*, Robert Goerge, *Data for the Public Good: Challenges and Barriers in the Context of Cities*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 153 (Julia Lane et al. eds., 2014).

without otherwise giving the topic any further attention.[212] More recently, innovative cities have taken up the privacy challenge by developing standardized data-sharing agreements with strong privacy provisions. New York City is a good example.[213]

In 2008, the Mayor's Office issued Executive Order 114, launching an initiative to facilitate data integration and exchange among multiple Health and Human Services (HHS) agencies; privacy concerns barely registered beyond requiring that data sharing comply "with all applicable Federal, State and local laws and regulations."[214] However, participating agencies had to sign an agreement providing for the protection and confidentiality of all data exchanged or accessed by "HHS-Connect" systems.[215] The agreement imposed various obligations under the Fair Information Practice Principles (FIPPs), which are the basis for modern privacy regulation.[216] Applicable principles included purpose limitations, access rights as determined by the source agency, use restrictions, access controls, and data security, training of personnel, and adherence to citywide IT policies (mainly security and responsible use).[217] Over the next decade, New York City continued to extoll data sharing while demonstrating limited concern for privacy. For example, the city enacted an Open Data Law, mandating that by the end of 2018, the city make freely available, on a single web portal, all "public" data sets.[218] It also created the Mayor's Office of Data Analytics (MODA), with responsibilities for collaborative, data-driven solutions, a citywide data platform, oversight for data projects, and

---

212. *See generally* GOLDSMITH & KLEIMAN, *supra* note 14.

213. *Data Sharing Cooperative*, NEW YORK STATE GIS, https://gis.ny.gov/co-op/ [https://perma.cc/432N-SWHZ] (last visited Mar. 28, 2020).

214. *See* N.Y. City Mayor Exec. Order No. 114 (Mar. 18, 2008), http://www.nyc.gov/html/om/pdf/eo/eo_114.pdf [https://perma.cc/4GVL-TF4W].

215. *See generally* Inter-Agency Data Exchange Agreement, Agencies of the City of N.Y. (Nov. 2010), https://www1.nyc.gov/assets/finance/downloads/pdf/mou/interagency_data_exchange_hhs.pdf [https://perma.cc/CE3E-URPV].

216. There are different formulations of FIPPs, which vary as to both the number of principles and their substantive content, but they generally address collection and use limitations, purpose specification, data quality, security, transparency, access and correction, and accountability. *See, e.g.*, ORGANISATION FOR ECON. CO-OPERATION & DEV. (OECD), REVISED OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2013).

217. *See* ALON YARONI ET AL., VERA INST. OF JUSTICE, WORKER CONNECT: A PROCESS EVALUATION OF A NEW YORK CITY DATA INTEGRATION SYSTEM (2015), https://www1.nyc.gov/assets/opportunity/pdf/workerbriefs7c.pdf [https://perma.cc/2M2L-9LG5].

218. *See* N.Y.C. ADMIN. CODE §§ 23-501–09 (McKinney 2012).

implementation of the Open Data Law. New York City's inattention to privacy concerns finally changed in November 2017, when the City enacted its first comprehensive privacy laws in the form of two laws designed to protect personal information collected by city employees and contractors in the course of providing local services and benefits.[219]

New York City has done an excellent job of addressing the privacy issues associated with data integration and analysis, evolving from data-sharing agreements to a local ordinance requiring comprehensive citywide privacy policies and protocols. In its zeal to improve city life by processing and analyzing massive amounts of data, however, the city has been less successful in identifying and correcting issues related to algorithmic fairness, accountability, and transparency. Over the past five years, both privacy scholars and far-sighted regulators have recognized, in the words of John Podesta, former advisor to President Obama, that "big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace."[220] For example, the use of predictive algorithms to maximize interest in online job postings can lead to ads being "delivered in a way that reinforces gender and racial stereotypes, even when employers have no such intent."[221] Algorithms recognize and, in some cases, reproduce existing patterns in employment, even when those patterns are the result of past discrimination.[222] Thus, while big data analytics can help identify patterns of bias and illegal exclusion, it can also hide continued bias

---

219. Local Law 245 requires every city agency to report on their data collection, retention, and disclosure policies and current practices. *See* N.Y.C., Local Law 245, Interim B. No. 1557-A (Dec. 17, 2017) (codified at N.Y.C. ADMIN. CODE §§ 23-1203–05 (McKinney 2017)). Local Law 247 requires city employees and contractors to protect all "identifying information" by limiting its collection, disclosure, and retention, except where required by law. Requests for the collection or disclosure of identifying information would be processed by a newly established privacy officer within each agency who would analyze whether the collection or disclosure would further the purpose or mission of the agency. N.Y.C., Local Law 247, Interim B. No. 1588-A (Dec. 17, 2017) (codified at N.Y.C. ADMIN. CODE §§ 23-1201–02 (McKinney 2017)). For a more detailed discussion of both laws, see Rubinstein, *supra* note 3, at 2010–13.

220. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES iii (2014).

221. *See, e.g.*, Miranda Bogen, *All the Ways Hiring Algorithms Can Introduce Bias*, HARV. BUS. REV. (May 6, 2019), https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias [https://perma.cc/U6RK-N5K8].

222. *Id.*

behind a veil of impartial mathematics.[223] This problem can be equally pernicious whether the algorithm in question was designed and implemented by the public or the private sector.[224]

In some ways, the city's neglect of these issues is not surprising. There is a long history of surveillance and policing of welfare applicants in the United States that predates data analytics.[225] More recently, scholars have identified "algorithmic discrimination" as an emergent topic in privacy scholarship and have called attention to both the due process deficits of data analytics and its harmful impact on people of color and other historically marginalized communities.[226] Although the city has taken a preliminary step toward addressing these concerns by appointing a cross-disciplinary group of experts to an Automated Decision Systems Task Force, with the goal of developing a process for reviewing the algorithms the city uses through the lens of equity, fairness, and accountability,[227] the task force is behind in its goal of issuing a report of policy

---

223. AARON RIEKE ET AL., UPTURN, CIVIL RIGHTS, BIG DATA, AND OUR ALGORITHMIC FUTURE 3, 12–14 (2014), https://bigdata.fairness.io/wp-content/uploads/2015/04/2015-04-20-Civil-Rights-Big-Data-and-Our-Algorithmic-Future-v1.2.pdf [https://perma.cc/CA23-9JW7].

224. *Id.*

225. *See generally* JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY (2001).

226. *See, e.g.*, LEADERSHIP CONFERENCE ON CIVIL & HUMAN RIGHTS, CIVIL RIGHTS PRINCIPLES FOR THE ERA OF BIG DATA (2014), https://civilrights.org/2014/02/27/civil-rights-principles-era-big-data/ [https://perma.cc/CTP5-WNV5]; Danielle Keats Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 18 (2014); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 99 (2014); Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 633 (2017); Andrew Selbst & Solon Barocas, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 671 (2016). More specifically, the same analytic tools driving digital innovation in city (and state) welfare programs may be invasive and punitive when examined from the perspective of their intended beneficiaries — such as the poor and the homeless. *See* VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 178–200 (2017). Eubanks evaluated an automated eligibility program for health care, food stamps and cash benefits in Indiana, an algorithm for evaluating comparative vulnerability of homeless people vying for limited housing placements in Los Angeles, and the use of a statistical model to predict child abuse in Pittsburgh and found a host of problems. These ranged from programming errors and inadequate (i.e., biased) data, to inflexibility and lack of accountability on the part of program administrators, to an utter lack of choice on the part of affected individuals whose data form a part of these systems.

227. *See* N.Y.C. AUTOMATED DECISION SYSTEMS TASK FORCE, AUTOMATED DECISION SYSTEMS TASK FORCE REPORT 2 (2019), https://www1.nyc.gov/assets/adstaskforce/downloads/pdf/ADS-Report-11192019.pdf [https://perma.cc/ZNS8-EMMC].

recommendations by Fall 2019.[228] More generally, responding to algorithmic discrimination remains one of the great unfinished tasks of city data governance.

B. Commercial Data Sharing Agreements

The preceding Sections suggest that in developing data-driven policies to improve the quality of urban life, cities have all the political power they need to govern the relevant data. In fact, the social service programs that cities hope to improve are mostly funded by federal and state programs that carry their own complex requirements and burdens. Apart from any constraints accompanying such programs, however, cities operate with a very free hand in governing local data.[229] Neither are the city's regulatory powers preempted by federal or state law, given that the federal Privacy Act applies exclusively to personal data held by federal agencies. Most states lack comparable laws regarding state agencies, and the minority states with such laws limit their scope exclusively to state, as opposed to local agencies.[230] When cities enter into commercial agreements with private firms, however, they must contend with the privacy practices and norms of some very large and powerful actors. Moreover, these market forces may exert greater sway over cities than any statutory rules from higher levels of government. This next Section examines commercial interactions with three sectors of great importance to twenty-first-century cities: broadband, the sharing economy, and smart city technology firms, including those engaged in high-profile projects such as Toronto Quayside.

Broadband, in the form of readily available and inexpensive fiber connections and advanced wireless capability, is increasingly important to economic growth, education, and healthcare.[231] Many cities have recognized that cheap, unlimited communication capacity is essential to the future prospects of their citizens and their community, while at the same time recognizing that a vast digital

---

228. *See* Diana Budds, *New York City's AI Task Force Stalls*, CURBED (Apr. 16, 2019), https://ny.curbed.com/2019/4/16/18335495/new-york-city-automated-decision-system-task-force-ai [https://perma.cc/49D9-FKGL].

229. *See* Rubinstein, *supra* note 3, at 2046–47.

230. *Id.* at 1981 (noting that "New York's Personal Privacy Protection Act requires that each state agency 'that maintains systems of records' must comply with the FIPs. But this law does not apply to local governments" (citations omitted)).

231. *See* SUSAN CRAWFORD, FIBER: THE COMING TECH REVOLUTION — AND WHY AMERICA MIGHT MISS IT 13–17 (2018).

divide separates rich and poor residents.[232] Cities have therefore made it an explicit policy objective to narrow this digital divide by investing in innovative ways to provide high-speed internet access to homes, businesses, and the public, or even rolling out free, public wireless services. Some of these initiatives have proven ill-advised from a privacy perspective and illustrate the same neglect of privacy issues by cities as in the early days of data-driven city services.

