"WE KNOW NOT WHERE WE GO": PROTECTING DIGITAL PRIVACY IN NEW YORK CITY'S MUNICIPAL WI-FI NETWORK

Eric Hornbeck[*]

---

[*] J.D. Candidate, 2019, Fordham University School of Law; B.S., 2008, Ohio University. I am indebted to Professor Olivier Sylvian for his invaluable support and guidance throughout this process, the editors and staff of the *Fordham Urban Law Journal* for their thoughtful edits and assistance, and my friends and family for their endless encouragement.

INTRODUCTION

In 2014, New York City launched its ambitious LinkNYC public-private partnership to replace the city's public payphones with citywide internet service. The city granted a new franchise agreement to the private companies behind LinkNYC, which would then install thousands of sidewalk kiosks to bathe the city in free high-speed wireless internet ("Wi-Fi"). The program would allow the city to accomplish two goals: bridge the digital divide and make New York a more modern "smart city." In exchange, LinkNYC's backers would receive lucrative advertising revenue.

But LinkNYC also had a potentially sinister side: the specter of a mass surveillance network of cameras and sensors for law enforcement to follow New Yorkers wherever they went. A public outcry erupted. In response, LinkNYC changed its privacy policy to curtail the amount of information the kiosks could collect. With these changes in place, the network's deployment has continued unabated, even as some concerns still linger about what data, exactly, the kiosks collect, with whom the data is shared, and how the data is used.

The changing privacy policy showed both the promise and the limits of relying on voluntary privacy policies to protect New Yorkers from mass surveillance. The privacy policy changed in reaction to public opinion before anyone could attempt to look to the courts for clarity on the kiosks' data collection. The courts, however, are not necessarily able to provide clear guidance as they grapple with ever-changing new technology. Indeed, the kiosks themselves combine several types of data collection that are each subject to different lines of Fourth Amendment cases, including real-time location tracking, historical location data, and (potentially) facial recognition technology.

New York City, however, does not need to wait for the courts to find a way through the judicial morass and respond to New Yorkers' privacy concerns. The city can use the power it wields over digital service providers through procurement and franchise decisions to enhance New Yorkers' digital privacy and curtail the specter of mass surveillance systems. As city officials express growing concern about

both privacy and closing the digital divide, the LinkNYC experience shows how they can better achieve those goals by requiring that franchisees like LinkNYC reveal more about what data privacy New Yorkers are sacrificing in exchange for the benefits of ubiquitous Wi-Fi and other smart city initiatives.

Part I of this Note explores the digital divide, the smart cities movement, how the LinkNYC kiosks fit in both concepts, and the changes that have occurred to the LinkNYC privacy policy. Part II discusses the Fourth Amendment applications to the new location-tracking technologies that make up, or could make up, the LinkNYC kiosks, including real-time location tracking, historical location tracking, and facial recognition technology. Part III proposes that the city take the changes it made to the LinkNYC privacy policy even further: require vendors to be more transparent about the data collected by smart city initiatives like LinkNYC and face consequences if promises are broken. Such an approach will better-inform New Yorkers about the data collected about them, will allow for a clearer judicial response if that collection goes too far, and is a practice that technology companies themselves have already adopted.

I. LINKNYC: NARROWING THE DIGITAL DIVIDE WHILE WIDENING DIGITAL SURVEILLANCE CONCERNS

New York City launched LinkNYC to do two things simultaneously: make the city more equitable by providing internet access to more New Yorkers and "smarter" with innovative technology polices. But the initial roll out of the kiosks' privacy policy revealed that the New Yorkers most in need of greater internet access could be paying for it with citywide surveillance of their movements. The subsequent changes to the privacy policy revealed, however, that it may be possible to make the city smarter without sacrificing New Yorkers' privacy.

A. Closing New York City's Digital Divide as Mobile Broadband Usage Increases

The "digital divide" refers to "the economic, educational, and social inequalities between those who have computers and online access and those who do not."[1] The divide can be one of access to

---

1. *Digital Divide*, MERRIAM WEBSTER, https://www.merriam-webster.com/dictionary/digital%20divide [https://perma.cc/WYJ5-QEDE]; *see* ORG. FOR ECON. CO-OPERATION & DEV., UNDERSTANDING THE DIGITAL DIVIDE 5 (2001), https://www.oecd.org/sti/1888451.pdf [https://perma.cc/23GH-RMMT]; *see also*

technology, people's comfort with new technology,[2] or socioeconomic factors that affect whether people will have access to and use modern technology such as computers, smartphones, and the internet.[3] Nationwide, nearly all young, affluent, and educated people have internet access.[4] But people who are older, less educated, and less affluent are less likely to use computers and less likely to have access to the internet.[5]

The digital divide is not just about technology and internet access; the quality and speed of the internet access that is available also play a role in the divide.[6] Internet users increasingly use services that consume more data and require more bandwidth, and yet there are fewer high-bandwidth providers than there are low-bandwidth providers.[7] Such fast, high-bandwidth internet is known as "broadband."[8] Increasingly, the digital divide is discussed not just as the gap between those who have internet access and those who do not, but also as the gap between those who have access to broadband and those who do not.[9] How fast an internet connection must be to

---

OFFICE OF THE N.Y.C. COMPTROLLER, INTERNET INEQUALITY: BROADBAND ACCESS IN NYC 1 (2015) [hereinafter 2015 COMPTROLLER REPORT], http://comptroller.nyc.gov/wp-content/uploads/documents/Internet_Inequality_UPDATE_September_2015.pdf [https://perma.cc/L4R3-M6B8].

2. JOHN B. HORRIGAN, PEW RESEARCH CTR., DIGITAL READINESS GAPS 2 (2016), http://assets.pewresearch.org/wp-content/uploads/sites/14/2016/09/PI_2016.09.20_Digital-Readiness-Gaps_FINAL.pdf [https://perma.cc/L9B9-W6LV].

3. ANDREW PERRIN & MAEVE DUGGAN, PEW RESEARCH CTR., AMERICANS' INTERNET ACCESS: 2000–2015, at 6 (2015), http://www.pewinternet.org/files/2015/06/2015-06-26_internet-usage-across-demographics-discover_FINAL.pdf [https://perma.cc/CL2Q-6UFM].

4. HORRIGAN, *supra* note 2, at 11; *Internet/Broadband Fact Sheet*, PEW RESEARCH CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/internet-broadband/ [https://perma.cc/2BLB-89Q5].

5. HORRIGAN, *supra* note 2, at 13.

6. COUNCIL OF ECON. ADVISERS ISSUE BRIEF, MAPPING THE DIGITAL DIVIDE 6 (2015), https://obamawhitehouse.archives.gov/sites/default/files/wh_digital_divide_issue_brief.pdf [https://perma.cc/66PL-AQPS].

7. DAVID N. BEEDE, U.S. DEP'T OF COMMERCE, COMPETITION AMONG U.S. BROADBAND SERVICE PROVIDERS, OCE ISSUE BRIEF # 01-14, at 2 (2014), http://esa.doc.gov/sites/default/files/competition-among-us-broadband-service-providers.pdf [https://perma.cc/YLS5-WQ6T].

8. *Getting Broadband*, FED. COMM. COMM'N, https://www.fcc.gov/consumers/guides/getting-broadband [https://perma.cc/SAG9-HHZC].

9. *See* LENNARD G. KRUGER & ANGELE A. GILROY, CONG. RESEARCH SERV., RL30719, BROADBAND INTERNET ACCESS AND THE DIGITAL DIVIDE: FEDERAL ASSISTANCE PROGRAMS 1 (2016), https://fas.org/sgp/crs/misc/RL30719.pdf [https://perma.cc/9JJA-HUG7]; *see also* KATHERINE BATES ET AL., ICF INT'L, CLOSING THE DIGITAL DIVIDE: PROMOTING BROADBAND ADOPTION AMONG UNDERSERVED POPULATIONS 1 (2012), http://www.nlc.org/sites/default/files/Closing_Digital_Divide_Promoting_Broadband_Adoption_Underserved_Populations.pdf

qualify as broadband varies, but the Federal Communications Commission ("FCC") has set a benchmark of 25 megabits per second ("Mbps") for downloads and 3 Mbps for uploads for fixed broadband services.[10] The FCC has not set a benchmark for how fast a connection has to be on mobile devices like smartphones to qualify as broadband.[11] In New York State, a grant program designed to increase broadband deployment throughout the state has set "a goal of 100 Mbps download speeds, with 25 Mbps acceptable in the most remote and rural areas."[12]

Efforts to increase broadband usage are slowed largely by two cost-based factors: broadband availability and broadband adoption.[13] First, broadband providers are reluctant to invest in broadband infrastructure in less-populated areas where their return on investment is lower because they must install more equipment to connect fewer people than in densely-populated areas.[14] This presence, or not, of broadband service to users in a particular area is

---

[https://perma.cc/M3CB-K3PZ]; James E. Prieger, *The Broadband Digital Divide and the Economic Benefits of Mobile Broadband for Rural Areas*, 37 TELECOMMS. POL'Y 483, 483 (2013); COUNCIL OF ECON. ADVISERS, *supra* note 6, at 6.

10. FED. COMMC'NS COMM'N, FCC 17-109, THIRTEENTH SECTION 706 REPORT NOTICE OF INQUIRY 5 (2017) https://ecfsapi.fcc.gov/file/0808160504329/FCC-17-109A1.pdf [https://perma.cc/BQ94-82KV].

11. *Id.* at 7.

12. Press Release, Governor Andrew M. Cuomo, Governor Cuomo Launches Third Round of New NY Broadband Program (Mar. 30, 2017), https://www.governor.ny.gov/news/governor-cuomo-launches-third-round-new-ny-broadband-program [https://perma.cc/G7UP-YNNK]. Prior to the launch of the program in 2017, the State had set a minimum speed of 6 Mbps download and 1.5 Mbps upload. Press Release, Governor Andrew M. Cuomo, 2015 Opportunity Agenda: Restoring Economic Opportunity (Jan. 16, 2015), https://www.governor.ny.gov/news/2015-opportunity-agenda-restoring-economic-opportunity-1 [https://perma.cc/3Y6T-X6X2].

13. KRUGER & GILROY, *supra* note 9, at 5; FED. COMMC'NS COMM'N, FCC 16-6, 2016 BROADBAND PROGRESS REPORT 44–45 (2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-6A1.pdf [https://perma.cc/KY9M-RCWH]. *But see* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-473, BROADBAND: INTENDED OUTCOMES AND EFFECTIVENESS OF EFFORTS TO ADDRESS ADOPTION BARRIERS ARE UNCLEAR 11–12 (2015), http://www.gao.gov/assets/680/670588.pdf [https://perma.cc/F8UX-REEB] (discussing other reasons people do not have or use broadband).

14. Mike Orcutt, *The Next President Will Inherit America's Embarrassing Digital Divide*, MIT TECH. REV. (Sept. 15, 2016), https://www.technologyreview.com/s/602393/the-next-president-will-inherit-americas-embarrassing-digital-divide/ [https://perma.cc/366J-3Z9L] ("Broadband providers get far more bang for their infrastructure buck by building in cities, where a new bit of fiber, say, will reach far more potential customers than it would out in the sticks.").

known as broadband availability.[15] Second, the high cost of internet plans makes people with limited income less likely to pay for access.[16] This is broadband adoption.[17] The cost of internet subscriptions for consumers is much higher in the United States than in other industrialized countries.[18] These dual costs of deploying infrastructure and of paying for use make the digital divide most persistent in poor rural and urban areas.[19] Even if broadband is available in a particular area, the costs to users can slow adoption of broadband in that area.[20] Those gaps can vary in different areas across the country.[21] In addition, the divide can be exacerbated by a lack of digital literacy, limited access to technology, and users' perception that broadband access would not be beneficial to them.[22]

But the digital divide is not a mere annoyance; its pernicious effects can include a lower likelihood of school enrollment in households that do not have access to a home computer,[23] difficulty in finding employment,[24] and lower economic growth and quality of life.[25] Even

---

15. KRUGER & GILROY, *supra* note 9, at 2 (noting that "[m]easurements of broadband availability depend on how broadband service is defined in terms of what download and upload speeds it offers[]").

16. JOHN B. HORRIGAN & MAEVE DUGGAN, PEW RESEARCH CTR., HOME BROADBAND 2015, at 15 (2015), http://www.pewinternet.org/files/2015/12/Broadband-adoption-full.pdf [https://perma.cc/7NWJ-8KF7].

17. KRUGER & GILROY, *supra* note 9, at 5.

18. Orcutt, *supra* note 14.

19. *See* David Talbot, *The Unacceptable Persistence of the Digital Divide*, MIT TECH. REV. (Dec. 16, 2016), https://www.technologyreview.com/s/603083/the-unacceptable-persistence-of-the-digital-divide/ [https://perma.cc/D86T-C7XG] ("[T]he United States lags far behind much of the industrialized world in available broadband speeds and affordability of fast services—a problem that is particularly acute in inner cities and rural areas.").

20. KRUGER & GILROY, *supra* note 9, at 5.

21. Mike Maciag, *Digital Divide Most Glaring in Low-Income Communities*, GOV'T TECH. (Sept. 7, 2017), http://www.govtech.com/computing/Where-the-Digital-Divide-Is-the-Worst.html [https://perma.cc/Y2QT-9LPY].

22. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 13, at 11–12; COUNCIL OF ECON. ADVISERS, ISSUE BRIEF, THE DIGITAL DIVIDE AND ECONOMIC BENEFITS OF BROADBAND ACCESS 9 (2016), https://obamawhitehouse.archives.gov/sites/default/files/page/files/20160308_broadband_cea_issue_brief.pdf [https://perma.cc/73TC-PTLB].

23. Robert W. Fairlie, *The Effects of Home Computers on School Enrollment*, 24 ECON. EDUC. REV. 533, 536–39 (Oct. 2005).

24. Golda Arthur, *Lack of Internet Access Makes Climb out of Poverty Harder*, AL JAZEERA AM. (Oct. 24, 2015), http://america.aljazeera.com/articles/2015/10/24/not-having-internet-access-at-home-hinders-education-employment.html [https://perma.cc/6FEA-EX4F].

25. WORLD ECON. FORUM, INTERNET FOR ALL: A FRAMEWORK FOR ACCELERATING INTERNET ACCESS AND ADOPTION 8 (2016), http://www3.weforum.org/docs/WEF_Internet_for_All_Framework_Accelerating_Inte

in urban environments such as Detroit, the digital divide between more and less affluent neighborhoods might also have stifled the city's growth by making it harder for unemployed people to find jobs.[26]

In New York City, the digital divide is deeper along socioeconomic and neighborhood lines—and is growing.[27] The higher cost of internet access in New York compared to other cities contributes to the digital divide.[28] In 2014, 16% of New York City households did not have computers.[29] According to 2016 U.S. Census Bureau figures, about 10.7% of households nationwide did not have a computer (which includes handheld computers like smartphones), and about 18.1% did not have a broadband subscription.[30] By 2016, in New York City, about 12% of households did not have computers and about 19.7% had no broadband subscription.[31] Even though those figures have improved, they hide big disparities among boroughs.[32] In Manhattan (New York County), about 9.4% of households did not have computers in 2016 and about 16.3% had no broadband

---

rnet_Access_Adoption_report_2016.pdf [https://perma.cc/3XFC-CE54]. *See generally* Brian Whitacre et al., *Broadband's Contribution to Economic Growth in Rural Areas: Moving Towards a Causal Relationship*, 38 TELECOMM. POL'Y 1011 (2014).

26. Cecilia Kang, *Unemployed Detroit Residents Are Trapped by a Digital Divide*, N.Y. TIMES (May 22, 2016), https://www.nytimes.com/2016/05/23/technology/unemployed-detroit-residents-are-trapped-by-a-digital-divide.html [https://nyti.ms/2jEuYPT].

27. 2015 COMPTROLLER REPORT, *supra* note 1, at 1 (comparing U.S. Census Bureau data from 2013 and 2014 reports).

28. OFFICE OF THE N.Y.C. COMPTROLLER, INTERNET INEQUALITY: BROADBAND ACCESS IN NYC 2–3 (Dec. 2014), https://comptroller.nyc.gov/wp-content/uploads/documents/Internet_Inequality.pdf [https://perma.cc/S5ST-K8QV].

29. 2015 COMPTROLLER REPORT, *supra* note 1, at 4.

30. U.S. CENSUS BUREAU, TYPES OF COMPUTERS AND INTERNET SUBSCRIPTIONS, S2801, 2016 AMERICAN COMMUNITY SURVEY 1-YEAR ESTIMATES (2017), https://factfinder.census.gov/bkmk/table/1.0/en/ACS/16_1YR/S2801 [https://perma.cc/Q62Q-5U3V]; *see also* CAMILLE RYAN & JAMIE M. LEWIS, U.S. CENSUS BUREAU, ACS-37, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2015, at 3–6 (2017), https://www.census.gov/content/dam/Census/library/publications/2017/acs/acs-37.pdf [https://perma.cc/GVW5-U65W] (analyzing 2015 data).

31. U.S. CENSUS BUREAU, TYPES OF COMPUTERS AND INTERNET SUBSCRIPTIONS, *supra* note 30 (data sorted for New York City).

32. *See* Press Release, N.Y.C. Public Advocate Letitia James & Council Member Ben Kallos, New York City Digital Divide Fact Sheet (Mar. 16, 2017), https://benkallos.com/sites/default/files/PressRelease_Spectrum_Internet_Assist_Fact_Sheet_20170316.pdf [https://perma.cc/ESG6-3RR9] (analyzing 2015 data); Jakob Winkler, *Mapping New York City's Digital Divide*, NEW SCH. (Spring 2017), https://gpia-gis.github.io/adv-spring2017/projects/mapping-new-york-city-s-digital-divide-/ [https://perma.cc/CK5C-YP7V] (displaying geographic differences in access to infrastructure necessary for broadband).

subscription.[33] But during the same period in the Bronx (Bronx County), about 14.8% of households did not have computers and about 26.2% had no broadband subscription.[34] From 2013 to 2014, data suggest that the percentage of households that lacked broadband actually increased in the South Bronx and Central and Eastern Brooklyn neighborhoods.[35] Other studies suggest that adoption of home broadband nationwide has plateaued in recent years.[36]

As home broadband adoption has stagnated, there has been an increase in those who use a smartphone to connect to the internet.[37] The Pew Research Center estimates that, nationwide, "smartphone-only" users increased from 8% in 2013 to 13% in 2015.[38] Younger, lower-income, and minority households are more likely to be smartphone-only.[39] Among those whose household income was less than $30,000 in 2016, 20% were smartphone-only users.[40]

Some researchers say that the increasing reliance on mobile devices could help close the digital divide.[41] The increasing use of mobile broadband has led the FCC, which has a statutory mandate to evaluate "whether advanced telecommunications capability is being deployed to all Americans in a reasonable and timely fashion,"[42] to consider changing how it measures that deployment to include mobile broadband.[43] But other researchers say that smartphone-only access

---

33. U.S. CENSUS BUREAU, TYPES OF COMPUTERS AND INTERNET SUBSCRIPTIONS, *supra* note 30 (data broken down by borough).

34. *Id.*

35. 2015 COMPTROLLER REPORT, *supra* note 1, at 2.

36. HORRIGAN & DUGGAN, *supra* note 16, at 2.

37. *Id.*

38. *Id.*

39. *Id* at 9–10.

40. *See* Monica Anderson, *Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption*, PEW RES. CTR. (Mar. 22, 2017), http://www.pewresearch.org/fact-tank/2017/03/22/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/ [https://perma.cc/P9QN-NZTL].

41. Jamie M. Lewis, *Handheld Device Ownership: Reducing the Digital Divide?* 2 (U.S. Census Bureau, Working Paper No. SEHSD 2017-04), https://census.gov/library/working-papers/2017/demo/SEHSD-WP2017-04.html [https://perma.cc/S2KA-MLBC].

42. 47 U.S.C. § 1302(b) (2012).

43. FED. COMMC'NS COMM'N, *supra* note 10, at 5. *But see id.* at 20 (concurring statement of Commissioner Mignon L. Clyburn) ("Consumers who are mobile only often find themselves in such a position, not by choice but because they cannot afford a fixed connection. Today, mobile and fixed broadband are complements, not substitutes.").

is not a complete salve for the digital divide.[44] Smartphone-only users face financial difficulties such as limits on the amount of data they can use, difficulty in finding and applying for jobs online, and little opportunity to develop digital skills necessary for jobs that require familiarity with computer use.[45] Smartphone-only students also face additional challenges if their schools require projects to be completed online that are difficult to do on a smartphone.[46]

A variety of methods to close the digital divide have been rolled out or suggested. Possibilities include beaming wireless signals from hot air balloons, tapping unused television signals to reach remote areas,[47] launching municipal broadband networks,[48] and transmitting Wi-Fi from cellular phone towers.[49] In 2015, New York State announced a $500 million infrastructure grant program to encourage broadband investments in rural areas of the state.[50] The State wants to make broadband more widely available in areas where wireline providers[51] only offer internet speeds of less than 100 Mbps.[52] The goal is to make broadband available in the entire state by the end of

---

44. *See generally* Monica Anderson & John B. Horrigan, *Smartphones Help Those Without Broadband Get Online, but Don't Necessarily Bridge the Digital Divide*, PEW RES. CTR. (Oct. 3, 2016), http://www.pewresearch.org/fact-tank/2016/10/03/smartphones-help-those-without-broadband-get-online-but-dont-necessarily-bridge-the-digital-divide/ [https://perma.cc/D8K2-AGHJ].

45. HORRIGAN & DUGGAN, *supra* note 16, at 3; *see also* Talbot, *supra* note 19 ("People without broadband are not necessarily entirely offline . . . some of them rely on smartphones. But because of small screens and data caps, phones are not an adequate substitute for home broadband.").

46. Talbot, *supra* note 19; Rick Karr, *New York City's Plan to Bridge the Digital Divide with WiFi*, THIRTEEN (June 11, 2014), http://www.thirteen.org/metrofocus/2014/06/new-york-citys-plan-to-bridge-the-digital-divide-with-wifi/ [https://perma.cc/B6PY-KUH2] ("[Y]ou're not going to see kids writing term papers on mobile devices, said [Christopher] Mitchell [the director of Community Broadband Networks Initiative in Minneapolis].").

47. Cecilia Kang, *To Close Digital Divide, Microsoft to Harness Unused Television Channels*, N.Y. TIMES (July 11, 2017), https://www.nytimes.com/2017/07/11/technology/to-close-digital-divide-microsoft-to-harness-unused-television-channels.html [https://nyti.ms/2v65FIO].

48. Olivier Sylvain, *Broadband Localism*, 73 OHIO ST. L.J. 795, 836–37 (2012).

49. David Sommerstein, *Mohawks Provide High Speed Internet to Lewis County, Clinton County Next*, N. COUNTRY PUB. RADIO (Mar. 20, 2017), https://www.northcountrypublicradio.org/news/story/33573/20170320/mohawks-provide-high-speed-internet-to-lewis-county-clinton-county-next [https://perma.cc/VQA4-8KDL].

50. Press Release, Governor Andrew M. Cuomo, *supra* note 12.

51. Wireline providers deliver broadband service through physical wires such as fiber, coaxial cables, or copper telephone lines. *See "What Is Broadband?"*, N.Y. STATE BROADBAND PROGRAM OFFICE, https://nysbroadband.ny.gov/broadband-overview [https://perma.cc/8VYT-27P7].

52. Press Release, Governor Andrew M. Cuomo, *supra* note 12.

2018.[53] The plan requires winners of the grants to make some subscriptions available for less than $60 per month.[54] But critics say this price is not affordable enough to address the often prohibitively high cost of internet access for users even in places where it is available.[55]

In New York City, there are a variety of efforts to increase access to broadband and narrow the digital divide.[56] Former Mayor Michael Bloomberg spearheaded Wi-Fi initiatives,[57] and Mayor Bill de Blasio's administration has also touted its efforts to close the digital divide.[58] For example, the New York Public Housing Authority has "digital vans" with computer workstations and instructors that travel to public housing projects.[59] Some of the city's parks have free Wi-Fi provided by AT&T.[60] The Harlem neighborhood in Manhattan is home to a ninety-five-square-block Wi-Fi zone the city launched with

---

53. *See* Joseph Spector, *NY Plans Broadband Expansion*, POUGHKEEPSIE J. (Aug. 3, 2016), http://www.app.com/story/news/local/new-york/2016/08/03/ny-plans-broadband-expansion/88008550/ [https://perma.cc/FJV3-C2BC].

54. JEFFREY NORDHAUS, N.Y. STATE BROADBAND PROGRAM OFFICE, NEW NY BROADBAND PROGRAM PHASE 3 BIDDERS CONFERENCE 14, 29 (2017), https://nysbroadband.ny.gov/sites/default/files/finall_introducing_phase_3.pdf [https://perma.cc/8CNF-YQUZ]. These plans can be slower; the minimum requirement is 25 Mbps for downloads and 4 Mbps for uploads. *Id.*

55. *See* Michael Reilly, *Could New York's Plan to Erase Its Digital Divide Work for America?*, MIT TECH. REV. (Mar. 21, 2017), https://www.technologyreview.com/s/603939/could-new-yorks-plan-to-erase-its-digital-divide-work-for-america/ [https://perma.cc/Q9VR-AFFH]; *see also* Susan Crawford, *New York's Dream of a High Speed Internet Empire*, WIRED (June 4, 2015), https://www.wired.com/2015/06/new-yorks-dream-of-a-high-speed-internet-empire/ [https://perma.cc/26JR-GKQ3] ("Affordability is a major barrier in New York State, as it is across the country.").

56. *Broadband Access*, N.Y.C. DEP'T OF INFO. TECH. & TELECOMMS., https://www1.nyc.gov/site/doitt/initiatives/broadband-access.page [https://perma.cc/U2TD-5PES].

57. Tessa Stuart, *Free Wi-Fi Coming to Brownsville, Harlem, the Bronx, and Housing Projects in Brooklyn*, VILLAGE VOICE (Oct. 1, 2013), https://www.villagevoice.com/2013/10/01/free-wi-fi-coming-to-brownsville-harlem-the-bronx-and-housing-projects-in-brooklyn/ [https://perma.cc/8ENF-VJDZ].

58. Maya Wiley, *Broadband City: How New York Is Bridging Its Digital Divide*, THE NATION (Jan. 8, 2016), https://www.thenation.com/article/broadband-city-how-new-york-is-bridging-its-digital-divide/ [https://perma.cc/N3U4-QYZD]; Press Release, City of New York, De Blasio Administration Escalates Efforts to Close Digital Divide and Drive Down Cost of Internet for New Yorkers (Apr. 9, 2015), http://www1.nyc.gov/office-of-the-mayor/news/226-15/de-blasio-administration-escalates-efforts-close-digital-divide-drive-down-cost-internet [https://perma.cc/CSS8-Q4N9].

59. *Digital Vans*, N.Y.C. HOUS. AUTH., http://www1.nyc.gov/site/nycha/residents/digital-van.page [https://perma.cc/W53X-SGRW].

60. *Wi-Fi in Parks*, N.Y.C. PARKS, https://www.nycgovparks.org/facilities/wifi [https://perma.cc/KH38-R4TC].

the help of a private foundation and a technology company.[61] Other city-backed programs aim to bring Wi-Fi and broadband internet directly into housing projects.[62] Some organizations, such as the New York Public Library and the Brooklyn Public Library, have also launched their own initiatives, lending out free Wi-Fi hotspots to public school children who do not have internet access at home.[63]

B. The Smart Cities Movement and Digital Inequality

On the flipside of the urban digital divide is the "smart cities" movement. A "smart city" is loosely defined as one that uses technology and the internet as tools to solve all sorts of urban ills.[64] For example, smart city projects include harnessing the "Internet of Things" to make a city run better,[65] such as using cameras and sensors

---

61. Press Release, City of New York, Mayor Bloomberg Announces Country's Largest Continuous Free Public WiFi Network (Dec. 10, 2013), http://www1.nyc.gov/office-of-the-mayor/news/394-13/mayor-bloomberg-country-s-largest-continuous-free-public-wifi-network [https://perma.cc/H5SU-NH7G]; *see also Free Harlem WiFi*, MAYOR'S FUND TO ADVANCE N.Y.C., https://www1.nyc.gov/site/fund/initiatives/free-harlem-wifi.page [https://perma.cc/C32N-R8RU].

62. 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/7SQD-M8A6]; Press Release, City of New York, Mayor de Blasio, HUD Secretary Castro, and T-Mobile Announce 5,000 Families in Bronx Public Housing to Receive Free Tablets and Mobile Internet Service (Dec. 16, 2016), http://www1.nyc.gov/office-of-the-mayor/news/956-16/mayor-de-blasio-hud-secretary-castro-t-mobile-5-000-families-bronx-public-housing#/0 [https://perma.cc/UFS9-RNPN]; Press Release, City of New York, Mayor de Blasio Announces up to $10 Million Investment in Free Broadband Service for Five NYCHA Developments (July 16, 2015), http://www1.nyc.gov/office-of-the-mayor/news/491-15/mayor-de-blasio-up-10-million-investment-free-broadband-service-five-nycha#/0 [https://perma.cc/4VTQ-8S35].

63. Keldy Oritz & Ginger Adams Otis, *New York Public Library Expands Wi-Fi Lending*, N.Y. DAILY NEWS (Apr. 23, 2015), http://www.nydailynews.com/new-york/new-york-public-library-expands-wi-fi-lending-article-1.2196477 [https://perma.cc/NWQ7-63LF]; *Library HotSpot Loan Program*, BROOKLYN PUB. LIBR., https://www.bklynlibrary.org/hotspot [https://perma.cc/YC5B-T9XK]; *Library HotSpot*, N.Y. PUB. LIBR., http://hotspot.nypl.org/ [https://perma.cc/S4JL-C89X].

64. Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581, 1583–84 (2014). *But see, e.g.*, Albert Meijer & Manuel Pedro Rodrígues Bolívar, *Governing the Smart City: A Review of the Literature on Smart Urban Governance*, 82 INT'L REV. ADMIN. SCI. 392, 394 (2016) (discussing the "fuzzy concept" of the "smart city" and the various ways it can be defined); Vito Albino, Umberto Berardi & Rosa Maria Dangelico, *Smart Cities: Definitions, Dimensions, and Performance*, 22 J. URB. TECH. 1, 2, 4 (2013) (same).

65. Devices that connect objects to the internet or other networks are broadly referred to as the "Internet of Things" ("IoT"). U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-570, INTERNET OF THINGS: COMMUNITIES DEPLOY PROJECTS BY COMBINING FEDERAL SUPPORT WITH OTHER FUNDS AND EXPERTISE 4–5 (2017),

on street lights to monitor and adjust red lights to ease traffic flows,[66] and installing "smart grids" that can use similar devices deployed throughout a given area to improve the efficiency and resiliency of the electric grid.[67] New York City has been particularly aggressive in converting itself into a smart city that uses sensors and other technology to better manage and understand urban life, including 817,000 wireless water meters to monitor water use and sensors on 700 solar-powered trash cans that can alert sanitation workers when the cans are full.[68]

"Open data" is another common smart city initiative.[69] Typically, open data refers to websites where a government posts some or all of the vast troves of data that it collects in a machine-readable format.[70] The goal of open data is to promote government transparency and to allow others to deploy government data in useful ways.[71] Initiatives like the Freedom of Information Act and some of the open data policies of the Obama administration tend to focus on transparency, while municipal open data initiatives tend to focus on using the data to improve city services.[72] For example, providing campaign finance information is meant to promote public accountability and transparency, while making bus schedule data available and machine-

---

https://www.gao.gov/assets/690/686106.pdf [https://perma.cc/ZKX3-B5BF]. In a community setting, the IoT is largely synonymous with the "smart city" concept and also "aim[s] to generally improve the livability, management, or service delivery of that community." *Id.* at 5.

66. *See* Press Release, City & Cty. of Denver, Denver Secures $6 Million Grant to Advance Smart Transportation Initiatives (Oct. 7, 2016), https://www.denvergov.org/content/denvergov/en/transportation-mobility/smart-city.html [https://perma.cc/ETU5-TRU6].

67. *See* Rosaldo J. F. Rossetti, *Smart Grids*, 1 READINGS ON SMART CITIES, no. 10, Nov. 2015, https://smartcities.ieee.org/articles-publications/ieee-xplore-readings-on-smart-cities/november-2015.html [https://perma.cc/Q7U2-TL3D].

68. Robert Lee Hotz, *As World Crowds In, Cities Become Digital Laboratories*, WALL ST. J. (Dec. 11, 2015, 11:10AM), https://www.wsj.com/articles/as-world-crowds-in-cities-become-digital-laboratories-1449850244 [https://perma.cc/R7R4-3RCP] ("Hundreds of aging cities have embraced digital technology, but few are moving as quickly as New York to link municipal computer networks, develop novel applications, make digital data public or install so many thousands of sensors to monitor urban life—from water quality, traffic and power use, to the sound of gunfire.").

69. *See generally* Rosaldo J. F. Rossetti, *Smartly Opening Up City Data*, 1 READINGS ON SMART CITIES, no. 4, Apr./May 2015, https://smartcities.ieee.org/articles-publications/ieee-xplore-readings-on-smart-cities/april-2015.html [https://perma.cc/DHW3-CD7D].

70. Harlan Yu & David G. Robinson, *The New Ambiguity of "Open Government,"* 59 UCLA L. REV. DISC. 178, 191–92 (2012).

71. *Id.* at 192.

72. *Id.* at 196–99.

readable is meant to allow developers to launch apps and other tools that enhance bus riders' experiences.[73] Of course, transparency is not a solution by itself.[74] Open data can be misused or expose people to other risks, such as using data to target vulnerable communities, using someone's data without their consent, compromising individual privacy, re-engineering ostensibly anonymous data to identify specific individuals, inadvertently disclosing data, and breaching or compromising data security, among others.[75]

New York City's open data disclosures are some of the most extensive in the world.[76] New York City has published some public data online since at least 1993.[77] In 2012, the city's open data law came into force, requiring all city agencies to publish public data they collect on a new web portal in a machine-readable format.[78] The law notes that the open data portal would make the city "more transparent, effective and accountable to the public."[79] About 1700 different public data sets are now available through the portal.[80] The

---

73. *Id.* at 207.

74. *See generally* Tiago Peixoto, *The Uncertain Relationship Between Open Data and Accountability: A Response to Yu and Robinson's* The New Ambiguity of "Open Government," 60 UCLA L. REV. DISC. 200 (2013); Jennifer Shkabatur, *Transparency With(out) Accountability: Open Government in the United States*, 31 YALE L. & POL'Y REV. 79 (2012). *Cf.* Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 658–60 (2017) (arguing that disclosure of technology companies' algorithms does not by itself solve the problem of the possibility of those algorithms making biased decisions).

75. *See generally* Emmie Tran & Ginny Scholtes, *Open Data Literature Review*, BERKELEY CTR. L. & TECH./BERKELEY TECH. L.J. SYMPOSIUM: OPEN DATA: ADDRESSING PRIVACY, SECURITY, & CIVIL RIGHTS CHALLENGES (2015), https://www.law.berkeley.edu/wp-content/uploads/2015/04/Final_OpenDataLit Review_2015-04-14_1.1.pdf [https://perma.cc/VWQ4-5ZY3] (surveying articles on open data as background materials for those attending annual symposium).

76. Hotz, *supra* note 68 ("New York has made more of its own data public than any other city in the world.").

77. *See* Craig Campbell, *New York City Open Data: A Brief History*, GOV'T TECH. (Mar. 10, 2017), http://www.govtech.com/data/New-York-City-Open-Data-A-Brief-History.html [https://perma.cc/9F67-AVH2].