Unlike the rollout of broadband, where cities try to attract private investment, the sharing economy needs the city as much as the city needs the sharing economy. Data-intense businesses in the sharing economy differ from platforms like Facebook or data brokers like Equifax because they offer "what might . . . be called 'real-world' goods and services," such as transportation and housing.[233] Urban density provides a critical mass of providers and consumers "sufficiently close to each other or to other amenities to make [sharing companies] work."[234] Beyond filling in shortages in housing and transportation by freeing up surplus goods, the sharing economy provides another crucial asset for the city: data. The troves of aggregate data amassed by sharing enterprises can improve local government by guiding urban planners toward the optimization of housing or reducing traffic congestion.[235] But the relevant data sharing agreements may — or may not — fully account for privacy costs to local residents. Cities have adopted vastly different approaches to data sharing arrangements with sharing economy firms ranging from intrusive regulations to experiments with data collaboratives.

"Smart city" is a buzzword with no fixed meaning.[236] At the very least, it describes cities permeated by "software-enabled infrastructures and networked digital devices and sensors that are used to augment urban management and governance."[237] At the same time, smart cities are cities where technology-driven innovation

---

232. *Id.* at 135–57. The digital divide also separates urban from rural Americans, but that topic is beyond the scope of this Article.

233. Nestor Davidson, *The Sharing Economy as an Urban Phenomenon*, 34 YALE L. & POL'Y REV. 215, 218 n.10 (2016).

234. *Id.* at 218.

235. *See generally* GOLDSMITH & CRAWFORD, *supra* note 14.

236. *See* Rob Kitchin et al., *Smart Cities and the Politics of Urban Data*, *in* SMART URBANISM: UTOPIAN VISION OR FALSE DAWN? 17 (Simon Marvin et al. eds., 2015). *See generally* ADAM GREENFIELD, AGAINST THE SMART CITY (2013); ANTHONY M. TOWNSEND, SMART CITIES: BIG DATA, CIVIC HACKERS, AND THE QUEST FOR A NEW UTOPIA (2013).

237. Kitchin et al., *supra* note 236, at 17.

and entrepreneurship both attract jobs and investments, and make government work better.[238] Some of the world's largest technology companies operate smart city initiatives combining networking infrastructure, IoT devices, and data-driven analysis. One of these firms, Sidewalk Labs — a division of Alphabet, and sister company of Google, which has an ambitious smart city project underway in Toronto, Ontario — perfectly illustrates the problems that arise when cities allow the private sector to set the agenda for governing the smart city.

i. Bargaining Away Privacy Rights

Both major cities and small towns across the country have begun experimenting with public-private partnerships as a way to offer free or low-cost Wi-Fi in public facilities (such as parks, stadiums, or low-income housing), and much faster but more conventionally priced internet access deals to the city's remaining population. Often, private firms receive certain benefits or regulatory concessions from local governments in return. For example, Google inked deals with the mayors of Kansas City, Kansas, and Kansas City, Missouri, to install "Google Fiber" in some government buildings in exchange for using city offices, equipment, and electricity free of charge. Moreover, Google negotiated its way around the "universal service" obligations that typically require big telecommunications companies to at least offer their services to an entire city or town.[239] Although Google Fiber originally had a free option, Google eventually canceled and replaced it with a $50 option that offers internet at slower speeds. Google Fiber also partnered with the Housing Authority of the City of Austin to offer free Wi-Fi at select affordable housing providers.[240]

New York City has launched multiple broadband initiatives ranging from promoting competition in the residential and commercial broadband markets, to investing in networks for the provision of free or low-cost high-speed residential access for low-income communities,[241] to a citywide implementation of digital

---

238. *Id. See generally* GOLDSMITH & CRAWFORD, *supra* note 14; GOLDSMITH & KLEIMAN, *supra* note 14.

239. *See* Erica Swanson, *Bringing Internet Access to Public Housing Resident*, OFFICIAL GOOGLE FIBER BLOG (July 15, 2015), https://fiber.google.com/blog/2015/bringing-internet-access-to-public-housing-residents/ [https://perma.cc/XD2Q-HZRU].

240. *Id.*

241. For example, the local housing authority partnered with Spot on Networks (SON) to provide free high-speed Wi-Fi to the residents of the country's largest

kiosks called "LinkNYC" (which offer high-speed Internet access and a range of other popular services including Wi-Fi phone calls, device charging, and a tablet for access to city services, maps, and directions).[242] In the latter deal, a company called CityBridge agreed to lay cable, install infrastructure, and operate the LinkNYC network "for free" in exchange for splitting advertising revenues with the city, valued at $1 billion over the life of the 12-year franchise agreement.[243] One of the major investors in LinkNYC is Sidewalk Labs.[244]

In *Fiber*, Susan Crawford describes how companies with monopoly power over broadband and Internet access (mainly Comcast and Verizon) use their tremendous lobbying resources to thwart broadband competition despite the obvious need for massive investments in fiber infrastructure (the so-called "last mile" problem).[245] Crawford also highlights a few smaller cities and towns that have invested in community-based broadband to build low-cost, high-speed networks at the local level. Although project financing is always a bit precarious for these communities, they have relied successfully on bonds, federal and state matching grants, and anticipated budgetary savings to build city-owned community fiber networks. These networks are designed to reach all local residents, thereby closing the digital divide and ensuring that the local community is well-positioned to enjoy future economic growth and related innovations in education, health, and local governance.[246]

---

public housing complex, Queensbridge Houses. *See About Queensbridge Connected*, NYC, https://www1.nyc.gov/site/queensbridge/about/about.page [https://perma.cc/V2MS-SLFW] (last visited Mar. 5, 2020).

242. LINKNYC, https://www.link.nyc/ [https://perma.cc/HM3X-X253] (last visited Aug. 20, 2019). The touchscreen tablet originally allowed Internet browsing, which led some people to use the kiosks to blast music and watch porn, forcing the removal of the browsing capability. *See* Joshua Brustein, *Building a Smart City? Have You Thought About Porn and Privacy?*, BLOOMBERG (Sept. 14, 2016), https://www.bloomberg.com/news/articles/2016-09-15/building-a-smart-city-have-you-thought-about-porn-and-privacy [https://perma.cc/ULU4-XFX7].

243. *See* Maren Maier et al., *LinkNYC*, *in* SMARTER NEW YORK CITY, HOW CITY AGENCIES INNOVATE 79–106 (André Corrêa d'Almeida ed., 2018).

244. *See* Elizabeth Woyke, *The Startup Behind NYC's Plan to Replace Phone Booths with 7,500 Connected Kiosks*, MIT TECH. REV. (July 18, 2017), https://www.technologyreview.com/s/608281/the-startup-behind-nycs-plan-to-replace-phone-booths-with-7500-connected-kiosks/ [https://perma.cc/QM77-7A4R].

245. CRAWFORD, *supra* note 231, at 37–66.

246. *Id.* at 67–96 (describing projects in Chattanooga, Tennessee; Wilson and Greensboro, North Carolina; Winthrop, Minnesota; and Otis, Massachusetts). *See generally* Olivier Sylvain, *Broadband Localism*, 73 OHIO ST. L.J. 796 (2012) (articulating a legal and public policy strategy for bolstering local authority to enter the broadband market as service providers).

There are notable differences between the privacy policies of these smaller, locally operated broadband providers and those of the larger firms seeking huge advertising revenues. For example, a glance at the relevant privacy policies of the towns Crawford highlights shows that their policies regarding the collection and use of data are reasonably protective of local users' privacy interests.[247] And a cursory review of the Spot on Networks (SON) privacy policy at the Queensbridge public housing project shows that not all locally operated broadband relies on targeted ads or sale of personal data to third parties to generate revenue.[248] Rather, it appears that local, and to some extent, federal tax revenues pay for the service.[249] Other large cities, including Boston[250] and Kansas City,[251] have similar programs that benefit low-income housing residents and do not sacrifice their privacy interests.

In sharp contrast, the ad-funded LinkNYC network raises several serious privacy concerns. The first is that by allowing LinkNYC to collect data from city residents and visitors for advertising purposes, the city government has relinquished its data stewardship role by trading away New Yorkers' privacy for LinkNYC's "free" services. According to privacy advocates, the original CityBridge privacy

---

247. *See, e.g.*, *Privacy Notice*, EPB FIBER OPTICS, https://epb.com/storage/app/media/uploaded-files/Privacy%20Notice.pdf [https://perma.cc/VWQ2-KWSH] (last visited Mar. 5, 2020); *Privacy Policy*, GREENLIGHT COMMUNITY BROADBAND, http://www.greenlightnc.com/privacy/ [https://perma.cc/RQ39-9ZXL] (last visited Mar. 5, 2020); *Privacy Policy*, RS FIBER, https://www.rsfiber.coop/privacy-policy/ [https://perma.cc/8P7H-R2QL] (last visited Mar. 5, 2020).

248. *See Privacy Policy*, SPOTON NETWORKS, https://www.spotonnetworks.com/legal/ [https://perma.cc/F8UB-2G8K] (last visited Mar. 5, 2020).

249. Gideon Lewis-Kraus, *Inside the Battle to Bring Broadband to New York's Public Housing*, WIRED (Nov. 3, 2016), https://www.wired.com/2016/11/bringing-internet-to-new-york-public-housing/ [https://perma.cc/M4ML-FMHL].

250. *City of Boston Wireless Wicked Free Wi-Fi Privacy Policy*, CITY OF BOS., https://www.boston.gov/departments/innovation-and-technology/city-boston-wireless-wicked-free-wi-fi-privacy-policy [https://perma.cc/HMN7-79TS] (last visited Mar. 5, 2020).

251. *See Free Network Foundation: Connected and Resilient*, KAN. CITY DIGITAL DRIVE, https://www.kcdigitaldrive.org/project/free-network-foundation/ [https://perma.cc/6QT7-8XGE] (last visited Apr. 3, 2020). Free Network Foundation worked with a local nonprofit organization to establish free networks serving more than 600 residences in two low-income housing developments in Kansas City. *Id.* This was in direct competition with the Google Fiber project. *See* Whitney Terrell, *Network Free K.C.*, HARPER'S (Mar. 20, 2013), https://harpers.org/blog/2013/03/network-free-k-c/ [https://perma.cc/562U-PJ7V].

policy governing the use of LinkNYC kiosks "allowed nearly limitless retention of user data, including browsing history."[252] Although CityBridge modified its privacy policy in response to these and other objections,[253] the updated policy still allows the system to track and retain "information such as IP addresses, anonymized MAC addresses, device type, device identifiers, and more, for up to 60 days" without users' consent.[254] A LinkNYC FAQ offers users various reassurances on these points,[255] but critics remain skeptical, noting that it is relatively easy to re-identify anonymized and aggregated information, that LinkNYC kiosks are equipped with Bluetooth beacons that have not been activated yet but may someday be used to push location-based mobile ads to passersby devices (even if they have not registered as Link users), and that Google has a prior history of Wi-Fi sniffing (the Google Street View case)[256] and of circumventing the anti-tracking protections built into Apple iPhones (the Safari case).[257]

The second concern is that the LinkNYC deal increases the risk of security breaches and unwanted surveillance of users and passersby. LinkNYC requires users to register with an email address and agree to allow CityBridge to gain access to their web traffic.[258] The kiosks

---

252. *See* Shahid Buttar & Amul Kalia, *LinkNYC Improves Privacy Policy, Yet Problems Remain*, EFF BLOG (Oct. 4, 2017), https://www.eff.org/deeplinks/2017/09/linknyc-improves-privacy-policy-yet-problems-remain [https://perma.cc/7WRZ-RHJ5].