78. *See* 2012 N.Y.C. Local Law No. 11 (codified as amended at N.Y.C. ADMIN. CODE §§ 23-501 to 23-503 (2018)). Not all data can be released. *See, e.g.*, CITY OF NEW YORK, DEP'T OF INFO. TECH. & TELECOMM., OPEN DATA FOR ALL 2017 PROGRESS REPORT 46 (2017), https://opendata.cityofnewyork.us/wp-content/uploads/2017/07/OD4A-report_2017-1.pdf [https://perma.cc/GP46-N6GZ] (noting that legal counsel has advices that live birth data cannot be released through the portal).

79. 2012 N.Y.C. Local Law No. 11 (codified as amended at N.Y.C. ADMIN. CODE §§ 23-501 to 23-503 (2018)).

80. *See* OPEN DATA FOR ALL 2017 PROGRESS REPORT, *supra* note 78, at 6. "'Public data set' means a comprehensive collection of interrelated data that is available for inspection by the public in accordance with any provision of law and is maintained on a computer system by, or on behalf of, an agency," subject to certain

portal's data sets show such varied information as neighborhood crime statistics, the species of every tree along New York City sidewalks,[81] and even rat sightings based on 311 calls.[82]

Smart city initiatives have also been seen as ways to address public safety.[83] The New York City Police Department ("NYPD") has touted various initiatives to use technology to fight crime.[84] For example, the NYPD releases crime statistics online in a variety of formats.[85] In addition, the city has deployed special sensors that detect gunshots and help deploy police to the scene quickly.[86]

But smart city projects also raise security and privacy concerns.[87] Such networks can be hard to secure from cyberattacks.[88] Vast

---

exceptions. 2012 N.Y.C. Local Law No. 11 § 2 (codified as amended at N.Y.C. ADMIN. CODE §§ 23-501 to 23-503 (2018)).

81. *See* CITY OF NEW YORK, DEP'T OF INFO. TECH. & TELECOMM., OPEN DATA FOR ALL: NYC OPEN DATA PLAN 2015, at 14 (2015), http://www1.nyc.gov/assets/home/downloads/pdf/reports/2015/NYC-Open-Data-Plan-2015.pdf [https://perma.cc/27B7-X3TT]; Achal Bassamboo & Tom Schenk, *How Open Data Is Changing Chicago*, KELLOGGINSIGHT (June 20, 2016), https://insight.kellogg.northwestern.edu/article/ow-open-data-is-changing-chicago [https://perma.cc/DQ2Z-2V9G].

82. *See* Emily Badger, *The Best Open Data Releases of 2012*, CITYLAB (Dec. 19, 2012), https://www.citylab.com/life/2012/12/best-open-data-releases-2012/4200/ [https://perma.cc/WCN6-SY34]; *see also Rat Sightings*, NYC OPEN DATA, https://nycopendata.socrata.com/Social-Services/Rat-Sightings/3q43-55fe [https://perma.cc/TRD8-YEUX].

83. *See* Liz Enbysk, *Outsourcing the Bad Guys with Smart Technologies*, SMART CITIES COUNCIL (Feb. 12, 2014), http://smartcitiescouncil.com/article/outsmarting-bad-guys-smart-technologies [https://perma.cc/T7WB-79FM] (Smart Cities Council is an organization made up of companies that promote deployment of smart-city technologies).

84. *See* Press Release, N.Y.C. Police Dep't, NYPD Technology: Helping the Finest Keep NYC Safe (Feb. 20, 2017), http://nypdnews.com/2017/02/nypd-technology-helping-the-finest-keep-nyc-safe/ [https://perma.cc/76PK-NHKN].

85. *See* Graham Rayman, *NYPD Releases Internet Database that Gives Details About All Major New York City Crimes*, N.Y. DAILY NEWS (Dec. 30, 2015, 4:16 PM), http://www.nydailynews.com/new-york/nypd-releases-online-crime-database-public-article-1.2481185 [https://perma.cc/3ZAT-J77N].

86. *See* Tatiana Schlossberg, *New York Police Begin Using ShotSpotter System to Detect Gunshots*, N.Y. TIMES (Mar. 16, 2015), https://www.nytimes.com/2015/03/17/nyregion/shotspotter-detection-system-pinpoints-gunshot-locations-and-sends-data-to-the-police.html [https://nyti.ms/2mdl3m7]; Press Release, City of New York, Fact Sheet: Mayor de Blasio Releases Preliminary Budget for Fiscal Year 2017 (Jan. 21, 2016), http://www1.nyc.gov/office-of-the-mayor/news/077-16/fact-sheet-mayor-de-blasio-releases-preliminary-budget-fiscal-year-2017 [https://perma.cc/F7CY-T3CD].

87. *See, e.g.*, Finch & Tene, *supra* note 64, at 1605; Chris Mellor, *Smart Cities? Tell It Like It Is, They're Surveillance Cities*, THE REGISTER (Sept. 7, 2017), https://www.theregister.co.uk/2017/09/07/smart_cities_are_surveillance_cities/ [https://perma.cc/BKM4-HCNG].

88. *See generally* Brian Nussbaum, *Smart Cities—the Cyber Security and Privacy Implications of Ubiquitous Urban Computing*, STAN. L. SCH. CTR. FOR INTERNET &

municipal wireless networks are tempting targets for hackers.[89] Smart city projects can also be used as mass surveillance systems: for example, gunshot sensors may eavesdrop on nearby pedestrians' private conversations.[90] Privacy groups and others have also raised concerns regarding the vast amounts of data about law-abiding citizens that are collected and stored, perhaps indefinitely, by the NYPD,[91] the lack of transparency about software used in "predictive policing" programs,[92] and the ability of smart city technology to track an individual's movements and life.[93]

Perhaps one of the most controversial such programs is the NYPD's Domain Awareness System, which uses cameras and sensors, combined with data, to quickly identify threats.[94] As of 2015, the system consisted of 10,000 public and private security cameras, 1000 license plate readers, and 600 radiation and chemical sensors throughout Manhattan.[95] The city developed the system with Microsoft Corp. and shares the revenue when it is sold to other

---

SOC'Y: BLOG, (Feb. 9, 2016, 5:53 PM), http://cyberlaw.stanford.edu/blog/2016/02/smart-cities-%E2%80%93-cyber-security-and-privacy-implications-ubiquitous-urban-computing [https://perma.cc/9447-FGPK].

89. *See* Joanna Stern, *The Future of Public Wi-Fi: What to Do Before Using Free, Fast Hot Spots*, WALL ST. J. (Jan. 19, 2016, 2:43 PM) https://www.wsj.com/articles/the-future-of-public-wi-fi-what-to-do-before-using-free-fast-hot-spots-1453232580 [https://perma.cc/2JW4-NQJ7] ("I was feeling great about how much more secure my data would be [on the LinkNYC Wi-Fi network] until I spoke to Mark Wuergler, a security professional at Immunity Inc., who gets paid to find vulnerabilities in high-value networks. 'An attack is inevitable on New York City's system,' he says. 'It is too big of a trophy.'").

90. *See* Jay Stanley, *Shotspotter CEO Answers Questions on Gunshot Detectors in Cities*, ACLU: BLOG (May 5, 2015, 9:15 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/shotspotter-ceo-answers-questions-gunshot [https://perma.cc/B32D-K32A].

91. *See* N.Y. CIVIL LIBERTIES UNION, BEYOND "DELIBERATE INDIFFERENCE": AN NYPD FOR ALL NEW YORKERS 28 (2013), https://www.nyclu.org/sites/default/files/publications/nypd_report_final_0.pdf [https://perma.cc/4SGL-368F].

92. *See* Rachel Levinson-Waldman, *Testimony on Int. 1696, Relating to the Disclosure of Source Code by Agencies Engaged in Policing and Other Services*, BRENNAN CTR. FOR JUSTICE (Oct. 16, 2017), https://www.brennancenter.org/analysis/testimony-int-1696-relating-disclosure-source-code-agencies-engaged-policing-and-other# [https://perma.cc/8HL6-87AM].

93. *See* Steven Poole, *The Truth About Smart Cities: "In the End, They Will Destroy Democracy,"* THE GUARDIAN (Dec. 17, 2014), https://www.theguardian.com/cities/2014/dec/17/truth-smart-city-destroy-democracy-urban-thinkers-buzzphrase [https://perma.cc/9PE3-Y77J].

94. *See* Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 48–50 (2014); *see also* N.Y.C. POLICE DEP'T, THE POLICE COMMISSIONER'S REPORT 72 (2017), http://www1.nyc.gov/assets/nypd/downloads/pdf/publications/pc-report-2017.pdf [https://perma.cc/P5PU-NGRB].

95. Hotz, *supra* note 68.

cities.[96] To supporters of the system, the Domain Awareness System is a cost-effective way to combine technology and data to thwart terrorism.[97] To skeptics, it is a vast state-sponsored spy network that is now being expanded to cities beyond New York.[98]

Despite the concerns, government officials continue to advance such smart city initiatives. The federal government has funded some of these programs in more than seventy local communities.[99] The National Institute of Standards and Technology is also developing a framework to make smart city technologies standardized and interoperable.[100] States have pushed their own open data policies.[101] The U.S. Department of Transportation sponsored a contest to spur local smart city initiatives.[102] Local officials and industry representatives have touted their own smart city initiatives, especially those that expand internet access to underserved communities, as tools that cities can use to bridge the digital divide.[103] New York City

---

96. *Id.*

97. *See, e.g.*, Richard A. Posner, *Privacy Is Overrated*, N.Y. DAILY NEWS (Apr. 28, 2013, 4:19 AM), http://www.nydailynews.com/opinion/privacy-overrated-article-1.1328656 [https://perma.cc/5NA6-YTX2]; Office of the Mayor, *Mayor Bloomberg Discusses How City's New, State-of-the-Art Law Enforcement Technology and New York's Finest Keep New York the Safest Big City in the Nation in Weekly Radio Address*, CITY OF N.Y. (Aug. 12, 2012), http://www1.nyc.gov/office-of-the-mayor/news/295-12/mayor-bloomberg-how-city-s-new-state-of-the-art-law-enforcement-technology-new [https://perma.cc/A9B9-YVXF]; *Developing the NYPD's Information Technology*, N.Y.C. POLICE DEP'T, http://home.nyc.gov/html/nypd/html/home/POA/pdf/Technology.pdf [https://perma.cc/DVA8-NQFX].

98. *See, e.g.*, Nat Hentoff, *Tourists Beware of Being Databased in New York City*, CATO INST. (Aug. 15, 2012), https://www.cato.org/publications/commentary/tourists-beware-being-databased-new-york-city [https://perma.cc/WEC4-7PHV]; Martin Kaste, *In 'Domain Awareness,' Detractors See Another NSA*, NAT'L PUB. RADIO (Feb. 21, 2014, 4:00 PM), http://www.npr.org/sections/alltechconsidered/2014/02/21/280749781/in-domain-awareness-detractors-see-another-nsa [https://perma.cc/UTD8-HAC8].

99. Press Release, White House, Announcing Over $80 Million in New Federal Investment and a Doubling of Participating Communities in the White House Smart Cities Initiative (Sept. 26, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/09/26/fact-sheet-announcing-over-80-million-new-federal-investment-and [https://perma.cc/KWD8-DPSH].

100. *International Technical Working Group on IoT-Enabled Smart City Framework*, NAT'L INST. OF STANDARDS & TECH., https://pages.nist.gov/smartcitiesarchitecture/ [https://perma.cc/E4PU-GRZK].

101. Laura Drees & Daniel Castro, *State Open Data Policies and Portals*, CTR. FOR DATA INNOVATION (Aug. 18, 2014), https://www.datainnovation.org/2014/08/state-open-data-policies-and-portals/ [https://perma.cc/4W6Y-27X2].

102. *Smart City Challenge*, U.S. DEP'T OF TRANSP., https://www.transportation.gov/smartcity [https://perma.cc/VX96-GYMM].

103. *See* Juliet Van Wagenen, *Smart Cities Week 2017: How to Bridge the Digital Divide Amid a Smart City Revolution*, STATETECH (Oct. 9, 2017),

has said that closing the digital divide "is central to the City's strategy for technology and innovation."[104]

C. LinkNYC Privacy Policy Changed After Public Outcry

Of all the proposals in New York City to close the digital divide and make New York "smarter," perhaps no other is as ambitious in scope—and troublesome to privacy advocates—as transforming the city's once-ubiquitous payphones into a citywide Wi-Fi network.[105] As New Yorkers largely abandoned the payphones in favor of smart phones, payphone usage dropped dramatically, and many payphones were valuable solely for their advertising space.[106] In 2012, the city began exploring options to replace the payphones, which were operated by private companies that had received franchises from the city.[107] The city began adding Wi-Fi to some existing payphones,[108]

---

https://statetechmagazine.com/article/2017/10/smart-cities-week-2017-how-bridge-digital-divide-amid-smart-city-revolution [https://perma.cc/UM5B-NY6A]. *See generally* INT'L DATA CORP., THE ROLE OF PUBLIC WI-FI IN ENABLING SMART CITIES (2017), http://ruckus-www.s3.amazonaws.com/pdf/other/role-of-public-wifi.pdf [https://perma.cc/UV4M-BN2L] (white paper sponsored by wireless company advocating Wi-Fi to close the digital divide); Dan Hoffman, *Bridging the Digital Divide*, CIO REV. (Oct. 21, 2017), https://smartcity.cioreview.com/cxoinsight/bridging-the-digital-divide-nid-24259-cid-134.html [https://perma.cc/SU4K-HL5V] (city official discussing distribution of sensors that "detect hazardous environments" to close the digital divide); Shireen Santosham, *A Model for Closing the Digital Divide?*, GOVERNING (June 9, 2016), http://www.governing.com/blogs/bfc/col-san-jose-model-closing-digital-divide-terragraph.html [https://perma.cc/VQ9Y-FX49] (city official discussing Wi-Fi deployment to close the digital divide).

104. *Building a Smart + Equitable City*, N.Y.C. MAYOR'S OFFICE OF TECH. & INNOVATION, https://www1.nyc.gov/site/forward/innovations/smartnyc.page [https://perma.cc/Y7JR-T89H].

105. *See, e.g.*, Sam Gustin, *LinkNYC's New Free Network Is Blazing Fast. But at What Cost to Privacy?*, MOTHERBOARD (Feb. 19, 2016, 7:00 AM), https://motherboard.vice.com/en_us/article/jpgmvg/linknycs-new-free-network-is-blazing-fast-but-at-what-cost-to-privacy [https://perma.cc/7AC7-4U3U]; Sam Gustin, *Amid Privacy Concerns, NYC Approves Bid to Turn Payphones into Wifi Hotspots*, MOTHERBOARD (Nov. 18, 2014, 6:00 AM), https://motherboard.vice.com/en_us/article/8qxbg4/amid-privacy-concerns-nyc-approves-bid-to-turn-payphones-into-wifi-hotspots [https://perma.cc/5NF2-2CDU]; Kyle VanHemert, *NYC's New Pay Phones Will Provide Super-Fast Wi-Fi—and Super-Smart Ads*, WIRED (Nov. 19, 2014, 4:24 PM), https://www.wired.com/2014/11/new-york-linknyc-free-internet/ [https://perma.cc/S3RX-V2QV].

106. *See* N.Y.C. Council, Comm. Rep., Oversight Hearing on the Dep't of Info. Tech. and Telecomm. Request for Proposals Concerning NYC WiFi and Information Hubs 4 (June 18, 2014) [hereinafter June 2014 Hearing Report], http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=1807534&GUID=95B5AE9B-EF21-44CE-B11D-57853E84B12B&Options=&Search= [https://perma.cc/M3ST-SN5W].

107. *Id.*

and in 2013, it received more than 125 submissions for a payphone redesign competition.[109]

In May 2014, the city's Department of Information Technology and Telecommunications ("DoITT") put out a request for proposals ("RFP") to radically alter the city's payphones.[110] The RFP said the city would give to a single bidder a contract, known as a franchise agreement, to install a citywide network of hotspots where the payphones had once been.[111] Those structures would then provide free Wi-Fi to New Yorkers as they walked the city's streets.[112] The city also encouraged proposals that included environmental sensors, text messaging, and free phone calls.[113] In exchange, the winning bidder would receive advertising revenue from advertisements placed on the structures.[114] The winning bidder would receive a franchise from the city to place up to 10,000 of the structures on city sidewalks, replacing the 7300 payphones then installed there.[115] The city required that bidders guarantee that at least $17 million[116] of the

---

108. *See* Press Release, City of New York Department of Technology and Telecommunications, Citywide Chief Information & Innovation Officer Merchant, Chief Digital Officer Sterne, Council Member Brewer, Van Wagner Communications, and Titan Announce Free Wi-Fi Service Provided Through Payphone Kiosks (July 11, 2012), https://www1.nyc.gov/site/doitt/about/pr-120711.page [https://perma.cc/QY7J-7X6K].

109. *Reinvent Payphones Design Challenge*, NYC DIGITAL, https://web.archive.org/web/20140823203527/nyc.gov/html/digital/html/opengov/reinventpayphones.shtml [https://perma.cc/8Y3Y-NQAW]; *Pay Phones*, CITY OF N.Y. DEP'T OF TECH. & TELECOMM., https://www1.nyc.gov/site/doitt/residents/pay-phones.page [https://perma.cc/E7PU-6WV7].

110. *See* Press Release, City of New York, New York City Issues Request for Proposals to Build Citywide Wi-Fi Network and State-of-the-Art Information Hubs (May 1, 2014) [hereinafter Press Release, NYC Issues Request for Proposals], http://www1.nyc.gov/office-of-the-mayor/news/193-14/new-york-city-issues-request-proposals-build-citywide-wi-fi-network-state-of-the-art [https://perma.cc/DCT7-5P5H]; *see also* June 2014 Hearing Report, *supra* note 106, at 1.

111. Press Release, NYC Issues Request for Proposals, *supra* note 110.

112. *Id.*

113. *See Fact Sheet: Request for Proposals: NYC WiFi & Communication Hubs*, CITY OF NEW YORK (Apr. 30, 2014), https://www1.nyc.gov/assets/doitt/downloads/pdf/Public-Comm-Structures-RFP-Fact-Sheet-04-30-14.pdf [https://perma.cc/P9AM-MW96].

114. *See* Press Release, NYC Issues Request for Proposals, *supra* note 110.

115. CITY OF NEW YORK, DEP'T OF TECH. & TELECOMM., REQUEST FOR PROPOSALS FOR A PUBLIC COMMUNICATIONS STRUCTURES FRANCHISE 4 (2014) [hereinafter RFP], https://www1.nyc.gov/assets/doitt/downloads/pdf/DoITT-Public-Communication-Structure-RFP-4-30-14.pdf [https://perma.cc/3GUS-WQMY].

116. The figure represented about what the city was then receiving in advertising revenues from existing payphones. *See* Jennifer Peltz, *Can You Download Me Now? NY Payphones Become Wi-Fi Hot Spots*, ASSOCIATED PRESS (Jan. 1, 2016).

advertising revenue be funneled back to the city every year for the length of the franchise agreement.[117]

The RFP did not, however, say much about data privacy or security. The RFP did not require bidders to describe how they would secure user data privacy, but did request that the bidders describe "how, and for what purposes, the data contained within the system will be utilized[.]"[118] Digital data security concerns were not addressed by the RFP.[119] Concerns raised at a city council subcommittee's oversight hearing in May 2014 focused on the anticompetitive potential of awarding the franchise to a single bidder.[120]

At least sixty organizations—including Google, Time Warner, Cisco, the Metropolitan Transit Authority, and Verizon—expressed interest in the RFP.[121] At a May 2014 conference with the DoITT, potential bidders asked about data collection, using that data to generate revenue, and whether the Wi-Fi could be used for "data mining and push advertising"; the city said it would "consider" such proposals.[122]

Ultimately, seven bidders submitted proposals[123]: a division of media and entertainment company Clear Channel Outdoor, Inc.;[124]

---

117. RFP, *supra* note 115, at 19.

118. *Id.* at 11.

119. Security concerns related to the physical kiosk structure itself. *See id.* at 10.

120. *See* N.Y.C. Council, Transcript of the Minutes of the Subcomm. on Zoning and Franchises Jointly with Comm. on Tech. 5 (June 18, 2014), http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=1807534&GUID=95B5AE9B-EF21-44CE-B11D-57853E84B12B&Options=&Search= [https://perma.cc/G367-4LTT] (statement of Chairman Mark Weprin).

121. Sam Gustin, *Google May Turn 7,000 New York City Payphones into WiFi Hotspots*, MOTHERBOARD (July 22, 2014, 2:04 PM), https://motherboard.vice.com/en_us/article/3dkvqk/google-may-turn-7000-new-york-city-payphones-into-wifi-hotspots [https://perma.cc/5HDN-DPAC]; *see also* City of N.Y. Dep't of Info. Tech. & Telecomm., Public Communications Structures RFP - Pre-proposal Conference Q&A (May 12, 2014) [hereinafter RFP - Pre-proposal Conference Q&A], https://web.archive.org/web/20141005093717/http://www.nyc.gov/html/doitt/downloads/pdf/RFP_Pre-proposal_conference_QA.pdf [https://perma.cc/B7HP-NXM7].

122. RFP - Pre-proposal Conference Q&A, *supra* note 121, at 4, 5.

123. Transcript of Public Hearing of the Franchise and Concession Review Comm. 12 (Dec. 8, 2014) [hereinafter Transcript of Public Hearing of the Franchise and Concession Review Comm.], https://web.archive.org/web/20150321025658/http://www.nyc.gov/html/mocs/downloads/pdf/fcrc_trans/FCRC_%20Public_Hearing_Transcript_12_8_14.pdf [https://perma.cc/X379-TJYX]; *see also* Letter from Dominic Mauro, Records Access Officer, City of New York, Dep't of Tech. & Telecomm., to Eric Hornbeck (Oct. 3, 2017) [hereinafter FOIL Request] (on file with the author).

124. Clear Channel Outdoor, NYC Public Communications Structures Proposal 5 (July 21, 2014) [hereinafter Clear Channel Bid] (on file with the author).

advertising company and payphone franchise holder Van Wagner;[125] LQD Wi-Fi NYC, LLC, a consortium of companies that included ones involved in the Harlem Wi-Fi project;[126] the United States Post Office, which proposed an alternative that would incorporate both Wi-Fi and structures with lock boxes for New Yorkers to receive packages;[127] Telebeam Telecommunications Corp., which held a payphone franchise;[128] an individual; and CityBridge LLC,[129] a consortium of companies that includes the previous owners of many of the city's payphones,[130] Qualcomm Inc., entities later controlled by Google parent Alphabet Inc., and others.[131] Revenue estimates in the proposals varied. Clear Channel said the city's specifications were too vague to make an accurate revenue estimate[132] and the Post Office did not make a revenue estimate.[133] Van Wagner estimated about $300 million over the period of the franchise;[134] LQD estimated $180 million in annual revenue for the city.[135]

In November 2014, the city selected CityBridge's "LinkNYC" as the winning bid.[136] LinkNYC kiosks promised internet access and

---

125. Van Wagner, Statement of Qualifications & Technical Proposal 5 (July 18, 2014) (on file with the author).

126. LQD NYC, LQD WiFi NYC Response 6–7, 41 (July 21, 2014) [hereinafter LQD Bid] (on file with the author).

127. U.S. Postal Service, Expanding Full Participation in the Digital Economy 1 (July 21, 2014) [hereinafter Post Office Bid] (on file with the author).

128. Exhibit 8 to Complaint at 4, Telebeam Telecomm. Corp. v. City of New York, No. 1:14-cv-07100 (E.D.N.Y. Dec. 4, 2014).

129. *See* FOIL Request, *supra* note 123.

130. *LinkNYC Spy Stations*, ELEVENTH HOPE CONFERENCE, INTERNET SOC'Y (July 24, 2016, 5:20PM) [hereinafter *Internet Society Conference*], https://livestream.com/internetsociety/hopeconf/videos/130816888 [https://perma.cc/JC8X-6DKS] (remarks of Benjamin Dean, Columbia Univ. fellow and consultant).

131. *See Frequently Asked Questions*, LINKNYC, https://www.link.nyc/faq.html [https://perma.cc/QE3Z-74WK]; *see also* 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/E7MW-VG9P]. *See generally* INTERSECTION, https://www.intersection.com/ [https://perma.cc/5SS7-FBT4] (indicating that LinkNYC was the first product of Intersection, which was formed from a merger between Titan and Control Group).

132. Clear Channel Bid, *supra* note 124, at 209.

133. Post Office Bid, *supra* note 127, at 14–15.

134. Van Wagner, Compensation Proposal 3 (on file with the author).

135. LQD Bid, *supra* note 126, at 127.

136. Press Release, City of New York, De Blasio Administration Announces Winner of Competition to Replace Payphones with Five-Borough Wi-Fi Network (Nov. 17, 2014) [hereinafter De Blasio Administration Announces Winner], http://www1.nyc.gov/office-of-the-mayor/news/923-14/de-blasio-administration-winner-competition-replace-payphones-five-borough [https://perma.cc/3T3B-FP5J];

city information services at the kiosks' tablets,[137] free high-speed Wi-Fi, free phone calls, and to funnel back to the city about half of the $1 billion in advertising revenue expected over the life of the franchise agreement.[138] The Wi-Fi ultimately provided by the kiosks was not only free, but also fast[139]: one estimate put the speed at 436 Mbps for downloads and 361 Mbps for uploads[140]—far faster than the FCC's fixed broadband benchmark of 25 Mbps for downloads and 3 Mbps for uploads.[141] Such speeds, some of the fastest of any such networks worldwide, are "dizzying."[142] "LinkNYC is ten times faster than New York's existing public internet, and infinitely quicker than [the public Wi-Fi at] Starbucks."[143] Mayor Bill de Blasio touted the project as one way to help close the city's digital divide by providing free access to low-income New Yorkers who rely on mobile devices.[144] The kiosks were part of the city's efforts to expand broadband deployment and availability.[145]

---

see also City of New York Dep't of Info. Tech. & Telecomm., Franchise Agreement for the Installation, Operation, & Maintenance of Public Communications Structures in the Boroughs of the Bronx, Brooklyn, Manhattan, Queens and Staten Island [hereinafter LinkNYC Franchise Agreement], https://www1.nyc.gov/assets/doitt/downloads/pdf/Franchise-Agreement-for-Public-Communications-Structures-(REVISED-FINAL-12-10-2014).pdf [https://perma.cc/C4CJ-BZVY].

137. The tablets initially allowed users to access the internet, but that functionality was disabled after community complaints about users lingering all day at the kiosks. Now, the tablets provide only maps and access to city services through the 311 network. Transcript of the Minutes of the N.Y.C. Council Comm. on Tech. 9-12 (Nov. 15, 2016) [hereinafter Nov. 2016 Council Hearing], http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=2865660&GUID=1B0A5153-F381-4EAB-AD01-99A3A616982D&Options=&Search= [https://perma.cc/E6ZP-7G73].

138. Peltz, *supra* note 116; *see* De Blasio Administration Announces Winner, *supra* note 136.

139. *Frequently Asked Questions*, *supra* note 131, at 5.

140. Bryan Lufkin, *NYC's New Public Wifi Is Obscenely Fast*, GIZMODO (Jan. 19, 2016, 3:20 PM), https://gizmodo.com/nycs-new-public-wifi-is-obscenely-fast-1753825735 [https://perma.cc/K5VA-NJ9A] (anecdotal speed test by journalist).

141. FED. COMMC'NS COMM'N, *supra* note 10, at 5.

142. Stern, *supra* note 89.

143. Lufkin, *supra* note 140.

144. Matt Flegenheimer, *Pay Phones in New York City Will Become Free Wi-Fi Hot Spots*, N.Y. TIMES (Nov. 17, 2014), https://www.nytimes.com/2014/11/18/nyregion/pay-phones-in-new-york-city-will-become-free-wi-fi-hot-spots.html [https://nyti.ms/2sbemTV]; De Blasio Administration Announces Winner, *supra* note 136.

145. Transcript, Press Release: Mayor de Blasio Announces Public Launch of LinkNYC Program, Largest and Fastest Free Municipal Wi-Fi Network in the World 5 (Feb. 18, 2016) [hereinafter Mayor de Blasio Announces Public Launch of LinkNYC Program], http://www1.nyc.gov/office-of-the-mayor/news/187-16/transcript-mayor-de-blasio-public-launch-linknyc-program-largest-fastest-free [https://perma.cc/8D7L-Q5KL].

The public viewed LinkNYC cautiously as a step toward closing the digital divide by bringing the internet to the poor[146] and the homeless.[147] The program also proved popular: by January 2017, more than one million people had signed up to access the kiosks' Wi-Fi service on their mobile devices.[148] By that point, about 71% of New Yorkers were aware of the kiosks, and of them, about 92% felt they were a positive addition to the city, according to a city-commissioned survey.[149]

The LinkNYC kiosks were also billed as secure and respectful of users' personal data.[150] The city said that users' personal data would be protected because the kiosk network would be one of the largest encrypted public Wi-Fi networks.[151] The privacy policy was billed as "customer-first" and one that would "ensure[] personal information is never shared or sold for third party use."[152]

The new service was not without its hiccups and criticisms, however. First, some questioned whether the kiosks would actually do enough to close the digital divide.[153] Some city officials complained that the franchise agreement would exacerbate the digital divide between richer Manhattan neighborhoods—where more lucrative advertising revenues incentivized a quicker and more extensive rollout of the kiosks—and poorer neighborhoods that were

---

146. Linda Huber, *Is New York City's Public Wi-Fi Actually Connecting the Poor?*, MOTHERBOARD (Sept. 14, 2016, 7:00 AM), https://motherboard.vice.com/en_us/article/linknyc-is-bringing-internet-to-new-yorks-most-disconnected-people [https://perma.cc/2J3S-KZNK].

147. Karen Matthews, *New Free Wi-Fi Kiosks a Hit with Homeless New Yorkers*, CHI. TRIB. (Aug. 24, 2016, 10:20 AM), http://www.chicagotribune.com/bluesky/technology/ct-homeless-wi-fi-kiosks-ap-bsi-20160824-story.html [https://perma.cc/9DGW-YDXC].

148. Press Release, De Blasio Administration and CityBridge Announce LinkNYC Has Reached One Million Users in Less than One Year (Jan. 18, 2017) [hereinafter One Million Users Press Release], http://www1.nyc.gov/office-of-the-mayor/news/031-17/de-blasio-administration-citybridge-linknyc-has-reached-one-million-users-less-than [https://perma.cc/6RA9-TZWF].

149. *Id.*

150. Mayor de Blasio Announces Public Launch of LinkNYC Program, *supra* note 145.

151. *Id.*; *see also Features Fact Sheet*, LINKNYC, https://www.link.nyc/assets/downloads/LinkNYC-Fact-Sheet.pdf [https://perma.cc/W3NE-ZVU2].

152. *Features Fact Sheet*, *supra* note 151; *see also* Mayor de Blasio Announces Public Launch of LinkNYC Program, *supra* note 145.

153. Huber, *supra* note 146 ("[O]nly 700 of the planned 7,500 Links are to be installed in the Bronx, the borough with the highest percentage of households without broadband. This raises the question of just *how* central the digital divide is to the mission of LinkNYC, or whether it is just the piece that seems sexiest to emphasize.").

less attractive to advertisers.[154] The city made changes to the franchise agreement before it was approved to placate those concerns.[155] In addition, the free internet access at the tablets on the kiosks led some users to gather for hours at kiosks,[156] watching pornography,[157] drinking, and doing drugs.[158] LinkNYC responded by reducing the volume on the kiosk speakers after a certain hour[159] and removing internet browsing capabilities from the kiosk tablets.[160] Other features remained unchanged, including the fast wireless internet, access to city services on the tablets, free phone calls, cell phone charging, and 311 and 911 access.[161] City officials have said they are open to restoring the internet access if they can properly filter objectionable content and set time limits.[162]

---

154. Press Release, Comptroller Stringer and Borough Presidents Diaz, Adams, Brewer, Katz And Oddo Call for Five Borough Broadband Bill of Rights on Public Wi-Fi Agreement (Dec. 3, 2014) [hereinafter Comptroller and Borough Presidents' Press Release], https://comptroller.nyc.gov/newsroom/comptroller-stringer-and-borough-presidents-diaz-adams-brewer-katz-and-oddo-call-for-five-borough-broadband-bill-of-rights-on-public-wi-fi-agreement/ [https://perma.cc/3XU8-ZFMY]; *see also* Kristen Meriwether, *Pay Phone Wi-Fi Deal Nears Approval Despite Concerns, Lawsuit*, GOTHAM GAZETTE (Dec. 8, 2014), http://www.gothamgazette.com/government/5459-pay-phone-wi-fi-deal-nears-approval-despite-concerns-lawsuit [https://perma.cc/GH3E-KDBR].

155. Miranda Neubauer, *Franchise Committee Approves New City Wi-Fi Proposal*, POLITICO N.Y. (Dec. 10, 2014, 6:46 PM), https://www.politico.com/states/new-york/city-hall/story/2016/05/franchise-committee-approves-new-city-wi-fi-proposal-051708 [https://perma.cc/L2ZH-XXP5].

156. Huber, *supra* note 146.

157. Joshua Brustein, *Building a Smart City? Have You Thought About Porn and Privacy*, BLOOMBERG TECH. (Sept. 14, 2016, 9:03 PM), https://www.bloomberg.com/news/articles/2016-09-15/building-a-smart-city-have-you-thought-about-porn-and-privacy [https://perma.cc/LES2-PBUY].

158. Patrick McGeehan, *Free Wi-Fi Kiosks Were to Aid New Yorkers. An Unsavory Side Has Spurred a Retreat*, N.Y. TIMES (Sept. 14, 2016), https://www.nytimes.com/2016/09/15/nyregion/internet-browsers-to-be-disabled-on-new-yorks-free-wi-fi-kiosks.html [https://nyti.ms/2krRPeu].

159. *Free Wi-Fi Kiosks Prompt Concerns of Potential Misuse by Homeless New Yorkers*, CBS N.Y. (June 13, 2016, 11:31 PM), http://newyork.cbslocal.com/2016/06/13/free-wi-fi-kiosks/ [https://perma.cc/HQF2-7KRJ].

160. *Service Update*, LINKNYC (Sept. 14, 2016), https://www.link.nyc/service-update.html [https://perma.cc/L7LK-QGD4].

161. *Id.*; *see also* Yoav Gonen & Reuven Fenton, *De Blasio Disables Internet Access on Wi-Fi Kiosks Screens*, N.Y. POST (Sept. 14, 2016, 2:53 PM), http://nypost.com/2016/09/14/de-blasio-disables-internet-access-on-wifi-kiosk-screens/ [https://perma.cc/98DX-5DLN]; Associated Press, *NYC to Pull Plug on Sidewalk Internet After Porn Complaints*, WASH. TIMES (Sept. 14, 2016), https://www.washingtontimes.com/news/2016/sep/14/nyc-to-pull-plug-on-sidewalk-internet-after-porn-c/ [https://perma.cc/CW9K-PKBY].

162. Rich Calder & Natalie O'Neill, *City Officials Had No Idea New Yorkers Are so Porn-Starved*, N.Y. POST (Nov. 15, 2016, 6:16 PM), http://nypost.com/2016/11/15/

LinkNYC's privacy protections were also met less enthusiastically by privacy activists and the technology press: in fact, one headline said the LinkNYC kiosks amounted to a "privacy nightmare."[163] The use of advertising revenue to fund such an ambitious project was described as a "Faustian bargain": trading personal privacy for ubiquitous tracking by advertisers.[164] A representative for the city's public advocate, Letitia James, had urged the city to reject the LinkNYC deal because of concerns that the lack of competition among franchisees could harm civil liberties, among other concerns.[165] Some New Yorkers expressed vague concerns over possible information sharing.[166] LinkNYC officials confirmed that they would hand over information about users from the kiosks to the police if legally required.[167] Adding to the unease, Titan, one of the backers of CityBridge, had been installing tracking beacons in its existing payphones without any public notice and was forced by the city to remove them once the news broke.[168]

But it was LinkNYC's privacy policy, which users must accept to access the kiosk's services,[169] that was met with particular scorn. Civil

---

city-officials-had-no-idea-new-yorkers-are-so-porn-starved/ [https://perma.cc/ZV3K-QV9F].