253. *Id.*

254. *Id.*; *see also CityBridge Privacy Policy*, LINKNYC (Mar. 17, 2017), https://www.link.nyc/privacy-policy.html#info [https://perma.cc/5R54-6NH6] (classifying such data as "Technical Information" as opposed to personally identifiable information).

255. *See Frequently Asked Questions*, LINKNYC, https://www.link.nyc/faq.html#data-collection [https://perma.cc/QR4V-DT9Q] (last visited Mar. 28, 2020).

256. *See* David Streitfeld, *Data Harvesting at Google Not a Rogue Act, Report Finds*, N.Y. TIMES (Apr. 28, 2012), https://www.nytimes.com/2012/04/29/technology/google-engineer-told-others-of-data-collection-fcc-report-reveals.html [https://perma.cc/J3BV-U2QR].

257. Nick Pinto, *Google Is Transforming NYC's Payphones into a 'Personalized Propaganda Engine'*, VILLAGE VOICE (July 6, 2016), https://www.villagevoice.com/2016/07/06/google-is-transforming-nycs-payphones-into-a-personalized-propaganda-engine/ [https://perma.cc/N9FP-FRLJ].

258. *City's Public Wi-Fi Raises Privacy Concerns*, N.Y. C.L. UNION (Mar. 16, 2016), http://www.nyclu.org/news/citys-public-wi-fi-raises-privacy-concerns [https://perma.cc/CJ5G-YND3] (noting that Link NYC users "must submit their e-mail addresses and agree to allow CityBridge to collect information about what websites they visit on their devices, where and how long they linger on certain information on a webpage, and what links they click on").

also contain video cameras that capture a 360-degree view of the surrounding streets and sidewalks.[259] The New York Civil Liberties Union (NYCLU) has argued that the sheer volume of information these devices gather "will create a massive database of information that will present attractive opportunities for hackers and for law enforcement surveillance, and will carry an undue risk of abuse, misuse and unauthorized access."[260]

A third concern (to which we return below)[261] is that LinkNYC is but the first stage in Alphabet/Sidewalk Lab's plans to extend the monetization of personal data from the online world to the physical landscape. Indeed, during a 2016 talk about reimagining cities, Dan Doctoroff, the founder and CEO of Sidewalk Labs and former deputy mayor under Michael Bloomberg, stated as much:

> By having access to the browsing activity of people who are using the Wi-Fi — all anonymized and aggregated — we can actually then target ads to people in proximity and then obviously over time track them through lots of different things, like beacons and location services, as well as their browsing activity. So in effect what we're doing is replicating the digital experience in physical space.[262]

The root cause of the privacy threats associated with LinkNYC is that New York City issued a design challenge without privacy requirements or much regard for preserving existing urban privacy on the streets of New York at all. Arguably, the city could have leveraged the worth of its extremely valuable sidewalk real estate by driving a hard bargain that both delivered a public Wi-Fi system with minimal impact on the city budget and protected New Yorkers' privacy rights from the get-go. Instead, the city traded its citizens' rights to a for-profit company deeply immersed in the surveillance economy.[263] Ironically, it is not even clear that LinkNYC helped the

---

259. Kofman, *supra* note 5. Kofman also notes that "according to documents obtained by ReCode, Sidewalk Labs is selling kiosks to other cities that will be able to 'monitor pedestrian, bike and car traffic, track passing wireless devices, listen to street noise and use the kiosks' built-in video cameras to identify abandoned packages.'" *Id.*

260. *City's Public Wi-Fi Raises Privacy Concerns*, *supra* note 258.

261. *See infra* Section III.B.iv.

262. *Google City: How the Tech Juggernaut Is Reimagining Cities*, INFO. (Apr. 5, 2016), https://vimeo.com/161980906 [https://perma.cc/3R69-UR36]. We discuss this new form of data extraction from the physical world in greater detail below in the context of Sidewalk Lab's Quayside project in Toronto. *See infra* Section III.B.iv.

263. Aaron Shapiro calls this a Faustian bargain — between free Wi-Fi and the privatization of urban data for profit. *See* Aaron Shapiro, Design, Control, Predict: Cultural Politics in the Actually Existing Smart City (2018) (unpublished Ph.D.

city achieve its goal of reducing the digital divide. As it happens, Sidewalk Labs located the LinkNYC kiosks mainly in high traffic touristy areas of Manhattan (which generate the highest advertising revenues) rather than in poorer residential neighborhoods in the outer boroughs.[264] Of course, at the end of the day, LinkNYC and its boosters can always fall back on the argument that those who object to the kiosks are welcome not to use them. But this is a false dichotomy based on an illusory choice. What it really amounts to is forcing citizens to comply with the (private) terms and conditions of their own surveillance or to stay off the (public) streets. As Nick Pinto points out, "there is a different issue at play here: the right of the City of New York to surrender [citizens'] data for us[.]"[265]

ii. Coercing Data Sharing in the Sharing Economy

At first glance, one might expect cities to encourage data-driven companies of the sharing economy to operate in their territory: above all, the shared economy epitomizes the cosmopolitan spirit, innovation, and modernity. As Daniel Rach and David Schleicher note, "the presence of bike-or car-or home-sharing services conveys something important about how progressive, how technologically advanced, and indeed how 'world class' a city is."[266] Presence does not necessarily mean the lack of any regulation, however.[267] When cities interact with data-intense companies to design their urban spaces, the quest to improve municipal services, whether well-intended or catering to the incumbent industry's interests,[268] may leave them indifferent to privacy issues.

---

dissertation, University of Pennsylvania) (on file with the University of Pennsylvania Library)

264. *See, e.g.*, Greg B. Smith, *De Blasio's Wi-Fi Plan Gives Slower Service to Poorer Neighborhoods*, N.Y. DAILY NEWS (Nov. 24, 2014), http://www.nydailynews.com/new-york/exclusive-de-blasio-wi-fi-plan-slower-poor-nabes-article-1.2021146 [https://perma.cc/J6DP-A3MB]; T.C. Sottek, *New York City's Ambitious Free Wi-Fi Plan Sounds Great, Unless You Live in a Poor Neighborhood*, VERGE (Nov. 24, 2014), https://www.theverge.com/2014/11/24/7275567/nyc-public-wifi-is-rich [https://perma.cc/E3J5-QNGA].

265. Pinto, *supra* note 257.

266. *See* Daniel E. Rauch & David Schleicher, *Like Uber, but for Local Government Law: The Future of Local Regulation of the Sharing Economy*, 76 OHIO ST. L.J. 901, 946 (2015).

267. *Id.* at 906–09 (arguing that cities will regulate the shared economy by providing subsidies to companies, promoting redistributive measures and co-opting them in exchange for municipal services).

268. *Id.* at 962–63

New York City offers several case studies of privacy-related tensions between the city government and the sharing economy. For example, New York City's powerful Taxi and Limousine Commission (TLC) has long required ride-hailing firms to provide the agency with information such as pick-up times and locations, license plate numbers, and base information. In May 2016, however, the TLC issued a "driver fatigue rule" that additionally required such firms (including Uber, its competitors, and other for-hire vehicles like black limos) to share more granular information, including the duration and destinations of drivers' trips.[269] Uber objected on both privacy and trade-secret grounds and even tried to avoid the rule by releasing a free tool allowing cities and developers to track car travel times.[270] Uber based its objections in part on a prior slip up in which the TLC released a dataset that contained identifiable information about yellow taxi trips, allowing civic hackers to deanonymize the released data and, by combining it with paparazzi photos of celebrities, figure out exactly which restaurants they visited and whether they added a tip to their taxi fare.[271] Despite these concerns, the TLC proceeded with the new rule and, to the delight of city transportation planners, as of February 1, 2019, ride-share companies must provide the TLC with "the date, time, and location of pickups and drop-offs (at least down to the intersection), the vehicle's license number, the trip mileage, itemized trip fare, route (including whether the vehicle entered traffic-choked Midtown), and how much the driver was paid."[272]

---

269. *See* Vincent Barone, *Uber, NYC at Odds Over Data Collection for New Safety Rule*, AM N.Y. (Dec. 5, 2016), https://www.amny.com/transit/uber-nyc-at-odds-over-data-collection-for-new-safety-rule-1.12707850 [https://perma.cc/ATJ2-7ZZQ]. The rule addressed driver fatigue by prohibiting all drivers from picking up passengers for more than 12 hours in any 24-hour period and more than 72 hours in any seven-day period. *See* Vincent Barone, *NYC Introduces New Taxi Rules to Keep Tired Drivers Off the Streets*, AM N.Y. (May 24, 2016), https://www.amny.com/transit/nyc-introduces-new-taxi-rules-to-keep-tired-drivers-off-the-streets-1.11836141/ [https://perma.cc/GKA3-FQ7M].

270. *See* Aarian Marshall, *The Secret Uber Data That Could Fix Your Commute*, WIRED (Feb. 3, 2017, 10:00 AM), https://www.wired.com/2017/02/ubers-coughing-data-nyc-fix-commute/ [https://perma.cc/9KU3-XESM].

271. *See* J.K. Trotter, *Public NYC Taxicab Database Lets You See How Celebrities Tip*, GAWKER (Oct. 23, 2014, 12:00 PM), https://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546 [https://perma.cc/44KQ-57JW].

272. *See* Aarian Marshall, *NYC Now Knows More Than Ever about Your Uber and Lyft Trips*, WIRED (Jan. 21, 2019, 6:18 PM),

In demanding this information, the TLC showed a near-perfect disregard for data stewardship. As Albert Gidari noted:

> The Commission conducted no privacy impact assessment; considered no alternatives with lesser privacy impacts; and failed to inform the public how long it would keep the data, with what other government agencies it would share it and for what purposes, or to whom it would disclose it such as in response to public records act requests or for commercial use. The Commission has no privacy officer and no privacy policy to govern its conduct. It is accountable to no one.[273]

New York City regulators have also taken an aggressive stance toward collecting data from home-sharing platforms such as Airbnb, which enable hosts to list their apartments for short-term rentals. Worried about the impact of removing these apartments from the long-term rental market, the availability of affordable housing and the deterioration in residential peace and quiet from a constant stream of visitors, the New York City Council enacted a ban on short-term apartment rentals in residential buildings with three or more units.[274] This law proved hard to enforce for the obvious reason that the Airbnb website "does not display the real names and addresses of its hosts," making it extremely difficult for enforcement agencies to "access a comprehensive list of Airbnb hosts in the city."[275] In the face of pervasive disregard of this law by Airbnb hosts,[276] the City Council then passed Local Law 146, requiring home-sharing firms to turn over voluminous monthly data regarding the rental activity of their customers ("hosts"); this included both personally identifying information and financial data and imposed large penalties on firms that failed to comply.[277] Airbnb and its competitor HomeAway then filed suit against the city seeking to enjoin enforcement of the ordinance on two main grounds: first, that

---

https://www.wired.com/story/nyc-uber-lyft-ride-hail-data/ [https://perma.cc/2PWK-SE8H].

273. Albert Gidari, *"Smart Cities" Are Too Smart for Your Privacy*, CTR. FOR INTERNET & SOC'Y (Feb. 20, 2017, 5:39 PM), http://cyberlaw.stanford.edu/blog/2017/02/smart-cities-are-too-smart-your-privacy [https://perma.cc/6X3K-PS5B].

274. *See generally* Tess Hofmann, Note, *Airbnb in New York City: Whose Privacy Rights Are Threatened by a Government Data Grab?*, 87 FORDHAM L. REV. 2589 (2019).

275. *Id.* at 2596 (citation omitted).

276. *Id.* at 2597 (citing a report by the New York State Attorney General that indicates that "72 percent of units booked as short-term rentals on Airbnb violated the ban on renting entire homes for fewer than thirty days.").

277. *See* N.Y.C. ADMIN. CODE §§ 26-2101–05 (McKinney 2019).

the ordinance violated the Fourth Amendment by compelling them to turn over protected business records without any opportunity for pre-compliance review before a neutral decisionmaker; and, second, that it conflicted with (and is preempted by) the Stored Communications Act (SCA) by requiring home-sharing platforms to divulge information about customers without a subpoena or other legal process as required by the SCA.[278] The Southern District of New York court granted their request for a preliminary injunction, finding that the large scale collection of private business records "unsupported by individualized suspicion or any tailored justification" fails to qualify as a reasonable search and seizure.[279]

In reaching its decision, the Southern District court relied heavily on the Supreme Court's judgment in *Patel v. Los Angeles*, in which a Los Angeles ordinance was found facially invalid under the Fourth Amendment for requiring hotel operators to record, maintain and make available for inspection by the police certain personal information about guests.[280] The court reasoned that just like a hotel, a home-sharing platform has two strong reasons to keep host and guest data private. One is competitive; the other involves the promotion of better customer relations.[281] The court also rejected the city's argument that the platforms' privacy interests in their customers' records were diminished due to the permissiveness of "administrative searches" in other industries.[282] Since the hotel industry does not involve inherently dangerous operations, the court was reluctant to extend precedents from more regulated industries to the present context.[283] After finding the ordinance within the scope of the Fourth Amendment, the court then analyzed whether the Fourth Amendment's reasonableness standard was met. The court reasoned that under the Fourth Amendment, administrative searches of commercial establishments required individualized suspicion for the search and an opportunity for a pre-compliance review before a neutral decisionmaker.[284] It concluded that:

> In its sweep, the Ordinance dwarfs that of the Los Angeles ordinance at issue in *Patel*. The universality of the [New York City] Ordinance's monthly production demand (covering all short-term

278. Airbnb, Inc. v. City of New York, 373 F. Supp. 3d 467, 476 (S.D.N.Y. 2019).
279. *Id.* at 492.
280. Patel v. City of Los Angeles, 135 S. Ct. 2443, 2447 (2015).
281. *See Airbnb, Inc.*, 373 F. Supp. 3d at 484.
282. *Id.* at 485.
283. *Id.*
284. *Id.* at 487–90.

> rentals in New York City), the sheer volume of guest records implicated, and the Ordinance's infinite time horizon all disfavour the Ordinance when evaluated for reasonableness under the Fourth Amendment.[285]

In addition to these privacy concerns, this approach is also an example of Richard Schragger's emphasis on agglomeration effects, which are more likely to occur in big cities. Instead of choosing to leave New York City for less regulated markets, Airbnb decided to stay and invest in a legal battle. Conversely, a few years back, Uber and Lyft chose to leave Austin, Texas, when the city introduced fingerprint-based background checks and other data reporting requirements on all hail-riding drivers in the city.[286] Uber and Lyft only returned — to the detriment of a locally grown alternative non-profit ride-share — when Texas overrode Austin's effort, passing a regulation requiring licensing of the service against a fee on the state level.[287] Disempowered by legal constraints on regulating their urban spaces, cities sometimes turn to data regulation — with varying degrees of privacy intrusion.[288]

After reviewing the current Airbnb litigation, this Article now turns to more collaborative forms of data sharing between cities and tech firms, focusing on a privacy-friendly-model spearheaded in Seattle.

iii. Collaborative Data Trusts

New York City resorted to a government data grab to gain access to ride- and home-sharing data from industry leaders. But other cities have followed a different path. For example, in January 2015, Uber agreed to provide Boston with "anonymous data about the duration,

---

285. *Id.* at 491. Although the court's main objection to the Ordinance was that it seemed to invite a fishing expedition, it also evoked the reasoning in the recently decided *Carpenter* case, stressing that "the test of reasonableness" under the Fourth Amendment "is not whether an investigative practice maximizes law enforcement efficacy" but rather must also balance other factors such as the extent of the intrusion on protected privacy interests. *Id.* at 492 (citing Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018)).

286. Associated Press, *Uber and Lyft Return to Austin after Texas Law Kills the City's Fingerprint Rule*, L.A. TIMES (May 29, 2017, 12:05 PM), https://www.latimes.com/business/technology/la-fi-tn-uber-austin-20170529-story.html [https://perma.cc/68D6-4EPM].

287. *Id.*

288. *See* MEG YOUNG ET AL., BEYOND OPEN VS. CLOSED: BALANCING INDIVIDUAL PRIVACY AND PUBLIC ACCOUNTABILITY IN DATA SHARING (2019), https://faculty.washington.edu/billhowe/publications/pdfs/young_open_v_closed_semi_synthetic_data.pdf [https://perma.cc/ASV2-U6WY].

general locations, and times of rides that start or end in the city" on a quarterly basis.[289] A year later, Boston city officials expressed some frustration at both Uber's refusal to allow data sharing with a regional planning agency and the utility for planning purposes of the underlying data.[290] In a nutshell, data sets limited to trips' start and end locations by zip codes did not allow "for analysis of how proximity to public transit affects Uber usage, or how a new building affects transportation patterns."[291] Where cooperative partnerships have had the most success to date is in the bike-sharing industry. Both New York City and Boston worked out arrangements with the operators of Citi Bike and Blue Bike, respectively, to make some ride data publicly available subject to a data license agreement that imposes a number of privacy-related restrictions.[292] Seattle has taken an even more innovative approach to cooperative data sharing. A proper analysis of the Seattle approach requires some background information on data trusts and their potential use in balancing the competing interests of cities, sharing economy firms, and local citizens and customers.

Data trusts are intended to create a fiduciary relationship between a trustee and a beneficiary, such that the former is under a duty to act for the benefit of the latter according to the particular terms of the trust.[293] For example, a group of Fitbit and Apple Watch users might

---

289. Nicole Dungca, *In First, Uber to Share Ride Data with Boston*, BOS. GLOBE (Jan. 14, 2015, 5:33 AM), https://www.bostonglobe.com/business/2015/01/13/uber-share-ridership-data-with-boston/4Klo40KZREtQ7jkoaZjoNN/story.html [https://perma.cc/29MT-9CB9] (noting that the ride-share data from Uber "would be stripped of identifying information and exact locations"). The agreement stipulated that this information was confidential and constituted Uber's trade secrets under the state public records law, thereby exempting it from disclosure; it also limited sharing such information beyond the city government without Uber's approval. *See* Uber Technologies Inc.-City of Boston Agreement on the Provision of Uber City Data (Jan. 12. 2015) *available at* https://www.documentcloud.org/documents/1513002-final-city-data-agreement-boston-uber-011215.html [https://perma.cc/QH22-N8R8].

290. *See* Adam Vaccaro, *Highly Touted Boston-Uber Partnership Has Not Lived Up to Hype So Far*, BOSTON.COM (June 16, 2016), https://www.boston.com/news/business/2016/06/16/bostons-uber-partnership-has-not-lived-up-to-promise [https://perma.cc/4NA7-SM3B].

291. *Id.*

292. *See, e.g.*, *Motivate Data License Agreement*, BLUEBIKES, https://www.bluebikes.com/data-license-agreement [https://perma.cc/37AK-BD4B] (last visited May 26, 2020); *CitiBike Data License Agreement*, CITI BIKE, https://www.citibikenyc.com/data-sharing-policy [https://perma.cc/QP3P-HQU6] (last visited Mar. 13, 2020).

293. *See* Sylvie Delacroix & Neil D. Lawrence, *Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, 9 INT'L DATA

agree to pool their medical data in a data trust with explicit terms for how the trustee may share the data for medical research purposes — subject to various limitations set out in advance, and to the trustee's independent judgment of which uses uphold the interests of the users. The benefits of such a trust structure are threefold. First, in the typical scenario in today's digital world, data controllers amass huge amounts of data about data subjects who have limited understanding of how controllers may use their data and almost no power to avoid unwanted or harmful uses.[294] In sharp contrast, the legal structure of a data trust guarantees that trustees manage beneficiaries' data according to the terms of the trust and subject to a legally enforceable fiduciary obligation.[295] Second, whereas data controllers seek to maximize the value of the personal data they collect for the benefit of shareholders, trustees owe a duty of undivided loyalty, requiring them to maintain their independence from profit-maximizing activities.[296] Finally, trust instruments are highly flexible and therefore allow a wide variety of data sharing policies, thereby providing data subjects a range of choices that reflect their own values and needs in a given context.[297] That said, a trust structure has certain disadvantages, including daunting implementation challenges. Sylvie Delacroix and Neil Lawrence identify two issues requiring special attention: uptake (i.e., how to educate potential users about the benefits of data trusts) and exit procedures (i.e., how to identify all data associated with a user wishing to leave a data trust).[298]

A 2016 article by internet scholars Jack Balkin and Jonathan Zittrain popularized the idea of imposing a general fiduciary duty on service providers like Google, Facebook, and Uber.[299] Their

---

PRIVACY L. 236, 240–41 (2019) (noting that in a data trust, data subjects tend to act as both settlors and beneficiaries).