163. Darren Orf, *NYC's Free Wifi Service Is Turning into a Privacy Nightmare*, GIZMODO (Mar. 17, 2016, 11:23 AM), http://gizmodo.com/nycs-free-wifi-service-is-turning-into-a-privacy-nightm-1765474061 [https://perma.cc/74GH-XBJD].

164. VanHemert, *supra* note 105.

165. Transcript of Public Hearing of the Franchise and Concession Review Comm., *supra* note 123 (testimony of Umair Khan, Deputy Counsel to the Public Advocate Letitia James).

166. One person told a reporter that "she did not feel comfortable using the Wi-Fi or connecting her phone to the USB outlet. 'For some reason, I don't trust it,' she said. 'They're trying to get everyone's information.'" Patrick McGeehan, *New Yorkers Greet the Arrival of Wi-Fi Kiosks with Panic, Skepticism and Relief*, N.Y. TIMES (July 26, 2016), https://www.nytimes.com/2016/07/27/nyregion/link-nyc-wi-fi-kiosks.html [https://nyti.ms/2kAHtJV]. Another person "said his primary concern was 'having to give them information,' not that he was certain who 'they' were." *Id. But see id.* (describing others who said the kiosks provided access to people who otherwise couldn't afford to get online). *See also* Peltz, *supra* note 116 (interviews with passersby expressing similar concerns).

167. Jillian Jorgensen, *De Blasio Unveils LinkNYC Wifi Kiosks, with Promises to Protect Privacy*, OBSERVER (Feb. 28, 2016, 6:37 PM), http://observer.com/2016/02/de-blasio-unveils-linknyc-wifi-kiosks-with-promises-to-protect-privacy/ [https://perma.cc/H58T-2XEQ].

168. Joseph Bernstein et al., *Exclusive: Hundreds of Devices Hidden Inside New York City Phone Booths*, BUZZFEED NEWS (Oct. 6, 2014, 3:00 AM), https://www.buzzfeed.com/josephbernstein/exclusive-hundreds-of-devices-hidden-inside-new-york-city-ph [https://perma.cc/6XHQ-62B7]; VanHemert, *supra* note 105.

169. *See* Exhibit 2, CityBridge Privacy Policy, Franchise Agreement for the Installation, Operation, and Maintenance of Public Communications Structures in

liberties groups, such as the New York Civil Liberties Union, decried LinkNYC's privacy policy as hopelessly vague about what sorts of data and information it would actually collect from users (such as what websites users visit and what links they click on) or how long LinkNYC might keep their data on file.[170] That data also could reveal much personal information about individual users if aggregated.[171] Similarly, even though CityBridge's policy said that it would not sell personally identifiable information, it did say that it "may" "share" that data with others, including law enforcement and anyone who might acquire CityBridge.[172] The privacy policy was hard to find, as well: the policy that CityBridge posted on LinkNYC's website only applied to that website, not the kiosks themselves.[173] Whether, and how easily, law enforcement could access the data was unclear in the policy.[174] Critics complained that it was not apparent why the kiosks would be mounted with cameras and who would be able to see the camera and sensor feeds.[175] One possibility suggested was that the video feed could significantly expand the NYPD's already vast camera network in the Domain Awareness System.[176]

---

the Boroughs of the Bronx, Brooklyn, Manhattan, Queens and Staten Island (Jan. 25, 2016) (on file with author).

170. *Internet Society Conference*, *supra* note 130, at 15:00; *see also* Press Release, N.Y. Civil Liberties Union, City's Public Wi-Fi Raises Privacy Concerns (Mar. 16, 2016) [hereinafter NYCLU March 2016 Press Release], https://www.nyclu.org/en/press-releases/nyclu-citys-public-wi-fi-raises-privacy-concerns [https://perma.cc/WH6W-CRQ5].

171. Alix Jean-Pharuns, *What the LinkNYC Project Means for the Average New Yorker*, MOTHERBOARD (Jan. 29, 2015, 10:10 AM), https://motherboard.vice.com/en_us/article/what-the-linknyc-project-means-for-the-average-new-yorker [https://perma.cc/NAX5-E3ZF]; *see also* Jorgensen, *supra* note 167.

172. *Internet Society Conference*, *supra* note 130, at 15:00.

173. Brady Dale, *Meet the Brave Souls Who Read LinkNYC's Two Different Privacy Policies*, OBSERVER (July 28, 2016, 9:17 AM), http://observer.com/2016/07/linknyc-intersection-sidewalk-labls-alphabet-google-privacy/ [https://perma.cc/89BB-MMUE].

174. Press Release, N.Y. Civil Liberties Union, Testimony Regarding Technology Oversight Hearing on LinkNYC (Nov. 15, 2016), https://www.nyclu.org/en/publications/testimony-regarding-technology-oversight-hearing-linknyc [https://perma.cc/JNR4-66XR].

175. Nov. 2016 Council Hearing, *supra* note 137, at 59, 76; *see also* Shahid Buttar & Amul Kalia, *LinkNYC Improves Privacy Policy, Yet Problems Remain*, ELEC. FRONTIER FOUND. (Oct. 4, 2017), https://www.eff.org/deeplinks/2017/09/linknyc-improves-privacy-policy-yet-problems-remain [https://perma.cc/7E8T-VLL4].

176. *Internet Society Conference*, *supra* note 130, at 31:30 (remarks of Mariko Hirose, New York Civil Liberties Union attorney); NYCLU March 2016 Press Release, *supra* note 170; *see also Developing the NYPD's Information Technology*, *supra* note 97 ("Plans are in place to expand the fiber network to connect non-NYPD sites that have camera feeds or other data sources that the Department wishes to access in real-time.").

The cameras also could collect information on passersby who never agreed to the privacy policy.[177] Indeed, the vague privacy policy seemed to lead to a perverse outcome: instead of closing the digital divide, LinkNYC would subject poor communities dependent on its free Wi-Fi to even more mass surveillance by law enforcement than ever before.[178]

Why would CityBridge want to collect all this information? The goal of LinkNYC's private developers is not just to close the digital divide but also to make money.[179] Even if the city has described LinkNYC benignly as "the largest and fastest network of its kind," advertisers see it as the "one of the largest digital [out-of-home advertising] networks in the world."[180] All of that data provides a rich trove for a deep analysis by advertisers.[181] Indeed, targeting advertising directly at specific people by using the data harvested from users seemed to be a driving force behind the companies that developed the kiosks.[182] The kiosks can allegedly use that data to create location-specific targeted advertising that is more valuable to advertisers.[183] The targeted advertising capabilities were also billed to advertisers as a key feature of the new kiosks, even though that possibility was obscured from users in the privacy policy.[184] All the data that LinkNYC is able to collect from users, cameras trained on pedestrians, and sensors monitoring traffic and environmental factors would allow City Bridge to generate $30,000 a year from each

---

177. *Internet Society Conference*, *supra* note 130, at 41:20 (remarks of Mariko Hirose).

178. Kaveh Waddell, *Will New York City's Free Wi-Fi Help Police Watch You?*, THE ATLANTIC (Apr. 11, 2016), https://www.theatlantic.com/technology/archive/2016/04/linknyc-new-york-wifi-privacy-security/477696/ [https://perma.cc/DY2W-D2H2]; *see* Transcript of the Minutes of the N.Y.C. Council Comm. on Tech 4 (Apr. 25, 2017) [hereinafter April 2017 Council Hearing], http://legistar.council.nyc.gov/View.ashx?M=F&ID=5153013&GUID=7D78C0C0-40AE-4811-9AD6-D170D33A504E [https://perma.cc/8LHF-5V4H].

179. Andrew J. Hawkins, *Sidewalk Labs Hires 'Dream Team' to Tackle City Design in the Self-Driving Age*, THE VERGE (Feb. 22, 2016, 9:00 AM), https://www.theverge.com/2016/2/22/11081968/sidewalk-labs-google-smart-city-product-link-nyc [https://perma.cc/84F6-6H65].

180. Janet Stilson, *What It Means for Consumers and Brands That New York Is Becoming a 'Smart City'*, ADWEEK (Feb. 15, 2016), http://www.adweek.com/digital/what-it-means-consumers-and-brands-new-york-becoming-smart-city-169643/ [https://perma.cc/DC5D-CPWD].

181. *See id.*

182. *Internet Society Conference*, *supra* note 130, at 18:20.

183. *Id.* at 25:30; Pinto, *supra* note 131.

184. *See* Pinto, *supra* note 131.

kiosk.[185] Essentially, the privacy policy was so vague that CityBridge could "collect anything and do anything."[186] LinkNYC officials said they did not plan to sell aggregated data.[187]

Then, a year after the New York Civil Liberties Union and other groups first criticized the policy and the public outcry erupted, CityBridge announced that it would change the policy.[188] The new policy was more specific about the data CityBridge would collect and how long it would retain that data.[189] The new policy said that it would only store "technical" data used to connect to the Wi-Fi for sixty days after inactivity.[190] Camera data would only be stored for seven days,[191] and video footage and other data could be obtained by law enforcement only through an official request such as a court order.[192] The new policy also promised that it "will not use facial recognition technology for any reason . . . [or the] cameras to track your movement throughout the city."[193] The policy still, however, said that LinkNYC could identify users' "general" location.[194] The New York Civil Liberties Union and city officials praised the changes.[195]

---

185. *See* Mark Harris, *Inside Alphabet's Money-Spinning, Terrorist-Foiling, Gigabit Wi-Fi Kiosks*, RECODE (July 1, 2016, 7:00 AM), https://www.recode.net/2016/7/1/12072122/alphabet-sidewalk-labs-city-wifi-sidewalk-kiosks [https://perma.cc/ZJ28-FXY4].

186. *Internet Society Conference*, *supra* note 130, at 33:20 (remarks of Mariko Hirose).

187. Mayor de Blasio Announces Public Launch of LinkNYC Program, *supra* note 145. Colin O'Donnell, the Chief Innovation Officer of Intersection, said, "The bundling and sale of anonymized data actually doesn't factor into the business plan." *Id.*

188. *See* LinkNYC (@LinkNYC), TWITTER (Mar. 17, 2017, 7:40 AM), https://twitter.com/LinkNYC/status/842747505569873920 [https://perma.cc/8G85-Y7WQ].

189. Press Release, N.Y. Civil Liberties Union, City Strengthens Public Wi-Fi Privacy Policy After NYCLU Raises Concerns (Mar. 17, 2017) [hereinafter NYCLU March 2017 Press Release], https://www.nyclu.org/en/press-releases/city-strengthens-public-wi-fi-privacy-policy-after-nyclu-raises-concerns [https://perma.cc/XC68-22CC].

190. Exhibit 2, CityBridge Privacy Policy, Franchise Agreement for the Installation, Operation, and Maintenance of Public Communications Structures in the Boroughs of the Bronx, Brooklyn, Manhattan, Queens and Staten Island 2 (Mar. 17, 2017) [hereinafter March 2017 LinkNYC Privacy Policy], http://www1.nyc.gov/assets/doitt/downloads/pdf/Proposed-PCS-Franchise-Exhibit-2-CityBridge-Privacy-Policy.pdf [https://perma.cc/KH2E-ESAK].

191. *Id.* at 5.

192. *Id.* at 4.

193. *Id.* at 6.

194. *Id.* at 3.

195. April 2017 Council Hearing, *supra* note 178, at 18; NYCLU March 2017 Press Release, *supra* note 189.

Nevertheless, the kiosks continue to generate tension between the much-praised goal of bringing internet access to more New Yorkers and concerns about what user data these kiosks run by a private entity may, or could, collect.[196] For example, the privacy policy can still be changed at any time.[197] The information that LinkNYC collects even under its more restrictive policy is still highly personal and could be de-anonymized.[198] Brooklyn residents have circulated petitions opposing the kiosks over surveillance concerns, and in Manhattan, some of the kiosks' cameras have been covered with tape.[199] Digital privacy group Electronic Frontier Foundation said that even though the changes were welcome, the process of changing the privacy policy remained "opaque."[200]

II. JUDICIAL APPROACHES TO THE TECHNOLOGIES THAT MAKE UP LINKNYC KIOSKS

LinkNYC's kiosks combine into a single device several technologies and tracking capabilities that courts have addressed in different lines of cases and using various standards. Information about where New Yorkers travel throughout the city each day could

---

196. *Compare* April 2017 Council Hearing, *supra* note 178, at 41 (statement of James Vacca) ("[W]e all love them[.]"), *with id.* at 4 (statement of James Vacca) ("[T]he city is executing several projects to provide internet to low income individuals most notably the ongoing roll out of LinkNYC and the expansion of broadband services in NYCHA developments. These efforts are to be commended but also represent an area in which we must be particularly vigilant. Many national studies indicate that lower income people are disproportionately burdened by data collection and privacy violations. Additionally, data digital advertising all too often targets these groups. Privacy is not a luxury item but a fundamental right of all people.").

197. The privacy policy states that users who provided an email address will be notified if the privacy policy changes and will then have an opportunity to stop using LinkNYC "if they do not consent to the changes." March 2017 LinkNYC Privacy Policy, *supra* note 190, at 6. Similarly, the NYPD's privacy policy for its Domain Awareness System contains limits on how long the NYPD can store data, but those limits can be extended if there is a "continuing law enforcement or public safety value or legal necessity." N.Y.C. Police Dep't, Public Security Privacy Guidelines 4 (Apr. 2, 2009), http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf [https://perma.cc/6QFN-UJ7H].

198. *See* Buttar & Kalia, *supra* note 175 (noting that the new policy still collects some personally identifiable information); Pinto, *supra* note 131 (describing how even anonymized "technical" information about device hardware can be used to identify specific people).

199. Deanna Paul, *Use the Wi-Fi and Smile for the Camera: LinkNYC Kiosks Come Uptown*, THE UPTOWNER (Oct. 18, 2017), https://theuptowner.org/use-the-wi-fi-and-smile-for-the-camera-linknyc-kiosks-come-uptown/ [https://perma.cc/X6ST-GHH2].

200. Buttar & Kalia, *supra* note 175.

be collected in multiple ways: their real-time movements tracked as they move around the city; their historical movements could be analyzed by government investigators; and even those who have never logged in could be tracked using the video cameras mounted on the kiosks and facial recognition software. Depending on which version of its privacy policy is at issue, LinkNYC may collect this information or not, or could hand it over to the government without even informing users. The law treats these different types of location data[201] differently: some jurisdictions require a warrant, others do not; in some jurisdictions these questions are percolating through appeals; and in others, these types of location data have yet to be addressed by a court or legislature at all.

LinkNYC and other smart city initiatives pose myriad privacy issues, including vulnerability to hackers and private companies selling personal information to advertisers or other third parties. This Note, however, focuses on the clash between law enforcement and citizens' privacy as courts struggle to react to rapid technological change. Specifically, how does the technology facilitate tracking a person's location, and what must law enforcement do to gain access to the location data collected by the kiosks?

A. Fourth Amendment "Expectations of Privacy" and the "Third-Party Doctrine"

The Fourth Amendment prohibits "unreasonable searches and seizures" by the government unless a judge determines that law enforcement has probable cause to conduct the search and the judge issues a warrant.[202] But what counts as a search, and what is unreasonable?

In 1967, the U.S. Supreme Court in *Katz v. United States*[203] said that one way to evaluate whether a search is constitutional without a warrant is to consider "expectations of privacy."[204] Prior to *Katz*, the Court had articulated a trespass-based approach to Fourth Amendment searches—that is, a search requiring a warrant occurred whenever the government made "an unauthorized physical

---

201. Many other types of data could also be collected from the kiosks, such as data about users' internet browsing history. *See* NYCLU March 2016 Press Release, *supra* note 170. The judicial treatment of these other types of non-location data is not addressed in this Note.

202. *See* U.S. CONST. amend. IV.

203. Katz v. United States, 389 U.S. 347 (1967).

204. *Id.* at 361–62 (Harlan, J., concurring).

encroachment within a constitutionally protected area."[205] As the Court noted several years before *Katz* in *Silverman v. United States*,[206] what matters was not just "the technicality of a trespass" but "the reality of an actual intrusion into a constitutionally protected area."[207]

In *Katz*, the Court redefined the reach of its trespass-based test[208] and replaced it with what became known as the "reasonable expectation of privacy" test.[209] In *Katz*, the government had placed an electronic listening device on the outside of a telephone booth to hear what a suspect inside was saying over the telephone.[210] The Court held that this was a search that violated the Fourth Amendment because the police did not have a warrant.[211] In doing so, the Court abandoned its focus in Fourth Amendment cases on a physical trespass occurring.[212] In a concurrence, Justice John M. Harlan II articulated the Court's new "reasonable expectation of privacy" test as "a twofold requirement": "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[213] But what is "reasonable" has not always been clear. In the years since articulating the test, "the meaning of the phrase 'reasonable expectation of privacy' remains remarkably opaque" and scholars have found the confusion over application of the test to be an "embarrassment."[214]

In addition to the "reasonable expectation of privacy," another long-held standard in Fourth Amendment jurisprudence is the

---

205. Silverman v. United States, 365 U.S. 505, 510 (1961).

206. *Id.*

207. *Id.* at 512.

208. WAYNE R. LAFAVE, SEARCH & SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(b) (5th ed. 2018) (citing Edmund W. Kitch, Katz v. United States*: The Limits of the Fourth Amendment*, 1968 SUP. CT. REV. 133, 133 (1968)).

209. *See* United States v. Jones, 565 U.S. 400, 405–06 (2012) (discussing the *Katz* shift to "reasonable expectation of privacy"). *Compare id.* at 409 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.") (emphasis in original), *with id.* at 421–23 (Alito, J., concurring) (arguing that *Katz* had done away with the "repeatedly criticized" trespass-based rule).