294. *Id.* at 239.

295. *Id.* at 241 (noting that if a dispute arises over a trustee's conduct, the burden of proof is on trustees to demonstrate that "they have sought to promote the beneficiaries' interests with appropriate degrees of impartiality, prudence, transparency and undivided loyalty").

296. *Id.*

297. *Id.*

298. *Id.* at 251; CHRIS REED, BPE SOLICITORS & PINSENT MASONS, DATA TRUSTS: LEGAL AND GOVERNANCE CONSIDERATIONS 8 (2019), https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf [https://perma.cc/YNS9-7AAV] (explaining how a recent report commissioned by the Open Data Institute finds even more severe problems with data trusts and concludes that "[t]rust law is not an appropriate legal structure for data trusts").

299. Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016),

argument turns on a provocative analogy between doctors, lawyers, and accountants, who are required by law to act in good faith towards their clients, and firms in the information industry that supposedly have many of the trappings of fiduciaries. The main shortcoming of their analysis is that it offers no compelling arguments as to why such firms would agree to assume fiduciary duties on a voluntary basis.[300] Of course, this problem is surmountable if Congress or state legislatures enact appropriate legislation imposing such duties on information-intensive firms.[301] Otherwise, the idea of information fiduciaries seems like a non-starter for the private sector.

But this is not the case for city governments. Despite the mixed reception of data trusts in the scholarly literature,[302] a few cities have proactively partnered with universities to develop trust-based infrastructures for managing sharing economy data in the public interest. One major difference between these efforts and earlier discussions of data trust is that instead of relying solely on the *legal* structure of trust to achieve their goals, city-university partnerships are adopting a *techno-legal* approach that incorporates sophisticated technical infrastructure for ensuring the protection of data deposited in the trust repository.

For example, in July 2017, Seattle began implementing a pilot program for "dockless-bikes" under which bike-share operators had two options for sharing granular data about their riders with the city: they may provide the city with anonymized trip information as specified in Seattle's Bike Share Permit Requirements, or they may share data under a signed agreement with the Transportation Data Collaborative (TDC) located at the University of Washington (UW).[303] The TDC is a protected and linked data repository of sensitive information from regional public and private transportation

---

https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ [https://perma.cc/3LLC-ZABD].

300. *Id.* This article is based on earlier work by Balkin. *See generally* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016). For a critical assessment of Balkin's ideas, see generally Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019).

301. On December 12, 2018, Senator Brian Schatz (D-HI) and a group of 15 Democratic senators introduced a bill that would impose duties of care, loyalty, and confidentiality on online service providers with respect to processing and securing user data. *See* Data Care Act of 2018, S. 3744, 115th Cong. (2d Sess. 2018).

302. For a critical assessment, see generally Khan & Pozen, *supra* note 300.

303. *See Seattle Bike Share Requirements*, SEATTLE.GOV (June 30, 2017), www.seattle.gov/Documents/Departments/SDOT/BikeProgram/BicycleSharePermitRequirements.pdf [https://perma.cc/7CKT-AKUS].

providers. It allows partnering agencies to create data-driven policy, support research uses, and provide individuals with authenticated access to their own transportation records.[304] More specifically, the TDC provides:

- Policies and protocols that address data ownership, access, use, and related privacy and ethics in the interest of partner organizations and the persons represented by the data, supported by the UW's Urban Infrastructure Lab;
- A neutral third-party host with transportation expertise (the Washington State Transportation Center (TRAC)) to enable data sharing and analysis;
- Protection from disclosure under the Washington Public Records Act via administrative, legal, and legislative efforts available to the UW; and
- A trusted data platform, which provides privacy and security tools, such as encryption for sensitive attributes, data tagging to track and audit the uses and users of data, and policy-based encryption.[305]

A recent paper co-authored by TDC staff members at UW makes a case for data collaboratives by observing that researchers and the public are very poorly served by the usual dichotomy between open (publicly available) and closed (proprietary) data systems.[306] Institutions are reluctant to make "sensitive" data openly available to researchers mainly on privacy and IP grounds, and therefore restrict access to such data or its linkage with other data sets, thereby instead sharing less interesting and useful information with the research community. As seen above, this tension is apparent in the transportation sector, where city agencies want more granular access to firm data than ride-hailing and bike-share firms wish to supply. Building on their work in creating the TDC, the co-authors describe

---

304. *See What Is the Transportation Data Collarborative?*, UW TRANSP. DATA COLLABORATIVE, https://www.uwtdc.org/about [https://perma.cc/U3MV-V2EN] (last visited Apr. 3, 2020).

305. *See Transportation Data Collaborative*, URBANALYTICS, https://urbanalytics.uw.edu/projects/transportationdatacollab/ [https://perma.cc/TQY9-ES5H] (last visited Apr. 3, 2020). Other university labs, most notably the Governance Lab (GovLab) at New York University's Tandon School of Engineering, have also sponsored initiatives to create and validate data collaboratives. *See* Stefaan Verhulst, *Data Collaboratives Can Transform the Way Civil Society Organisations Find Solutions*, LIVING LIBR. (Feb. 22, 2018), https://thelivinglib.org/data-collaboratives-can-transform-the-way-civil-society-organisations-find-solutions [https://perma.cc/S6K9-B7NF].

306. *See* YOUNG ET AL., *supra* note 288.

the design of a "legal-technical infrastructure" they call Collaborative Data Trusts (CDTs), which they offer as an alternative to the open versus closed data dichotomy.[307]

One important way in which the UW data trust achieves privacy goals is by relying on differential privacy and synthetic datasets, which allow for the responsible use of sensitive data by removing causal relationships between variables (basically adding noise to prevent re-identification) while preserving relationships in all other cases (thereby preserving utility).[308] The use of customized synthetic datasets also allows researchers to remove signals that could expose proprietary data (and hence competitive advantage for the data providers) or preserve biases that could reinforce discriminatory policies.[309] Finally, the integrated techno-legal infrastructure utilizes data sharing and use agreements to specify in advance the data to be shared, the scope of research, and the legal recourse of the data trust if data quality is deficient and of the data sources in the event of unauthorized disclosure.[310] Data trusts hold enormous promise for cities engaged in data management activities. They enable city governments to maintain their role as data stewards while benefiting from data-driven activities, even as they interact with the private sector in a highly collaborative manner.[311]

iv. From Data Sharing to Toronto's Outsourcing of Data Governance

The largest and most controversial smart city project in which data trusts play a prominent role is Sidewalk Lab's efforts to build a smart city of the future in Toronto.[312] In the spring of 2017, Waterfront

---

307. *See id.* For a very similar approach, see Lisa M. Austin & David Lie, *Safe Sharing Sites*, 94 N.Y.U. L. REV. 581, 584–85 (2019).

308. YOUNG ET AL., *supra* note 288.

309. *Id.*

310. *Id.*

311. *Id.*

312. Shortly before publication of this Article, Sidewalk Labs announced that it was no longer pursuing this project, attributing its decision to the "unprecedented economic uncertainty" both worldwide and in the Toronto real estate market. *See* Daniel L. Doctoroff, *Why We're No Longer Pursuing the Quayside Project — And What's Next for Sidewalk Labs*, MEDIUM (May 7, 2020), https://medium.com/sidewalk-talk/why-were-no-longer-pursuing-the-quayside-project-and-what-s-next-for-sidewalk-labs-9a61de3fee3 [https://perma.cc/T8U5-WA2J]. Doctoroff (Sidewalk Labs' CEO) also stated that the ideas developed in the Quayside project "represent a meaningful contribution to the work of tackling big urban problems, particularly in the areas of affordability and sustainability. This is a vital societal endeavor, and Sidewalk Labs will continue our work to contribute to it." *Id.* Thus, despite the demise of Sidewalk Labs role, the Quayside project remains an

Toronto (WT), a Canadian redevelopment agency established in 2002 by the government of Canada, the government of Ontario, and the city of Toronto to oversee the revitalization of Toronto's eastern waterfront, issued a Request for Proposal (RFP) for the Quayside Development project.[313] It sought an "Innovation and Funding Partner" to help create and fund "a globally-significant community that will showcase advanced technologies, building materials, sustainable practices[,] and innovative business models that demonstrate pragmatic solutions toward climate-positive urban development."[314] Six weeks later — a rather short time for an RFP of such complexity — WT selected Sidewalk Labs.[315]

In the fall of 2017, WT and Sidewalk Labs signed a Framework Agreement for what many now referred to as the "Sidewalk Toronto" project. This agreement generated criticism and controversy mostly due to the secrecy over the full agreement. Only a summary was ever

---

important learning experience for cities, urban innovation firms, and information law scholars.

313. *See* WATERFRONT TORONTO, REQUEST FOR PROPOSALS: INNOVATION AND FUNDING PARTNER FOR THE QUAYSIDE DEVELOPMENT OPPORTUNITY 6 (2017), https://storage.googleapis.com/sidewalk-toronto-ca/wp-content/uploads/2019/06/13214337/Waterfront-Toronto-RFP-No.-2017-13.pdf [https://perma.cc/6R37-F9Z5]. By 2015, WT was approaching the end of its 20-year lifespan. Although it lacked borrowing authority or the capacity to create subsidiaries due to restrictions in its enabling act, it owned a 12-acre waterfront parcel on Lake Ontario known as "Quayside" and decided to make it the showpiece of a new, second phase of waterfront revitalization. *Id.*; *see also* CITY OF TORONTO, STAFF REPORT FOR ACTION ON WATERFRONT STRATEGIC REVIEW TO EXECUTIVE COMMITTEE 1–4 (2015), https://www.toronto.ca/legdocs/mmis/2015/ex/bgrd/backgroundfile-81763.pdf [https://perma.cc/J5ZX-SLXH]. *See generally* Ellen P. Goodman & Julia Powles, *Urbanism Under Google: Lessons from Sidewalk Toronto*, 88 FORDHAM L. REV. 457 (2019).

314. WATERFRONT TORONTO, REQUEST FOR PROPOSALS: INNOVATION AND FUNDING PARTNER FOR THE QUAYSIDE DEVELOPMENT OPPORTUNITY (2017), https://storage.googleapis.com/sidewalk-toronto-ca/wp-content/uploads/2019/06/13214337/Waterfront-Toronto-RFP-No.-2017-13.pdf [https://perma.cc/6R37-F9Z5] (explaining how WT viewed Quayside as potentially a "national and global model" and it fully intended to expand the project to an adjacent 880-acre waterfront site owned by the City of Toronto and known as the Port Lands public redevelopment area).

315. A report by the Ontario Auditor General subsequently criticized the selection process, noting that Sidewalk Labs was chosen precipitously and without adequate consultation with government. *See generally* Marianna Valverde & Alexandra Flynn, *Mystery on the Waterfront: How the "Smart City" Allure Led a Major Public Agency in Toronto into a Reckless Deal with Big Tech*, CENTRE FOR FREE EXPRESSION (Dec. 3, 2018), https://cfe.ryerson.ca/blog/2018/12/mystery-waterfront-how-smart-city-allure-led-major-public-agency-toronto-reckless-deal [https://perma.cc/HZK8-F592] (describing intense lobbying efforts by Sidewalk Labs and related companies).

published, and it failed to clarify key terms and concepts regarding data ownership and digital governance.[316] Over the next year, Sidewalk Labs took the lead in convening an advisory board and holding public consultations with very limited participation by any city officials.[317] But prominent privacy experts eventually resigned from their role as company consultants or advisory board members.[318]

With this background in mind, the remainder of this Section examines Sidewalk Labs' original data governance and privacy proposal for Sidewalk Toronto as set out in its Master Innovation and Development Plan, a three-volume, 1500-page document issued in June 2019.[319] In a chapter devoted to "Digital Innovation," the firm proposed the creation of an independent "trust" with broad authority over data governance issues within both Quayside and the much larger adjacent site that Sidewalk Labs refers to *in toto* as the "IDEA District."[320] In a nutshell, the proposed Urban Data Trust (UDT) would establish privacy guidelines and a related assessment process administered by its Chief Data Officer who reviews and approves projects using data collected in the physical environment of the IDEA District.

In developing a "trusted process for responsible data use," Sidewalk Labs sought to respond to three concerns raised during the public consultations: first, that data collection in the public realm amounted to a form of surveillance; second, that the collection and

316. *See generally* Goodman & Powles, *supra* note 313.

317. *See* Valverde & Flynn, *supra* note 315.

318. *See* Gabrielle Canon, *'City of Surveillance': Privacy Expert Quits Toronto's Smart-City Project*, GUARDIAN (Oct. 23, 2018), https://www.theguardian.com/world/2018/oct/23/toronto-smart-city-surveillance-ann-cavoukian-resigns-privacy [https://perma.cc/X7RH-8A5T]. Saadia Muzaffar, a tech expert and founder of TechGirls Canada, stepped down because Sidewalk Toronto "was not adequately addressing privacy issues" she and others had raised. *Id.* And former Ontario Privacy Commissioner Ann Cavoukian resigned after learning that "third parties could access identifiable information" gathered in the Quayside district. *Id.*

319. SIDEWALK LABS, MASTER INNOVATION AND DEVELOPMENT PLAN: CHAPTER 5 376–466 (2019), https://quaysideto.ca/wp-content/uploads/2019/09/MIDP-Volume-2-Chapter-5-Digital-Innovation-Accessible.pdf [https://perma.cc/A3QP-AL36]. This chapter builds upon and refines Sidewalk Labs' earlier discussions of a digital governance framework. *See* Alyssa Harvey Dawson, *Digital Governance Proposals for DSAP Consultation*, SIDEWALK LABS 13–17 (Oct. 16, 2018), https://storage.googleapis.com/sidewalk-toronto-ca/wp-content/uploads/2019/06/20223247/Digital-Governance-Proposals-for-DSAP-Consultation.pdf [https://perma.cc/DMU7-YUGZ].

320. *See* SIDEWALK LABS, *supra* note 319, at 378–79.

use of such data should be treated as a public resource (provided privacy risks have been addressed) and not solely benefit the private or public sector; and, third, that Sidewalk Labs should not enjoy any special advantages in developing the core digital services for the IDEA District.[321] The company sought to address these concerns by creating a new category of "urban data" (defined as "information gathered in the city's public realm, its publicly accessible spaces, and even some private buildings")[322] and giving it additional privacy protections by treating urban data as a "collective" asset that would not be owned "in the traditional sense" but rather managed by an independent entity (the UDT) and made publicly accessible by default; and applying consistent processes and guidelines to all entities collecting urban data in the district including Sidewalk Labs. While this strategy sounds reasonable at first glance, it suffers from many shortcomings. The most severe among them is a democratic deficit or lack of political legitimacy.

To begin with, the RFP called upon *the partner* to work closely with WT in creating "the required governance constructs to stimulate the growth of an urban innovation cluster, including legal frameworks (e.g., Intellectual Property, privacy, data sharing)[.]"[323] As many commentators have observed, it is highly problematic for a vendor "to propose the structure, operation, and regulatory power" of the governing entity with authority over the vendor.[324] WT should have set the governance rules for data collected in public spaces that it owned and controlled instead of allowing the proverbial fox to guard the henhouse.

A lack of legitimacy also undermines Sidewalk Lab's conception of a data trust. According to the MIDP, the final agreement between WT and Sidewalk Labs would set up the structure of the UDT and

---

321. *Id.* at 416–18.

322. *Id.* at 377. The distinguishing features of urban data include its connection to a specific physical environment and the difficulty of obtaining informed consent for its collection from individuals as they transit public spaces. This makes urban data different from "more traditional forms of data, termed here 'transaction data,' in which individuals affirmatively — albeit with varying levels of understanding — provide information about themselves through websites, mobile phones, or paper documents." *Id.* at 416.

323. WATERFRONT TORONTO, *supra* note 313, at 17.

324. Natasha Tusikov, *"Urban Data" & "Civic Data Trusts" in the Smart City*, CTR. FOR FREE EXPRESSION (Aug. 6, 2019), https://cfe.ryerson.ca/blog/2019/08/%E2%80%9Curban-data%E2%80%9D-%E2%80%9Ccivic-data-trusts%E2%80%9D-smart-city [https://perma.cc/UZ5C-MG64]; *see also* Goodman & Powles, *supra* note 313, at 474 (asking "why is a vendor making policy?").

authorize the creation of a non-profit entity with "the charter to address the digital governance challenges related to urban data while also promoting data-driven innovations that benefit individuals and society."[325] This oversight entity would have a five-member board (drawn from various sectors) and a Chief Data Officer (CDO) responsible for developing the UDT charter, promulgating "Responsible Data Use (RDU) Guidelines," and structuring oversight and review processes. Subject to the oversight board's approval, the CDO would also determine how the entity would be staffed, operated, funded, and perform various other tasks.[326] Although Sidewalk Labs offers a number of ideas for ensuring the board's independence and avoiding conflicts of interest, it is silent as to the basics of governance such as who appoints board members, their qualifications and the necessary expertise in relation to their defined tasks, the board's procedures for handling complaints about the CDO's policy decisions, or their powers of enforcement. Additionally, it has very little to say about the sources of funding for the UDT or what happens if, down the road, Sidewalk Labs walks away from the project.

This lack of legitimacy has two probable consequences for Sidewalk Labs' data governance proposal. First, although the RDU Guidelines incorporate well-established privacy principles and outline an RDU Assessment process covering any collection or use of urban data,[327] it is not at all clear how the CDO will handle the difficult choices he or she will likely encounter. For example, will the CDO balance risks and benefits in the public or corporate interest? As Sean McDonald notes, "[t]he Urban Data Trust is likely to have to weather a significant amount of political and financial pressures, which is a challenge for any institution — let alone one trying to maintain the public's interest in data governance amidst financial dependence."[328] This suggests that the UDT will have to draw on its

---

325. SIDEWALK LABS, *supra* note 319, at 420.

326. *Id.* at 420–21.

327. The assessment process considers the purpose of the project, the data sources (including questions of storage, access, and transfer), legal compliance, and risk-benefit analysis. The CDO weighs these factors and then makes a final decision, denying, approving, or approving with conditions. *See id.* at 420. Overall, this process is quite similar to the familiar concept of Privacy Impact Assessments, although it is somewhat broader given its attention to the ethical implications of artificial intelligence.

328. Sean McDonald, *MIDP: The Data Governance Proposal*, MEDIUM (June 26, 2019), https://medium.com/swlh/midp-the-data-governance-proposal-55272767dd40 [https://perma.cc/7D5R-YWDW].

political capital to maintain its independence, but in reality, it will have very little capital to draw upon.

Second, this democratic deficit leaves Sidewalk Labs in a weak position to mitigate any controversies resulting from its creation of a new category of urban data. The company asserts that it heard public concerns over the collection of such data and responded by laying out the guidelines and assessment process described above.[329] Absent from this response is any discussion of simply restricting the collection of urban data or strengthening Canadian privacy law.[330] Unsurprisingly, critics have dismissed the very notion of urban data as "an elaborate contortion aimed at giving Sidewalk Labs the regulatory cover it needs to collect data without consent in public places that it quasi-owns."[331] Nor does Sidewalk Labs allay these concerns by emphasizing open standards and open data. To its credit, the company offers a plan to ensure a digitally open city. This plan is laudable, yet it seems disingenuous given that Sidewalk Labs already enjoys advantages that few other companies can ever match, even if Quayside achieves the status of a digitally open city. These include deep expertise with collecting and using urban data, ownership interests or investments in other companies that have already developed many of the tools needed to make Quayside successful,[332] and access to the financial resources and technical sophistication of its multibillion-dollar sister firm, Google.

Following the release of the MIDP, the chair of WT issued an open letter identifying concerns with the size, scope, and funding of Sidewalk Labs proposal, and seeking additional information on data governance issues.[333] On October 31, 2019, the chair released a second open letter announcing that the parties had reached "alignment" on these and other "threshold issues" based on Sidewalk Labs confirmation that it would scale back the proposal from the

---

329. *See* SIDEWALK LABS, *supra* note 319, at 416.

330. *See* Tusikov, *supra* note 324.

331. McDonald, *supra* note 328; *see also* Goodman & Powles, *supra* note 313, at 472 (explaining how "it is notable that the trust mechanism envisaged *no* limits on data collection or use, nor did it ensure that there will be surveillance-free zones.").

332. These include Flow Inc. (which makes a traffic-management system); Intersection (which makes public Wi-Fi networks); and Cityblock Health, Inc. (which delivers innovative healthcare to low-income neighborhoods). *See* Valverde & Flynn, *supra* note 315.

333. *See* Stephen Diamond, *Open Letter from Waterfront Toronto Board Chair, Stephen Diamond Regarding Quayside*, WATERFRONT TORONTO (June 24, 2019), https://www.waterfrontoronto.ca/nbe/portal/waterfront/Home/waterfronthome/newsroom/newsarchive/news/2019/june/open+letter+from+waterfront+toronto+board+chair%2C+stephen+diamond+regarding+quayside [https://perma.cc/N3D9-L6VC].