210. Katz v. United States, 389 U.S. 347, 348 (1967).

211. *Id.* at 359.

212. *Id.* at 353.

213. *Id.* at 361 (Harlan, J., concurring).

214. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504–05 (2007) (discussing four models to categorize the Court's various applications of the *Katz* test); *see also* discussion *infra* Section II.E.

controversial "third-party doctrine."[215] "The rule is simple: By disclosing information to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed."[216] The doctrine has roots in *Katz*, in which the Court noted that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[217] The Court further refined the doctrine in the 1970s cases *United States v. Miller*[218] and *Smith v. Maryland*.[219] In *Miller*, the Court said that a person suspected of tax fraud had no expectation of privacy in his bank records because he had known the bank might show the records to others when he gave the information to the bank.[220] Similarly, in *Smith*, the Court said that there is no expectation of privacy in the phone numbers a person dials because people know that the phone company keeps a record of those calls.[221] In addition to those articulations of the third-party doctrine, the Court has also held that people do not have a reasonable expectation of privacy when traveling along public thoroughfares, such as driving a car along a highway, because doing so knowingly exposes the person to "anyone who wanted to look."[222] This doctrine, too, has been criticized.[223]

As indicated by *Katz* and the third-party doctrine, while government surveillance is typically subject to a warrant requirement, commercial transactions that implicate the third-party doctrine are held to a much lower standard.[224] Modern technology, such as "smart home" devices that communicate intimate data to technology companies, has expanded the pervasiveness of data that could be handed over to law enforcement without a warrant under the

---

215. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 570–73 (2009) (defending the doctrine while noting that criticism of it is "widespread").

216. *Id.* at 563.

217. *Katz*, 389 U.S. at 351.

218. United States v. Miller, 425 U.S. 435, 442–43 (1976).

219. Smith v. Maryland, 442 U.S. 735, 742–45 (1979).

220. *Miller*, 425 U.S. at 442–43.

221. *Smith*, 442 U.S. at 742–45.

222. United States v. Knotts, 460 U.S. 276, 281–82 (1983).

223. Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, ABA J. (Aug. 2012), http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/ [https://perma.cc/Q6NE-LD7U]. *But see* Kerr, *supra* note 215, at 570–73.

224. *See* Olivier Sylvain, *Failing Expectations: Fourth Amendment Doctrine in the Era of Total Surveillance*, 49 WAKE FOREST L. REV. 485, 486–88 (2014).

doctrine.[225] Indeed, as the "frightening paraphernalia"[226] of modern technology has advanced, that distinction and the differences between the *Katz* and third-party doctrine concepts have been questioned.[227] The clash of these and other concepts in Fourth Amendment search jurisprudence have shown up in the cases that deal with technology embedded in the LinkNYC kiosks: real-time location tracking, historical location data collected by cell phone providers, and facial recognition technology.[228]

B. Tracking Real-Time Location Using GPS Technology

After relying on Justice Harlan's test in the ensuing decades,[229] the Court in 2012 questioned its own Fourth Amendment jurisprudence with its decision in *United States v. Jones*.[230] In *Jones*, the police had surreptitiously placed a global positioning system ("GPS") device on a suspect's car and tracked his movements for twenty-eight days.[231] All the justices said that doing so without a warrant was an

---

225. Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1925 (2017).

226. Silverman v. United States, 365 U.S. 505, 509 (1961). Decided before *Katz*, *Silverman* involved a device that the police had inserted into a shared party wall that, when it touched a heating duct, allowed the police to listen to conversations in the house. *Id.* at 506–07. The government had argued that the Court needed to revisit its Fourth Amendment precedents in light of imminent technological developments that would make it possible to eavesdrop on conversations from even farther away. *Id.* at 508–09. But the Court refused to do so in that case: "We need not here contemplate the Fourth Amendment implications of these and other frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society." *Id.* at 509.

227. *See, e.g.*, Rex R. Perschbacher, *Symposium: Welcoming Remarks:* Katz v. U.S.*: 40 Years Later*, 41 U.C. DAVIS L. REV. 775, 778–79 (2007); John Castellano, *Symposium: Justices Poised to Consider, or Reconsider, Fourth Amendment Doctrines as They Assess the Scope of Privacy in a Digital Age*, SCOTUSBLOG (Aug. 1, 2017, 2:49 PM), http://www.scotusblog.com/2017/08/symposium-justices-poised-consider-reconsider-fourth-amendment-doctrines-assess-scope-privacy-digital-age/ [https://perma.cc/WZ98-YRNX].

228. Currently, most of the data that LinkNYC collects is anonymized or not stored for extended periods. *See* discussion *supra* Section I.C.

229. *See* United States v. Jones, 565 U.S. 400, 406 (2012) ("Our later cases have applied the analysis of Justice Harlan's concurrence in that case . . . .").

230. *Id.*

231. The police had obtained a warrant, but did not install the GPS until after the warrant had expired. *Id.* at 403.

unconstitutional search—but they were divided across three opinions as to why.[232]

Justice Antonin Scalia, writing for five justices, said that the *Katz* test did not replace the Court's earlier trespass-based approach: it merely supplemented the trespass doctrine for use in cases where no physical trespass had occurred.[233] Justice Scalia said that because there was a physical intrusion into a space—the police physically placing the GPS device on the suspect's car—there was no need to invoke the *Katz* test to find an unconstitutional search.[234]

Justice Samuel Alito, writing for four justices, agreed that the police needed a warrant to attach the GPS device to the car, but not because of the trespass. Instead, he said long-term surveillance of a suspect's location without a warrant was unreasonable under the *Katz* test.[235] Justice Alito criticized the majority for resurrecting the "repeatedly criticized" trespass-based rule.[236] Among other reasons, he noted that the trespass-based rule will create problems in a digital world: increasingly, the movements of an object like a car can be tracked electronically without any physical contact with the object to be tracked.[237]

Justice Alito also questioned whether the Court was the best place to resolve such thorny issues. The *Katz* test is far from perfect, and judges often "confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks."[238] The test is further complicated by the increasingly rapid pace of technological change, keeping public opinion about privacy expectations "in flux."[239] People may continue to object to some practices, or they could decide that the conveniences they receive in exchange for decreased privacy are worthwhile.[240] Against such a backdrop, legislative solutions are perhaps better than judicial fiat, he

---

232. Miriam H. Baer, *Secrecy, Intimacy, and Workable Rules: Justice Sotomayor Stakes Out the Middle Ground in* United States v. Jones, 123 YALE L.J. FORUM 393, 394 (2014).

233. *Jones*, 565 U.S. at 411.

234. *Id.* at 406–07.

235. *Id.* at 430–31 (Alito, J., concurring).

236. *Id.* at 421–23.

237. *Id.* at 426.

238. *Id.* at 427.

239. *Id.*

240. *Id.*

said.[241] In fact, Congress passed wiretapping legislation shortly after the *Katz* decision.[242]

Justice Sonia Sotomayor provided the fifth vote for Justice Scalia's opinion, but supported both Justice Scalia's argument and Justice Alito's argument in her own concurrence.[243] She agreed with Justice Scalia that the *Katz* test augmented, but did not eliminate, the trespass test, which she described as an "irreducible constitutional minimum."[244] But she also agreed with Justice Alito's assessment that long-term warrantless GPS tracking is unreasonable and that the *Katz* rubric is still necessary in the modern world because "physical intrusion is now unnecessary to many forms of surveillance."[245] "In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance."[246]

Justice Sotomayor also cast doubt on "two of the oldest and most criticized doctrines in modern Fourth Amendment jurisprudence": the *Katz* reasonable expectation of privacy test and the third-party doctrine.[247] She said GPS technology is particularly susceptible to government abuse[248] because it "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[249] She also said that the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[250] However, because the particular search at issue in *Jones* could be resolved solely on the basis of the trespass, she said there was no need to decide those issues.[251]

Justice Sotomayor's critique touched on the power of the "mosaic" theory—that is, that law enforcement can glean incredibly revealing knowledge about a person when aggregating bits of data that are individually innocuous, especially with the help of modern

---

241. *Id.* at 428.
242. *Id.* at 427–28.
243. *Id.* at 413–14 (Sotomayor, J., concurring).
244. *Id.* at 413.
245. *Id.* at 413–15.
246. *Id.* at 414–15.
247. Baer, *supra* note 232, at 395.
248. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).
249. *Id.* at 415–16 (citing People v. Weaver, 12 N.Y.3d 433, 441–442 (2009)).
250. *Id.* at 417–18.
251. *Id.* at 413–14.

technologies that go beyond just GPS tracking.[252] One such modern technological tool is "metadata," the bits of digital information that are generated when creating a document or using the internet that the user might not realize are there.[253] For example, metadata in a Microsoft Word document might reveal when it was created, whose computer it was written on, or what edits were made to it.[254] Similarly, browsing the internet can leave traces of metadata, such as email addresses, photos, computer location information, and the like.[255] Like the long-term location tracking at issue in *Jones* and the New York state case *People v. Weaver*,[256] discussed below, such data points can reveal a great deal about a person, especially when aggregated.[257] Even though it can be just as revealing, such metadata typically comes without the legal protections that the contents of communications themselves would have.[258] Metadata from telephone calls, such as who a person calls and when, can reveal sensitive information as readily as the contents of those calls, such as gun ownership or a medical diagnosis.[259] In striking down a vast telephone metadata collection program run by the National Security Agency on statutory grounds in 2015, the Second Circuit noted how the power of metadata combined with the ubiquity of its collection by modern technology means that people "can barely function without involuntarily creating metadata that can reveal a great deal of information about them."[260]

New York, meanwhile, has approached the issue tackled by the split *Jones* ruling in a different way. Confronting similar facts in 2009, New York's highest court found in *People v. Weaver* that its state

---

252. Joshua Vittor, Note, *What Would a Martian Think of Cell Phones? The Third-Party Doctrine and Technological Extensions of the Human Self*, 10 HARV. L. & POL'Y REV. 255, 263 n.48 (2016).

253. ACLU OF CAL., METADATA: PIECING TOGETHER A PRIVACY SOLUTION 3 (2014) [hereinafter METADATA PRIVACY SOLUTION], https://www.aclunc.org/sites/default/files/Metadata%20report%20FINAL%202%2021%2014%20cover%20%2B%20inside%20for%20web%20%283%29.pdf [https://perma.cc/SA3R-S85X].

254. *What is Metadata?*, HARV. LAW SCH., http://hls.harvard.edu/dept/its/what-is-metadata/ [https://perma.cc/Q2L8-U2DT].

255. METADATA PRIVACY SOLUTION, *supra* note 253, at 10.

256. People v. Weaver, 12 N.Y.3d 433, 442 (2009).

257. *Surveillance Self-Defense: Why Metadata Matters*, ELEC. FRONTIER FOUND., https://ssd.eff.org/en/module/why-metadata-matters [https://perma.cc/4FVS-UYTJ].

258. *Id.*

259. *See* Jonathan Mayer et al., *Evaluating the Privacy Properties of Telephone Metadata*, 113 PROC. NAT'L ACAD. SCI. 5539, 5539–40 (2016).

260. ACLU v. Clapper, 785 F.3d 787, 824 (2d Cir. 2015).

constitution prohibited the warrantless GPS tracking of a suspect for sixty-five days.[261]

The court said that GPS technology made the case different than earlier cases about tracking motor vehicles along public roads.[262] In *United States v. Knotts*,[263] the U.S. Supreme Court had held that police use of a "beeper," which transmitted a signal that made it easier for a police car to follow a suspect's car, did not require a warrant because the suspect did not have an expectation of privacy while driving on a public road.[264] But the New York Court of Appeals said that GPS is not a "mere enhancement of human sensory capacity" comparable to a beeper.[265] "GPS is a vastly different and exponentially more sophisticated and powerful technology that is easily and cheaply deployed and has virtually unlimited and remarkably precise tracking capability."[266] Echoing concerns that Justice Sotomayor would later raise in *Jones*, the court warned that law enforcement can use GPS-tracked movements to collect a "breathtaking quality and quantity" of personal information to create "a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits."[267] In light of the differences between beepers and GPS, the court rejected the idea that being on a public roadway negated all expectations of privacy.[268] Such warrantless tracking was therefore prohibited.[269]

However, the court noted that the issue was unsettled in federal law.[270] Rather than relying on any federal precedent, it based its ruling on article I, section 12 of the New York State Constitution, the analogous provision to the Federal Fourth Amendment.[271] The state provision provided greater protection, the court said, and relied on a line of cases on searches and seizures independent from federal law.[272] The court said protecting New Yorkers from unreasonable

---

261. People v. Weaver, 12 N.Y.3d 433, 447 (2009).
262. *See id.* at 440–42.
263. 460 U.S. 276, 285 (1983).
264. *See Weaver*, 12 N.Y.3d at 440–41 (discussing *Knotts*, 460 U.S. 276).
265. *See id.* at 441.
266. *Id.*
267. *Id.* at 442.
268. *See id.* at 443–44.
269. *See id.* at 445.
270. *Id.*
271. *Id.*
272. *See id.*

searches in the face of new technology was more important than aligning state constitutional standards with federal ones.[273]

In dissent, Judge Susan Phillips Read said that it should be the legislature, and not the courts, who regulates such new technology.[274] Judge Read criticized the court's majority for imposing a bright-line rule and "constitutionalizing" GPS.[275] The legislature, she said, can better weigh New Yorkers concerns' with privacy and security, "balance these competing values and fashion a comprehensive regulatory program."[276]

The line the court drew in *Weaver* is not necessarily brighter than the one the multiple opinions of the U.S. Supreme Court tried to draw in *Jones*: subsequent decisions have had to deal with other applications of *Weaver*. For example, in 2013 the New York Court of Appeals found that a state agency did not need to obtain a warrant before attaching a GPS device to an employee's car to investigate whether a state employee was falsifying time sheets because such a search fell into a "workplace" exception to the warrant requirement.[277] But the search was still unconstitutionally unreasonable because the State did not limit its search to business hours.[278] Also in 2013, a trial court judge found that "pinging" a suspect's cell phone to determine his current location without a warrant was permitted under both *Jones* and *Weaver*.[279] In 2017, a state trial judge suggested that other types of location-tracking technology required warrants under *Weaver*.[280]

C. Tracking Real-Time and Historical Location Using Cell Phones

In addition to GPS devices, law enforcement can also track a person's location using a cell phone.[281] When a person's cell phone is

---

273. *Id.*

274. *Id.* at 457–59 (Read, J., dissenting).

275. *Id.* at 459.

276. *Id.* at 458–59 (Read, J., dissenting). *But see id.* at 446 (majority opinion) ("Nothing prevents the Legislature from acting to regulate the use of GPS devices within constitutional limits, but, we think it manifest that the continuous GPS surveillance and recording by law enforcement authorities of the defendant's every automotive movement cannot be described except as a search of constitutional dimension and consequence.").

277. Cunningham v. N.Y. State Dep't of Labor, 21 N.Y.3d 515, 521 (2013).

278. *Id.* at 521–23.

279. People v. Moorer, 959 N.Y.S.2d 868, 876–81 (N.Y. Cty. Ct. 2013).

280. People v. Gordon, 68 N.Y.S.3d 306, 308–11 (N.Y. Sup. Ct. 2017) (cell-site simulators); *see also* discussion *infra* Section II.C.

281. *See* Robinson Meyer, *How the Government Surveils Cellphones: A Primer*, THE ATLANTIC (Sept. 11, 2015), https://www.theatlantic.com/technology/archive/

on, it reveals its approximate location by periodically pinging nearby cell phone towers.[282] The cellular phone company stores that data.[283] The third-party doctrine has meant that law enforcement can easily obtain historical location data collected by cell phones (cell-site location information or "CSLI").[284] Under the Federal Stored Communications Act, instead of using an ordinary subpoena that can be obtained without the showing of probable cause required for a warrant, law enforcement must show "reasonable grounds" to obtain CSLI.[285] Some state laws require law enforcement to obtain a warrant to access the historical CSLI that is created by this process and stored by cellular phone companies.[286] But because the CSLI is voluntarily given by the person's cell phone to the cellular phone company, the third-party doctrine places it outside the Fourth Amendment protections in federal cases.[287]

Five federal circuit courts have held that the third-party doctrine applies to CSLI—but only after "generat[ing] 18 separate majority, concurring, and dissenting opinions" that "attempt[] to grapple with the same basic issue."[288] One of those courts, the Sixth Circuit, held that the third-party doctrine meant that the police did not need a warrant to obtain 127 days' worth of CSLI about a robbery suspect.[289] A host of different groups, including libertarian groups,[290] defense

---

2015/09/how-the-government-surveils-cell-phones-a-primer/404818/ [https://perma.cc/HMC8-ZYNL].

282. *See* Robinson Meyer, *This Very Common Cellphone Surveillance Still Doesn't Require a Warrant*, THE ATLANTIC (Apr. 14, 2016), https://www.theatlantic.com/technology/archive/2016/04/sixth-circuit-cellphone-tracking-csli-warrant/478197/ [https://perma.cc/NGJ6-VWD4].

283. *See* Meyer, *supra* note 281.

284. *See* Meyer, *supra* note 282.

285. 18 U.S.C. § 2703(d) (2012); *see* United States v. Davis, 785 F.3d 498, 505–06 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015); *see also* United States v. Graham, 824 F.3d 421, 437 (4th Cir. 2016) (explaining that Congress struck a balance following *Smith* in the Stored Communications Act by requiring higher requirements for law enforcement to view the contents of certain electronic communications collected by companies).

286. *See Cell Phone Location Tracking Laws by State*, ACLU, https://www.aclu.org/map/cell-phone-location-tracking-laws-state [https://perma.cc/946M-ZCW5].

287. *See* Meyer, *supra* note 282.

288. *See* Petition for Writ of Certiorari for Defendant-Petitioner at 13–15, Carpenter v. United States, 137 S. Ct. 2211 (2017) (No. 16-402), 2016 WL 5462796, at *13–15.

289. United States v. Carpenter, 819 F.3d 880, 884–87 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

290. *See* Brief for Competitive Enter. Inst. et al. as Amici Curiae in Support of Petitioner, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-

attorneys,[291] scholars,[292] journalists,[293] technology companies,[294] technology experts,[295] privacy advocates,[296] and others urged the U.S. Supreme Court to hear an appeal of the Sixth Circuit's ruling, while law enforcement groups[297] and others[298] argued that the decision

---

content/uploads/2017/08/16-402-tsac-competitive-enterprise-inst.pdf [https://perma.cc/2XT5-4AXB].

291. *See* Brief of Amici Curiae Elec. Frontier Found. et al. in Support of Petitioner, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2016/11/16-402-cert-amicus-EFF.pdf [https://perma.cc/8UCU-HG3W].

292. *See, e.g.*, Brief of Scholars of Criminal Procedure & Privacy as Amici Curiae in Support of Petitioner, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2017/08/16-402-tsac-Scholars-of-Criminal-Procedure-and-Privacy.pdf [https://perma.cc/H9VU-GHGP]; *see also* Brief of Scholars of the History & Original Meaning of the Fourth Amendment as Amici Curiae in Support of Petitioner, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2017/08/16-402-tsac-ScholarsOfThe HistoryAnd-OriginalMeaning.pdf [https://perma.cc/D9RT-NG8H].

293. *See* Brief Amici Curiae of the Reporters Comm. for Freedom of the Press & 19 Media Orgs. in Support of Petitioner, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2017/08/16-402_tsac_reporters_committee_for_freedom_of_the_press.pdf [https://perma.cc/XP6G-FDPJ].

294. *See* Brief for Tech. Cos. as Amici Curiae in Support of Neither Party, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2017/08/16-402-ac-technology-companies.pdf [https://perma.cc/K8WE-SD5E] (including Airbnb, Apple, Facebook, Google, Microsoft, Verizon, and nine others).

295. *See* Brief of Tech. Experts as Amici Curiae in Support of Petitioner, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2017/08/16-402-tsac-technology-experts.pdf [https://perma.cc/33TT-ZCFQ].

296. *See, e.g.*, Brief of Amicus Curiae the Rutherford Inst. in Support of Petitioner, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2017/08/16-402-tsac-rutherford-inst.pdf [https://perma.cc/ZHZ8-XFW2]; Brief of the Ctr. for Democracy & Tech. as Amicus Curiae in Support of Petitioner, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2017/08/16-402-tsac-democracy-and-technology.pdf [https://perma.cc/3SJL-XS8Q]; Brief of Amici Curiae Elec. Privacy Info. Ctr. (EPIC) & Thirty-Six Technical Experts & Legal Scholars in Support of Petitioner, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2017/10/Carpenter-v-US-amicus-EPICtsac16-402.pdf [https://perma.cc/6VD4-2LQP].

297. *See* Brief for the States of Alabama, Arizona, Colorado, Florida, Idaho, Indiana, Kansas, Kentucky, Maryland, Michigan, Montana, Nebraska, New Hampshire, New Mexico, Oklahoma, Pennsylvania, South Carolina, Tennessee, & Wyoming as Amici Curiae in Support of Respondents, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2017/10/16-402-bsac-states-of-alabama.pdf [https://perma.cc/4QKW-7UYV]; Amicus Curiae Brief for Nat'l Dist. Attorneys Ass'n in Support of Respondent, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2017/10/16-402-bsac-ndaa.pdf [https://perma.cc/5QEP-RPNF].

298. *See* Brief of Professor Orin S. Kerr as Amicus Curiae in Support of Respondent, *Carpenter*, No. 16-402 (U.S. Aug. 14, 2017), http://www.scotusblog.com/wp-content/uploads/2017/10/16-402-bsac-Orin-Kerr.pdf [https://perma.cc/9BAA-LQ8S] (scholar); Brief of Amicus Curiae Michael Varco in Support of Respondent,

should stand. The U.S. Supreme Court has decided to hear that appeal, *Carpenter v. United States*,[299] and possibly resolve the CSLI issue. The justices' questions during oral arguments suggested, commentators said, that a majority wanted to somehow limit the government's power to collect CSLI without a warrant, but had little idea how to do so.[300] "[T]his is an open box," Justice Stephen Breyer remarked, "[w]e know not where we go."[301] Any changes the Court might make in *Carpenter* to the third-party doctrine could have implications for issues as diverse as revenge porn, medical records, and National Security Agency programs.[302]

No matter how *Carpenter* ultimately comes out, it involves CSLI obtained from cellular phone companies—but law enforcement can collect real-time location information from a cell phone itself without going through those companies.[303] One of the more controversial methods is with devices called cell-site simulators or sometimes by the trade name "Stingrays."[304] The briefcase-sized device surreptitiously mimics a cell phone tower, "pinging" nearby devices to collect data from them, such as their location and even what numbers they have

---

Carpenter, 137 S. Ct. 2211 (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2017/10/16-402-bsac-varco.pdf [https://perma.cc/7DAZ-T9DN] (victim).

299. 819 F.3d 880, 884–87 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

300. *See, e.g.*, Robert Barnes, *Justices Appear to Favor More Restraints on Government Access to Digital Information*, WASH. POST (Nov. 29, 2017), https://www.washingtonpost.com/politics/courts_law/justices-appear-to-favor-more-restraints-on-access-to-digital-information/2017/11/29/5f7aaae2-d499-11e7-b62d-d9345ced896d_story.html [https://perma.cc/R8W3-RQJ4]; Tony Mauro, *Justices Fret Over Access to Cellphone Data in Key Privacy Case*, NAT'L L.J. (Nov. 29, 2017), https://www.law.com/nationallawjournal/sites/nationallawjournal/2017/11/29/justices-fret-over-access-to-cellphone-data-in-key-privacy-case/ [https://perma.cc/W2RX-ZJAK]; Greg Stohr, *Supreme Court Justices Hint at More Digital-Privacy Protection*, BLOOMBERG (Nov. 29, 2017), https://www.bloomberg.com/news/articles/2017-11-29/supreme-court-justices-hint-at-new-digital-privacy-protections [https://perma.cc/TME6-CPFY]; *The Supreme Court's Justices Want to Enhance Privacy Protections for a Digital Age*, ECONOMIST (Nov. 30, 2017), https://www.economist.com/news/united-states/21731880-carpenter-v-united-states-shows-they-are-unsure-about-how-do-so-supreme-courts [https://perma.cc/XK3B-BVB5].

301. Transcript of Oral Argument at 34, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), 2017 WL 5890155, at *34.

302. *See* Isabella McKinley Corbo, *Your Digital Privacy Rights Will Be Redefined by This Supreme Court Case*, VICE NEWS (Nov. 28, 2017), https://news.vice.com/story/impact-of-supreme-court-case-carpenter-v-u-s [https://perma.cc/4HYQ-FJ7D].

303. *See* Meyer, *supra* note 281 (describing various technologies and law enforcement methods of collecting CSLI).

304. *Id.*

dialed.[305] The mock cell phone towers also collect information from nearby non-suspects whose phones are also pinged.[306] Federal law enforcement has also deployed similar devices in airplanes, vastly increasing their range.[307]

The technology was largely secret for years.[308] Law enforcement agencies worked hard to hide information about their cell-site simulators from defense attorneys, judges, and the public, going so far as to drop cases instead of reveal the technology[309] or even lying to judges.[310] After more information came to light about law enforcement use of the devices, federal policy changed[311] to require federal law enforcement to seek a warrant before using a cell-site simulator.[312] State law enforcement agencies, however, are not bound by the federal policy.[313] The NYPD used cell-site simulators more than 1000 times between 2008 and 2015,[314] but did not acknowledge that it used the devices until 2016.[315] The New York Civil Liberties

---

305. *See Cell Site Simulators Primer*, NAT'L ASS'N OF CRIMINAL DEF. LAWYERS, https://www.nacdl.org/fourthamendment [https://perma.cc/5AP5-D79T] (click on hyperlink labeled "Cell Site Simulators Primer").

306. *Id.*

307. *See* Devlin Barrett, *Airplanes Secretly Track U.S. Cellphones*, WALL ST. J. (Nov. 14, 2014), https://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533 [https://perma.cc/8TT3-3CEL].

308. *See* Cyrus Farivar, *'PING SUSP PHONE'—An Oakland Shooting Reveals How Cops Snoop on Cell Phones*, ARS TECHNICA (Aug. 6, 2015), https://arstechnica.com/tech-policy/2015/08/ping-susp-phone-an-oakland-shooting-reveals-how-cops-snoop-on-cell-phones/ [https://perma.cc/4Q2T-KJ22].

309. *See* ADAM BATES, CATO INST., POLICY ANALYSIS NO. 809, STINGRAY: A NEW FRONTIER IN POLICE SURVEILLANCE 6–9, 13 (2017), https://object.cato.org/sites/cato.org/files/pubs/pdf/pa-809-revised.pdf [https://perma.cc/3UXE-9JF8].

310. *See* Cyrus Farivar, *Legal Experts: Cops Lying About Cell Tracking "Is a Stupid Thing to Do,"* ARS TECHNICA (June 20, 2015, 12:30 PM), https://arstechnica.com/tech-policy/2014/06/legal-experts-cops-lying-about-cell-tracking-is-a-stupid-thing-to-do [https://perma.cc/DY57-CFUN].

311. *See generally* Farivar, *supra* note 308.

312. U.S. DEP'T OF JUSTICE, DEP'T OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 3–4 (2015), https://www.justice.gov/opa/file/767321/download [https://perma.cc/67DB-J8BS].

313. *See* Meyer, *supra* note 281.

314. *See* Press Release, N.Y. Civil Liberties Union, NYPD Has Used Stingrays More Than 1,000 Times Since 2008 (Feb. 11, 2016), https://www.nyclu.org/en/press-releases/nypd-has-used-stingrays-more-1000-times-2008 [https://perma.cc/J7HG-22XE].

315. *See* Alex Emmons, *New York Police Have Used Stingrays Widely, New Documents Show*, THE INTERCEPT (Feb. 11, 2016), https://theintercept.com/2016/02/11/new-york-police-have-used-stingrays-widely-new-documents-show/ [https://perma.cc/C8RW-9U2U].

Union has sued for more information about how much money the department spends on the devices.[316]

Now that more is known about how such devices are used, some courts have also pushed back: a New York state judge,[317] the District of Columbia Court of Appeals,[318] a Maryland appeals court,[319] and some federal district courts[320] have found that law enforcement must obtain a warrant before using a cell-site simulator. Courts have noted that historical cell site data, which the government obtains from a cell phone company that is voluntarily storing it through the third-party doctrine, is different from a cell-site simulator—rather than getting location data that someone else collected, cell-site simulators actively send signals to a cell phone to force it to reveal its location.[321]

D. Tracking Location Using Facial Recognition Technology

Other location-tracking features made possible by the kiosks—notably, increasingly sophisticated facial recognition technology—face an even more uncertain reception in the courts than other types of location data.

Facial recognition technology, also made possible by LinkNYC, adds a new dimension to the case law. Long within the realm of science fiction, facial recognition is now technologically feasible.[322] Camera software can analyze a face plucked out from a crowd and compare it to a database of photos to identify that person.[323] Courts have held that cameras in public places can collect images with little to no restrictions—even if trained toward private property—because

---

316. *See* Verified Petition, N.Y. Civil Liberties Union v. N.Y. Police Dep't, No. 100788/2016 (N.Y. Sup. Ct. May 19, 2016), https://www.nyclu.org/sites/default/files/releases/Stingrays_verified_petition.pdf [https://perma.cc/T6GQ-2HFX].

317. People v. Gordon, 68 N.Y.S.3d 306, 310–11 (N.Y. Sup. Ct. 2017).

318. Jones v. United States, 168 A.3d 703, 707 (D.C. 2017).

319. *See* State v. Andrews, 134 A.3d 324, 350 (Md. 2016). *But see* State v. Copes, 165 A.3d 418, 439 (Md. 2017) (declining to review the reasoning in *Andrews* because of, among other things, the pending *Carpenter* case).

320. *See, e.g.*, United States v. Ellis, 270 F. Supp. 3d 1134, 1149–50, 1153 (N.D. Cal. 2017) (finding that using a cell-site simulator generally requires a warrant, but that exigent circumstances existed in the case to excuse the police from seeking one).

321. *See* United States v. Lambis, 197 F. Supp. 3d 606, 615–16 (S.D.N.Y. 2016); *see also Gordon*, 68 N.Y.S.3d at 310–11.

322. FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES, at i (2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf [https://perma.cc/W6QG-VLY3].

323. *See id.* at 3–4.

there is no reasonable expectation of privacy in video footage "that recorded the same views enjoyed by passersby on public roads."[324]

For individual recognition, facial recognition technology must be able to compare the images it captures to other images stored in a database.[325] Similar technology is used in automated license-plate readers, which take photographs of cars' license plates, convert those photographs into data that can be read by a computer, and then compare them to a database of license plates.[326] Both federal and New York state courts have said that the Fourth Amendment is not implicated when a police officer searches for a license plate number in a government database,[327] suggesting that an automated query by a license-plate reader—or facial recognition software—might also be permissible. But the mass, automated collection of people's movements through the license plate reader technology could also be so broad that it violates the *Weaver* court's prohibition on such massive collection of location data.[328]

Yet there is no state or federal statute governing the use of facial recognition technology by law enforcement.[329] Some states do, however, have laws that restrict the use of biometric data, like facial

---

324. United States v. Houston, 813 F.3d 282, 287–90 (6th Cir. 2016), *cert. denied*, 137 S. Ct. 567 (2016); *see also* People v. Bauer, 528 N.Y.S.3d 153, 153–54 (N.Y. App. Div. 1988) (holding that police can take photographs of people in public spaces without a warrant).

325. *See* FED. TRADE COMM'N, *supra* note 322, at 3–4.

326. NAT'L ASS'N OF CRIMINAL DEF. LAWYERS, AUTOMATED LICENSE PLATE READERS 1–2 (2016), https://www.nacdl.org/uploadedFiles/files/criminal_defense/fourth_amendment/2016-4-28_ALPR%20Primer_Final.pdf [https://perma.cc/EUT8-LGU7].

327. *See, e.g.*, United States v. Miranda-Sotolongo, 827 F.3d 663, 668 (7th Cir. 2016) (finding that entering a license plate number, which was in plain view in public, into a database of license plate numbers did not violate the Fourth Amendment); United States v. Ellison, 462 F.3d 557, 563 (6th Cir. 2006) (same); People v. Bushey, 75 N.E.3d 1165, 1169 (N.Y. 2017) (finding that such a search was neither a violation of the Fourth Amendment nor of the New York State Constitution). *But see Ellison*, 462 F.3d at 567–72 (Moore, J., dissenting) (arguing that suspicionless searches of computer databases are "in tension" with other Fourth Amendment concerns).

328. People v. Weaver, 12 N.Y.3d 433, 446 (2009) ("[D]ragnet use of the [GPS] technology at the sole discretion of law enforcement authorities to pry into the details of people's daily lives is not consistent with the values at the core of our State Constitution's prohibition against unreasonable searches."). *But see id.* at 460 n.1 (Smith, J., dissenting) ("This case . . . involves the use of GPS monitoring technology in the criminal investigation of an individual suspect, not dragnet-type or mass surveillance.").

329. "[T]here are currently no New York or federals laws, and no generally accepted scientific standards, controlling the use of facial recognition by law enforcement." Memorandum of Law in Support of Verified Petition at 1, Ctr. of Privacy & Tech. v. N.Y.C. Police Dep't, No. 154060/2017 (N.Y. Sup. Ct. May 2, 2017).

recognition technology, by private companies.[330] But what should the law say about facial recognition? Tort laws about privacy have been criticized as inadequate to deal with facial recognition technology.[331] Meanwhile, law enforcement is expanding its use of people's images in databases: sixteen states let the Federal Bureau of Investigation access their databases of driver's license photos to use in its own facial recognition software.[332] As many as thirty states allow facial recognition searches of some kind of their databases.[333] The technology is not always that effective: the FBI itself has acknowledged that it identifies the wrong person twenty percent of the time.[334]

The NYPD had been tight-lipped about its use not only of facial recognition technology[335] but also of other technological policing tools like predictive policing software.[336] LinkNYC's current privacy policy states that it will not use facial recognition technology.[337] But without legal standards, law enforcement is free to use facial

---

330. *See* Illinois Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15(a) (2008); *see also* Conor Dougherty, *Push for Internet Privacy Rules Moves to Statehouses*, N.Y. TIMES (Mar. 26, 2017), https://www.nytimes.com/2017/03/26/technology/internet-privacy-state-legislation-illinois.html [https://nyti.ms/2mFfAVU].

331. *See* AJ McClrug, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1875–80 (2007).

332. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY & ACCURACY 50 (2016).

333. *See* CLARE GARVIE ET AL., GEORGETOWN LAW CTR. ON PRIVACY & TECH., THE PERPETUAL LINE-UP 2 (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/9BM3-NQM6].

334. GAO-16-267, *supra* note 332, at 26–27.

335. Verified Petition & Complaint at 2, Ctr. of Privacy & Tech. v. N.Y.C. Police Dep't, No. 154060/2017 (N.Y. Sup. Ct. May 2, 2017) (request under state freedom of information law for documents about NYPD's use of facial recognition technology). The NYPD later agreed to release some documents. *See* So Ordered Stipulation of Adjournment at 2, *Ctr. of Privacy & Tech.*, No. 154060/2017 (N.Y. Sup. Ct. Feb. 28, 2018).

336. *See* Memorandum of Law in Support of Verified Petition at 13, Brennan Ctr. for Justice at N.Y. Univ. Sch. of Law v. N.Y.C. Police Dep't, No. 160541/2016 (N.Y. Sup. Ct. Dec. 15, 2016) (request under state freedom of information law for documents about NYPD's use of predictive policing technology after its "egregious" refusal to provide relevant documents). A state judge later ordered the NYPD to produce some of the documents. *See* Decision & Judgment at 15, *Brennan Ctr. for Justice*, No. 160541/2016 (N.Y. Sup. Ct. Dec. 27, 2017).