190-acre IDEA District to the original 12-acre Quayside site; switch to a new, WT-led approach to data governance based on existing Canadian privacy law; partner with other real estate developers rather than act as lead developer and modify its revenue-sharing plans with WT; and make various other concessions.[334]

The WT letter emphasizes that this compromise does not represent a final agreement. Rather, it allows WT to proceed with the formal evaluation of the MIDP subject to further public consultation and assessment with a final decision anticipated by March 31, 2020. As to data governance and privacy issues, Sidewalk Labs agreed that going forward, WT will act as the lead on any future discussions with governmental entities; comply with all existing and future privacy legislation, regulations, and policy framework; accept that relevant municipal provisions and federal laws will determine data governance; store all personal information collected in its digital operations within Canada; and not use "Urban Data" as a term and otherwise eliminate the UDT from its proposal.[335] As required by the agreement on threshold issues, Sidewalk Labs very recently delivered a Digital Innovation Appendix (DIA) that updates the MIDP and will become the basis for formal evaluation of the project.[336]

In short, it is too soon to say how the Sidewalk Toronto project will play out or even if it will move forward to the building stage.[337] Still,

---

334. Stephen Diamond, *Open Letter from Waterfront Toronto Board Chair*, WATERFRONT TORONTO (Oct. 31, 2019), https://www.waterfrontoronto.ca/nbe/portal/waterfront/Home/waterfronthome/newsroom/newsarchive/news/2019/october/open+letter+from+waterfront+toronto+board+chair+-+october+31%2C+2019 [https://perma.cc/7VPD-M2N9]. For a summary of the letter, see Nick Summers, *Toronto Is Reining in Sidewalk Labs' Smart City Dream*, ENGADGET (Oct. 31, 2019), https://www.engadget.com/2019/10/31/sidewalk-labs-waterfront-toronto-threshold-issues/ [https://perma.cc/CQ2A-DFJ5].

335. *See* Letter from Waterfront Toronto to Sidewalk Labs 5–7 (Oct. 29, 2019), https://www.waterfrontoronto.ca/nbe/wcm/connect/waterfront/86d92f81-20be-4029-a616-00522abbd34a/Threshold+Issues+Resolution+Documents.pdf?MOD=AJPERES [https://perma.cc/J7Z5-JUEE].

336. SIDEWALK LABS, MASTER INNOVATION & DEVELOPMENT PLAN: DIGITAL INNOVATION APPENDIX (2019), https://storage.googleapis.com/sidewalk-toronto-ca/wp-content/uploads/2019/11/15093613/Sidewalk-Labs-Digital-Innovation-Appendix.pdf [https://perma.cc/7B6V-HBJD]; Sarah Wray, *Sidewalk Labs Details Digital Systems, Says It Won't Sell Data or Use Facial Recognition*, SMART CITIES WORLD (Nov. 19, 2019), https://www.smartcitiesworld.net/news/news/sidewalk-labs-details-digital-systems-says-it-wont-sell-data-or-use-facial-recognition—4797 [https://perma.cc/K8DE-7AVV].

337. Quite apart from the question of WT's ultimate approval, there is a lawsuit pending that seeks to block the agreements between Sidewalk Labs and Waterfront

we can speculate about why it shaped up the way it has. Richard Schragger has described a market-based theory of local government whose two key features — dependence on private investment and competition for private investment with other municipalities — results in "development and business-friendly policies."[338] Something along these lines is no doubt at work with WT, a redevelopment agency nearing the end of its mandate and its funding and lacking the ability to borrow money. In Sidewalk Labs, WT found an ideal partner, at least at the outset. From Alphabet's point of view, Sidewalk Toronto was the opportunity it had been looking for to build a city "from 'the Internet up.'" "What I mean by that," writes Sidewalk Labs CEO Dan Doctoroff, "is a place where ubiquitous connectivity is truly built into the foundation of the city, and where people use the data that's generated to enhance quality of life."[339] In *The Age of Surveillance Capitalism,* Shoshana Zuboff portrays the marriage between development-favoring cities and the information industry somewhat differently. For Zuboff, the industry's relentless drive for new sources of data leads inevitably to the "real" world, and hence to the city as one of the few remaining virgin tracts for data extraction and monetization. "Whether what even . . . Doctoroff . . . refers to as a 'Google city' succeeds," Zuboff notes, "the company has interested the public by recasting our central gathering places as a commercial operation in which once public-assets and functions are reborn as the cornered raw materials earmarked for a new marketplace."[340]

In sum, the above case studies establish that cities vary widely in their attitudes towards data stewardship and their dedication of resources to building out programs that include all five components identified by Finch and Tene (in brief, adoption of privacy principles, the appointment of a privacy lead, risk management, vendor

---

Toronto in its entirety. *See* Donovan Vincent & Rob Ferguson, *Civil Liberties Group Launches Court Action to Stop Quayside, Says Canadians Should Not Be 'Lab Rats'*, STAR (Apr. 16, 2019), https://www.thestar.com/news/gta/2019/04/16/civil-liberties-group-launches-court-action-to-stop-quayside-says-canadians-should-not-be-lab-rats.html [https://perma.cc/VT6S-SCCV].

338. Richard Schragger, *The Political Economy of City Power*, 44 FORDHAM URB. L.J. 91, 96–98 (2017).

339. Daniel L. Doctoroff, *Reimagining Cities from the Internet Up*, MEDIUM (Nov. 30, 2016), https://medium.com/sidewalk-talk/reimagining-cities-from-the-internet-up-5923d6be63ba [https://perma.cc/UG26-XARY].

340. ZUBOFF, *supra* note 79, at 228.

management and ethical review of AI programs).[341] Moreover, some cities are quite inconsistent in their privacy awareness, depending on their desired goals. For example, New York City's local laws protecting personal data held by city agencies is a model of data stewardship with its strong embrace of privacy principles and internal management programs using a risk-based approach. In sharp contrast, the LinkNYC broadband initiative allows a private firm to set the terms of engagement. While it may succeed in generating high revenues for the city while providing Wi-Fi access to a small number of residents, it scores a failing grade on all five components. Similarly, New York City wanted and got sharing economy data from the likes of Uber and Airbnb by relying on aggressive rulemaking that sparked lawsuits. But in the process, it almost completely disregarded data stewardship. Seattle and several other cities have experimented with alternative approaches to data stewardship by embracing the idea of data trusts, with Seattle demonstrating leadership by developing both the technical and legal aspects of such trusts. Finally, Toronto — a complex and ongoing saga of privacy in the smart city — offered a plan that matched up very nicely with the five components, in the sense that it checked every box. Toronto's government, however, had to fall on its sword and withdraw much of its proposed plan when it became clear that the citizens of Toronto would not stand for a private firm setting its own rules for governing data in public (or quasi-public) spaces.

IV. THE RHETORIC OF BARCELONA: THE PROMISE OF A "PUBLIC" SMART CITY

Critics of smart city solutions have pointed to the neoliberal turn around which municipalities have started to converge worldwide. The heart of the criticism goes into the very framing of the smart city concept, dominated by a logic of inevitability and an aura of a self-evidently progressive project.[342] Can we reimagine the relationship between technology companies and cities in which technology is used for the benefit of citizens instead of big companies? In which Sidewalk Labs does not use the data from Quayside simply to perfect its AI but to build digital solutions that promote citizen participation, help personalize services, and de-bureaucratize national and local governments, all the while

341. *See* Finch & Tene, *supra* note 196, at 127–34.

342. *See* EVGENY MOROZOV & FRANCESCA BRIA, RETHINKING THE SMART CITY: DEMOCRATIZING URBAN TECHNOLOGY 23–24 (2018).

preserving privacy and creating a more enjoyable local environment that stimulates growth? A Spanish city in Europe — Barcelona — is now branding itself as the alternative smart city, one in which the municipality retains control over critical urban infrastructure and services.

Francisco Franco's dictatorship in Spain in the 1940s–50s epitomized centralism. Thereafter, the resurgent Basque and Catalan nationalist movements were appeased with accentuating regionalism in the 1978 Spanish Constitution — a move toward "non-institutional federalism" that was based on the territorial division of the country into 17 autonomous communities.[343] By 2012, half of the Spanish state spending was managed at a regional and municipal level, whilst these two tiers of government also employed 70% of all state employees.[344] Municipal governments were given wide responsibilities in areas as broad as land use, public utilities, sport, transportation, and even childcare.[345] Total local public expenditure tripled during the years of economic expansion, that is, between 1993 and 2009.[346] However, after a pan-European financial crisis, in 2010, the Spanish model of deep decentralization came under severe pressure. The initial reaction to the 2009 financial crisis of the Spanish government was to draw up an expansionist program of €25 billion. The program, known as "Plan E," involved funding projects that were to be carried out by local governments, including small to medium investments in infrastructure and other specific policies like technological development. However, in May 2010, the central government adopted a strict economic stability package in close adherence to the criteria laid down by the European economic authorities. This program sought to cut public debt from 9.2% of GDP in 2010 to just 3% by 2013 and incorporated a wide range of austerity measures that hit especially hard the local governments in Spain.[347]

---

343. Andrew Dowling, *A Tale of Two Cities: Barcelona and Madrid in Spain*, *in* CITIES AS POLITICAL OBJECTS: HISTORICAL EVOLUTION, ANALYTICAL CATEGORIZATIONS AND INSTITUTIONAL CHALLENGES OF METROPOLITANIZATION 81 (Alistair Cole & Renaud Payre eds., 2016).

344. *Id.*

345. Carmen Navarro & Esther Panos, *Spanish Local Government and the Austerity Plan: In the Eye of the Perfect Storm*, *in* LOCAL PUBLIC SERVICES IN TIMES OF AUSTERITY ACROSS MEDITERRANEAN EUROPE 102–03 (Andrea Lippi & Theodore Tsekos eds., 2019).

346. *Id.* at 103.

347. *Id.* at 100.

It is against this background that in 2015 Barcelona — the capital of Catalonia and the second-largest city in the country — elected a mayor with a radically progressive agenda centered around the principle of data sovereignty. Ada Colau ran her first election campaign with slogans on the re-municipalization of water and energy, social housing, and promises about turning Barcelona into a commons-based digital city built from the bottom-up.[348] The Mayor's Committee on Digital Innovation came up with a Digital Plan, putting emphasis on data ownership by the city, open-source code, and the publication of a technology procurement handbook that specifies contractual clauses mandating ethical standards — fostering a culture of transparency that encourages whistleblowers against corruption and crowdsourcing of ideas for dealing with urban problems.[349] Francesca Bria, Barcelona's Chief Digital Officer, has been called "the Robin Hood of data."[350] Bria is also heading a European-funded pilot project called DECODE (Decentralised Citizen-Owned Data Ecosystems).[351]

Although privacy and data protection are enshrined as separate human rights both on the level of European law[352] and in the Spanish Constitution,[353] they have not been central to Barcelona's vision of data sovereignty. The newly enacted European statutory framework that could potentially challenge the commodification of data — the GDPR — allows the processing of personal data only when under a

348. *See generally*, MOROZOV & BRIA, *supra* note 342.

349. Dowling, *supra* note 343, at 92.

350. Amy Lewin, *Barcelona's Robin Hood of Data: Francesca Bria*, SIFTED (Nov. 16, 2018), https://sifted.eu/articles/barcelonas-robin-hood-of-data-francesca-bria/ [https://perma.cc/HB86-Q9JZ]. The role of a Chief Digital Officer (CDO) is to "convert traditional 'analog' operations to digitized systems." *See* Kristin Musulin, *Why Cities Should Consider a Chief Digital Officer — Even If the C-Suite Is Crowded*, SMART CITIES DIVE (Aug. 23, 2018), https://www.smartcitiesdive.com/news/cities-should-consider-chief-digital-officer/530625/ [https://perma.cc/86AR-82YY]. This position is a novelty in the European context, however, so the responsibilities and general role of the Chief Digital Officer for Barcelona will be shaped primarily by the initiatives of its first holder, Francesca Bria.

351. DECODE, https://decodeproject.eu [https://perma.cc/PC79-DMHQ] (last visited Mar. 16, 2020).

352. *See generally* Charter of Fundamental Rights of the European Union, art. 7 & 8, 2012 O.J. (C 326/02); *see also* Case C-293/12 & Case C-594/12, Digital Rights Ireland Ltd. v. Minister for Communications, 2014 EUR-Lex CELEX LEXIS 238; Case C-131/12, Google Spain v. Agencia Española de Protección de Datos (AEPD), 2014 EUR-Lex CELEX LEXIS 317; Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, 2015 EUR-Lex CELEX LEXIS 650.

353. *See* Art. 18.1, 18.2, Constitución Española, B.O.E. n. 311, Dec. 29, 1978 (Spain).

legitimate basis. Furthermore, smart city business models that rely on consent as a default legal basis (such as LinkNYC or Quayside to some extent) may run into trouble given the high bar the GDPR places on establishing that consent is valid. [354] For example, most recently, the German Federal Cartel Office (FCO) — the country's antitrust watchdog — partnered with data protection authorities in other European countries to raise a legal challenge against Facebook for abuse of its dominant position. The FCO claimed that the all-embracing consent sought from Facebook users for the collection of their personal data through third-party websites and applications that are embedded in Facebook's interface (e.g., through its "Like," "Share," and "Login" buttons) did not meet the criteria for informed consent because users were not made aware of the extent of Facebook's data-sharing practices.[355] Moreover, in 2019 on data protection grounds alone, in France, Google was fined €50 million for breaching the GDPR requirements of "informed," "specific," and "unambiguous" consent in providing personalized advertisements.[356] At a recent conference, however, instead of referring to the GDPR, Bria emphasized the advent of blockchain technology for ensuring the privacy of Barcelona's residents who contribute their personal data to the city's data commons.[357] The statement chimes in with recent academic interpretations that place blockchain technology outside the scope of the GDPR.[358] Future reliance on blockchain for the rollout of smart city applications in Europe might thus mean that, in spite of its differentiating rhetoric, the "European" data stewardship model exemplified by Barcelona is, in fact, steadily converging with North American data practices in the urban context.

In many ways, Europe and North America "remain two worlds apart because of their very different understandings of the role that the public and the private sector should play in society."[359] Since

---

354. *See* Council Regulation, 2016/679, 2016 O.J. (L 119) (EU).

355. Adrian Künzler, Assistant Professor of Law, Univ. of Zurich, *Facebook Under Investigation*, Presentation at Yale Information Society Project (Sept. 3, 2019).

356. *The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against Google LLC*, CNIL (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc [https://perma.cc/62DZ-Q5MS].

357. Smart Cities and Strategy for Digital Sovereignty, Pictet Talk (Jan 20) (transcript on file with authors)

358. *See* Georgios Dimitropoulos, *The Law of Blockchain*, 94 WASH. L. REV. (forthcoming 2020).

359. Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUR. L.J. 119, 153 (2019).

Europeans place their trust in the public sector, a narrative centered around public data ownership seems intuitively appealing to European sensitivities, and in Spain, it was also embedded into the discourse of local anti-austerity opposition. However, in June 2019, Barcelona's Mayor Colau was very narrowly reelected, and it remains to be seen to what extent she can keep up with her bold electoral promises and go beyond the rhetoric of Barcelona as a "neoliberal city with a human face."[360] The idea of advancing public interest goals through procurement seems well-intentioned, although achieving purely public ownership of data generated through the use of devices supplied by private companies might prove difficult. Moreover, much like the synchronized action of state and city actors in the United States that has a better chance of achieving regulatory experimentation, the interlocking nature of Spain's "non-institutional" federalism makes coordination and close cooperation between the regional, provincial and municipal level essential. With independence and nationalist demands (mostly in rural Catalonia but increasingly spreading also in Barcelona)[361] clashing with the urban agenda of Colau, the actual outcome of the data sovereignty brand remains unsure.

CONCLUSION

Urbanization is here to stay, and so is the growing interest in the City. Jane Jacob's evergreen account of organic urban development remains relevant in the era of technology-driven datafication: "[C]ities may fairly be called natural economic generators of diversity and natural economic incubators of new enterprises[.]"[362] Privacy, broadly conceptualized, becomes an intrinsic part of a global city's identity as it intersects with the social capital that characterizes big cities — diversity and economic growth. This Article has sought to blend insights from the literature on global cities, American federalism, and localism studies, as well as on smart cities and privacy

360. *See* MOROZOV & BRIA, *supra* note 342, at 27–28.

361. In 2017, the Spanish Constitutional Court declared unconstitutional a referendum law on independence in Catalonia, spurring a crisis that continues to this day. *See* S.T.C., Oct. 17, 2017 (No. 4334) (Spain), https://www.tribunalconstitucional.es/ResolucionesTraducidas/Ley%20referendum%20ENGLISH.pdf [https://perma.cc/DB3S-TJVY]; *see also* David Gardner, *Autonomy Under Fire*, FIN. TIMES (Aug. 16, 2012), https://www.ft.com/content/00d27e14-e63a-11e1-ac5f-00144feab49a [https://perma.cc/HP7Y-8ERJ] (detailing Catalonia's demands for fiscal autonomy in the wake of the central government's then austerity measures).

362. JACOBS, *supra* note 6, at 148.

scholarship to show that U.S. cosmopolitan urbanism intersects privacy activism with data stewardship.

First, cities use their legal arsenal to litigate under federal, state, or city law in order to protect the personal information of their city dwellers in a variety of contexts ranging from political participation to consumer protection. Regardless of whether such experiments turn out to be successful — and they sometimes may well be[363] — cities' privacy activism, likely amplified by the stance of their states, may serve as a trigger for bipartisan policy debates and a catalyst for enforcement. Second, regarding technology's courtship with the city, privacy may be respected to a certain degree by local agencies, but privacy concerns increasingly give way to open data practices worldwide. Privacy is also not a priority in emerging new business models that monetize data and are facilitated through contract law. But big cities can and should leverage their existing powers to push hard for privacy-by-design in public procurement projects that may jumpstart the market in privacy-preserving "smart" systems. Yet what we observe across the board in large, cosmopolitan North American cities is a tendency toward data stewardship with a wide spectrum of approaches.

As data stewards, cities sometimes abdicate public power and control over public spaces, behaving more like a commercial actor. Toronto's Quayside project is a harbinger of what we might be seeing more often, albeit to a varying degree, across U.S. cities and elsewhere. Surely the very nature of public spaces — open and accessible to all, without a fee, without government restriction on speech and assembly other than reasonable time, place, manner restrictions, available for community and not privately owned — seems to dictate that public authorities should oversee public spaces. As we have seen, however, instead of relying on their police powers as regulators of local-level broadband, housing, and transportation services, some city governments either negotiate data-sharing agreements that may bring them direct revenues or try to deal with street-level problems through collecting ever more data. Privacy issues in such cases need to be treated with caution and, in any case,

---

363. In 2004, San Francisco brought claims under the California Constitution's Equal Protection Clause, raising state constitutional liberty and privacy protections to challenge statues limiting same-sex marriage. *See In re* Marriage Cases, 49 Cal. Rptr. 3d 675 (Cal. Dist. Ct. App. 2006). Later, the City intervened in the landmark case of *Perry v. Schwarzenegger*, asserting Due Process and Fourteenth Amendment protections under the federal Constitution. 704 F. Supp. 2d 921 (N.D. Cal. 2010). These efforts ultimately brought marriage equality to California, and with time, to the rest of the country. *See* Obergefell v. Hodges, 135 S. Ct. 2584 (2015).

with an eye toward greater proportionality. On the one hand, regulation through data cannot be left unchecked against the Constitution. On the other, it would be unwise to see the Fourth Amendment take a *Lochner*-like turn much like the First Amendment arguably has done.[364] In Europe, conversely, a different cultural understanding of the role of the public over the private sector seems to be the defining factor for the relationship between cities and technology firms. To some extent, the robust privacy framework enacted at a higher level of government (otherwise present in Canada as well), but mostly the entrenched conviction of preference for public ownership over public spaces, drives rhetoric on data sovereignty spearheaded by Barcelona. However, since technology firms can gain control over a public infrastructure not only through procurement but also over the duration of projects, it remains to be seen whether the promise of Barcelona for a publicly structured smart city will remain merely rhetorical.

Finally, consistent with the ideal of local autonomy and assuming cities can exceed a certain constitutionally protected threshold of privacy interests, cities may choose where to locate themselves on the sliding scale between privacy activism and data stewardship. Will we see citizens instead of businesses "vote with their feet,"[365] choosing to live in cities with less privacy but more autonomous cars and security cameras? Or will the trend of local politicking and the predominance of Voice over Exit[366] signal that more frequent local mobilization can change policies, as with San Franciscans, which recently banned the use of facial recognition by the local police force in their city,[367] or what may soon occur in Toronto? Changes might be underway.

---

364. *See* Robert Post & Amanda Shanor, *Adam Smith's First Amendment*, 128 HARV. L. REV. FORUM 165, 166–67 (2015).

365. *See* Tiebout, *supra* note 40, at 419–20.

366. *See generally* Schragger, *supra* note 28. The reference is to the classic work in federalism debates: ALBERT HIRSCHMAN, EXIT, VOICE AND LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES (1972) (explaining how "Voice" can be understood as the effort of the community to share concerns and fight to shape policies on the local level whereas "Exit" signifies a decision to leave).

367. Kate Conger et al., *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/LR2P-PK2M].