337. March 2017 LinkNYC Privacy Policy, *supra* note 190, at 6.

recognition technology wherever it has access to cameras without taking precautions to protect privacy.[338]

E. Judges and the Public Have Different Ideas About Privacy

While courts grabble over what is a "reasonable expectation of privacy" in the digital age, the public has its own ideas. For example, many people are willing to freely hand over their personal information if they receive a valuable service in return, despite concerns raised by LinkNYC and other modern technology.[339] Indeed, New York and CityBridge trumpeted the more than one million users who logged into the LinkNYC network in its first year and the seventy-eight percent of New Yorkers who had a favorable view of the network.[340] LinkNYC reached those milestones before the newer, less-intrusive privacy policy was rolled out. But overall, the public is divided over how to balance privacy and the disclosure of their personal information.[341]

Like the public, judges themselves do not always agree on what is "reasonable." The split *Jones* and *Weaver* courts, the conflicting ways cell-site location data is treated, and the uncertainty of new, emerging technologies like facial recognition highlight this judicial divide. Academics have argued over what factors judges should consider—such as public views—in a "reasonableness" analysis.[342] Judges have also critiqued each other's views on the subject. In *Jones*, Justice Sotomayor took issue with what Justice Alito speculated people would consider a reasonable tradeoff when sacrificing privacy for convenience.[343] Indeed, what privacy

---

338. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-489T, FACE RECOGNITION TECHNOLOGY: DOJ & FBI NEED TO TAKE ADDITIONAL ACTIONS TO ENSURE PRIVACY & ACCURACY 7–11 (2017).

339. LEE RAINIE & MAEVE DUGGAN, PEW RESEARCH CTR., PRIVACY & INFORMATION SHARING 2 (2016), http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf [https://perma.cc/G2AR-MLHG].

340. *See* One Million Users Press Release, *supra* note 148.

341. RAINIE & DUGGAN, *supra* note 339, at 2–3 ("[T]he phrase that best captures Americans' views on the choice between privacy vs. disclosure of personal information is, 'It depends.' People's views on the key tradeoff of the modern, digital economy—namely, that consumers offer information about themselves in exchange for something of value—are shaped by both the conditions of the deal and the circumstances of their lives.").

342. *See generally* Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. 1, 18–22 (2011) (discussing the debate over whether the severity of the charged crime should be considered when deciding if a search is reasonable); Kerr, *supra* note 214.

343. *See* United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring).

limitations are people prepared to recognize as "reasonable"? As Justice Alito noted, courts often substitute their own idea of reasonableness for that of "the hypothetical reasonable person."[344] Is there a difference between the judgment of a "reasonable person" and that of a judge?

There is a danger in drawing bright lines on particular technologies and locking in a judicial rule[345]: public views about privacy often do not align with the hard rules courts have laid down.[346] Several attempts have been made to empirically study what people would actually consider reasonable expectations of privacy.[347] One recent study found people believed that the police should obtain a warrant before searching a suspect's cell phone.[348] The Supreme Court has agreed that this expectation is reasonable—when the search is incident to arrest.[349] But people also believed that the police should obtain a warrant before accessing cell phone data from cellular towers.[350] Federal circuit courts have found the opposite.[351]

---

344. *Id.* at 427 (Alito, J., concurring).

345. *See* People v. Weaver, 12 N.Y.3d 433, 458–59 (2009) (Read, J., dissenting) ("Police surveillance techniques implicate competing values of great importance to all New Yorkers—privacy and security. Absent this decision, our Legislature would have been in a position to . . . balance these competing values and fashion a comprehensive regulatory program . . . readily capable of amendment as the science evolves.").

346. *See* Christine S. Scott-Hayward et al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 58 (2015); *see also* Brief of Amici Curiae Empirical Fourth Amendment Scholars in Support of Petitioner at 10, Carpenter v. United States, 137 S. Ct. 2211 (2017) (No. 16-402), http://www.scotusblog.com/wp-content/uploads/2017/08/16-402-tsac-emprical-fourth-amendment-scholars.pdf [https://perma.cc/B4NU-7GGG] (noting that even though studies have indicated that more than sixty percent of people believed they had a privacy interest in the information that their cell phones store or transmit, courts have held that they give up that privacy interest under the third-party doctrine when the information is shared with cellular phone companies).

347. *See* Alisa Smith et al., *An Empirical Examination of Societal Expectations of Privacy in the Digital Age of GPS, Cell Phone Towers & Drones*, 26 ALB. L.J. SCI. & TECH. 111, 112–13 (2016); *see also* Henry F. Fradella et al., *Quantifying* Katz*: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 293 (2011); Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 522 (2012). *See generally* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727 (1993).

348. *See* Smith et al., *supra* note 347, at 134.

349. *See* Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

350. *See* Smith et al., *supra* note 347, at 133–34.

Still, people's views on the privacy-convenience tradeoff depend on the particular technology and data at issue, and who is looking at it. A Pew Research Center study found that in commercial settings, people view the collection of location data taken from their cell phones more negatively than other types of data gathering.[352] Many people said that they did not like it when their data is collected for one purpose but then "used for other, often more invasive purposes."[353] Study participants also said they were frustrated by "how hard they feel it is to get information about what is collected and uncertainty about who is collecting the data" and wanted data collection to be controlled through legal and technological means.[354] Another study conducted by Professor Christopher Slobogin asked participants about how intrusive they viewed various types of searches subject to different levels of Fourth Amendment protection and compared those findings to how intrusive they viewed a public network of police cameras spaced 300 yards apart from each other with the ability to zoom in and out.[355] Survey respondents said the camera network was more intrusive than a police vehicle checkpoint or roadblock, which the U.S. Supreme Court has held is a search requiring a warrant.[356] Professor Slobogin's other surveys have also shown that government searches of people's internet activity and transactions with their banks and pharmacies "are perceived to be as intrusive as a search of a car."[357]

How then to thread the needle between people's views of what they want kept private and courts' struggle to understand the privacy implications of new technologies? As Judge Read noted in her

---

351. *See* discussion *supra* Section II.C.

352. *See* RAINIE & DUGGAN, *supra* note 339, at 5 ("Some of the most strongly negative reactions came in response to scenarios involving the sharing of personal location data.").

353. *Id.* at 6.

354. *Id.* at 7.

355. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 275–77 (2002).

356. *Id.* at 278 (citing United States v. Martinez-Fuerte, 428 U.S. 543, 556 (1976)).

357. Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 2010 MINN. L. REV. 1588, 1593 (2012) (describing several such surveys the author has conducted). *But see* Orin Kerr, *Answering Justice Alito's Question: What Makes an Expectation of Privacy 'Reasonable'?*, WASH. POST (May 28, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/28/answering-justice-alitos-question-what-makes-an-expectation-of-privacy-reasonable [https://perma.cc/N5FB-TT98] ("[T]he nature of the *Katz* "reasonable expectation of privacy" inquiry is normative, not descriptive: The Court says what is a search. What reasonable people actually expect to happen as an empirical matter is not part of the test, except in some very limited ways.").

Weaver dissent, New Yorkers deserve "the full benefit of the carefully wrought balance between privacy and security interests."[358] Courts may one day strike that balance. But in the meantime, local legislatures and agencies can make those decisions today.

III. NEW YORK CITY CAN USE ITS CONTRACTING POWERS TO PROTECT PRIVACY IN THIRD-PARTY SMART CITY SERVICES SUCH AS LINKNYC

New York City's much-praised goals with the LinkNYC project—closing the digital divide and making New York a smart city—stand in tension with the privacy concerns that continue to swirl around the kiosks.[359] The LinkNYC kiosks combine into a single service the possibility of tracking a New Yorker's current location, analyzing their activity with their historical movements, and even using facial recognition to track people who never even logged in to the kiosk. Therefore, if left to the courts, the kiosks' historical location data (if collected) could be available to the police or might face a new test after the *Carpenter* case over CSLI. The kiosks' ability, albeit unused, to utilize facial recognition technology is untested by the courts. Even the kiosks' GPS tracking abilities would be subject to the divided reasoning of *Jones* and the unclear implications of *Weaver*—if, that is, those cases would even apply to LinkNYC because of its different mechanisms for tracking people.[360] Furthermore, despite the changes to the LinkNYC privacy policy, much discretion is still left to the private companies to change the policy, and there is no way to challenge them if they violate it.[361] If New Yorkers do not know what information the kiosks are even collecting, it is difficult to challenge that collection in court.[362] And

---

358. People v. Weaver, 12 N.Y.3d 433, 458–60 (2009) (Read, J., dissenting).

359. *Cf.* Gina Bellafante, *The Watchmen's Misdirected Gaze*, N.Y. TIMES: BIG CITY (Aug. 18, 2012), http://www.nytimes.com/2012/08/19/nyregion/the-watchmens-misdirected-gaze.html [https://perma.cc/Z5TD-968J] (noting that low-income people in a high-crime area wanted more video surveillance of their neighborhood to deter crime; "[p]rivacy debates surrounding this kind of surveillance are to a great extent the privilege of the better off").

360. Those cases involved "the use of GPS monitoring technology in the criminal investigation of an individual suspect, not dragnet-type or mass surveillance." *See Weaver*, 12 N.Y.3d at 452 n.1.

361. Buttar & Kalia, *supra* note 175.

362. *Compare* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401–02 (2013) (no standing to challenge Foreign Intelligence Surveillance Act because potential injury too speculative), *with* ACLU v. Clapper, 785 F.3d 787, 801–02 (2d Cir. 2015) (standing established after existence of National Security Agency metadata collection program revealed).

even if the use of a surveillance technology can be challenged, courts are still befuddled by contemporary expectations of privacy and are sometimes at odds with public opinion.[363] With the judicial goalposts still shifting, local legislatures and agencies can protect privacy in networks they oversee, such as LinkNYC, while the issues percolate in the courts and the technology develops.

A. Legislative Responses Can Protect Privacy While Courts Mull Issues

In the court decisions grappling with GPS tracking, several judges noted that legislatures are better suited to resolve these issues than the courts. In *Jones*, Justice Alito said that legislatures are better situated to understand public attitudes about privacy, make tradeoff decisions, and fashion comprehensive regulation among conflicting interests.[364] "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative," he wrote.[365] In her dissent from the New York Court of Appeals decision about warrantless GPS tracking, Judge Read also called on the court to let the legislature act.[366] New York's legislature can fashion a legislative scheme that balances privacy and security, she said, just like many other state legislatures have done.[367]

Commentators are divided over whether courts or legislatures are the appropriate place to regulate electronic surveillance, including technology such as wiretaps, video cameras, and data collection.[368] Legislative approaches have tended to be more protective of privacy, comprehensive in their regulation of the data collected, and flexible to changing technology.[369] The judiciary, others argue, is less susceptible to law enforcement and industry capture, and courts could regulate surveillance more aggressively simply if they chose to.[370]

---

363. *See* discussion *supra* Section II.E.

364. United States v. Jones, 564 U.S. 400, 429–30 (2012).

365. *Id.* (citing Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805–06 (2004)).

366. People v. Weaver, 12 N.Y.3d 433, 458–60 (2009) (Read, J., dissenting).

367. *Id.* at 458–59.

368. *See* Christopher Slobogin, *Legislative Regulation of Surveillance*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 596, 605–06 (David Gray & Stephen E. Henderson eds., 2017).

369. *See id.* at 606–07 (citing Kerr, *supra* note 365).

370. *See id.* at 607–10 (citing Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747 (2005); Peter P. Swire, Katz *is Dead, Long Live* Katz, 102 MICH. L. REV. 904, 922 (2004); Erin Murphy, *The Politics of Privacy in the Criminal Justice System:*

Federal considerations are also different and often, like judicial decisions, merely set a regulatory floor above which states and local governments can regulate.[371] Indeed, most police surveillance is done by local law enforcement, so a national scheme might not make sense.[372] "Surveillance that impinges solely on a particular locale, such as city-wide cameras systems, is probably best handled through municipal ordinances."[373]

Administrative rulemaking processes are another avenue to regulate surveillance by forcing public participation and an explicit weighing of pros and cons.[374] In 2015, the New York Court of Appeals reaffirmed the power of city agencies to engage in rulemaking within their area of expertise that "fills in the details" left by legislation, as long as the agency is not doing its own policymaking.[375] A group of taxicab owners had challenged regulations from the city's Taxi and Limousine Commission mandating a particular make and model of car for use as iconic yellow taxis because the commission allegedly acted outside of the authority granted by the city council.[376] But the court said the regulations were within the agency's "extremely broad authority to enact rules" for the city's taxis under the city charter because it balanced different groups' concerns, did not regulate an area the city had failed to legislate, and acted within the limits set by the city council.[377]

Much like the Taxi and Limousine Commission, the city's charter gives the DoITT broad powers "to plan, formulate, coordinate and advance information technology and telecommunications policies for

---

Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions, 111 MICH. L. REV. 485, 536–39 (2013)).

371. *See id.* at 611–12.

372. *See id.* at 612–14.

373. *Id.* at 613–14. *Cf.* Sylvain, *supra* note 48, at 836–38 (arguing that broadband networks created by local governments encourage competition among industry incumbents, promote local accountability, provide room for experimentation of different models, and help close the digital divide).

374. Slobogin, *supra* note 368, at 615; *see also* Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 134–52 (2016) (arguing that administrative law principles should be used to oversee the NYPD's Domain Awareness System).

375. Greater N.Y. Taxi Ass'n v. N.Y.C. Taxi & Limousine Comm'n, 36 N.E.3d 632, 636–37, 640 (N.Y. 2015).

376. *Id.* at 636.

377. *Id.* at 638. The New York Court of Appeals has also struck down city agencies' attempts to regulate without the benefit of a legislative scheme. *See, e.g.*, N.Y. Statewide Coal. of Hispanic Chambers of Commerce v. N.Y.C. Dep't of Health & Mental Hygiene, 16 N.E.3d 538, 546–50 (N.Y. 2014) (striking down an agency's ban on certain types of sugary drinks).

the city."[378] Those powers extend to payphone and other franchise agreements,[379] such as LinkNYC, and "to ensur[ing] security for data and other information handled by this department,"[380] among other duties.[381] Its decisions have been reviewed by courts[382] and, like the Taxi and Limousine Commission, it cannot act beyond the powers granted to it by the charter and city council.[383] But there is room to act within those limits: DoITT can fill in gaps left by the city council in a statute.[384] DoITT has the power not only to grant payphone franchises, but to consider the impact of the payphones on the community.[385] A court reviewing a DoITT action within its statutory authority will not disturb it as long as the agency decision was rational.[386]

Both city and state lawmakers have shown an interest in regulating in this area. At the time that the LinkNYC program was first proposed, concerns focused mostly on the digital divide. In 2014, the city's borough presidents worried that the then-proposed LinkNYC would not do enough to bridge the digital divide because kiosks would be concentrated disproportionately in wealthier neighborhoods where advertising revenues are higher.[387] The proposal was subsequently altered to deploy more kiosks in boroughs outside Manhattan than had been planned in earlier proposals (although some lawmakers were still disappointed with the rollout).[388]

---

378. N.Y. CITY CHARTER § 1072(a) (2004).

379. *Id.* § 1072(c).

380. *Id.* § 1072(n).

381. *See generally id.* § 1072.

382. *See, e.g.*, Dianet Commc'ns, LLC v. Franchise & Concession Review Comm. of City of N.Y., No. 107805/08, 2008 WL 5490948, at *1–2 (N.Y. Sup. Ct. Dec. 18, 2008) (upholding DoITT's award of a payphone franchise following a request for proposals process).

383. *Compare* Verizon N.Y., Inc. v. Envtl. Control Bd. of City of N.Y., 892 N.Y.S.2d 84, 85 (N.Y. App. Div. 2009) (finding that a DoITT regulation conflicted with its authorizing statute), *with* Coastal Commc'n Serv., Inc. v. N.Y.C. Dep't of Info. Tech. & Telecomm., No. 112312/05, 2006 WL 1879115, at *4 (N.Y. Sup. Ct. July 5, 2006), *aff'd*, 843 N.Y.S.2d 23 (N.Y. App. Div. 2007) (upholding a DoITT regulation as within the powers granted to it by statute).

384. "Although the local law does not expressly authorize the challenged regulation, an agency may adopt a regulation that goes beyond the text of the enabling legislation so as to 'fill in the interstices in the legislative product.'" *Coastal Commc'n*, 2006 WL 1879115, at *5.

385. *Id.* at *4.

386. *Id.* at *6.

387. Comptroller and Borough Presidents' Press Release, *supra* note 154, at 1.

388. Nov. 2016 Council Hearing, *supra* note 137, at 25–30.

Now, New York lawmakers' priorities have expanded into greater concern for privacy protections in services like LinkNYC. Their efforts gained steam in the wake of the rescission of FCC regulations preventing internet service providers from selling customers' data without their permission.[389] For example, in April 2017, more than two dozen New York state legislators introduced bills in both chambers of the State Legislature that would prohibit the sale of consumers' personally identifiable information to third-party advertisers without consumers' consent.[390] Those bills would also apply to entities like LinkNYC that have franchise agreements, or any entities that use the kiosk structures themselves.[391]

In New York City, city officials have vowed to more vigorously protect New Yorkers' privacy. The city council committee that oversees LinkNYC has shown a willingness to require openness about the data it collects and how private companies use it.[392] For example, the committee recently put forward a now-enacted local law that creates a task force to study how city agencies use automated processes in their decision-making and whether to require disclosure of the relevant computer code.[393] Officials have also suggested that the city may use franchise agreements to enhance digital privacy protections for New Yorkers.[394] At the April 24, 2017 meeting of the New York City Council's technology committee, the committee's

---

389. *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Pub. L. No. 115-22, 131 Stat. 88 (2017) (resolution of disapproval effectuated by 82 Fed. Reg. 44,118, 44,118 (Sept. 21, 2017)); *see also* Press Release, Assemblymember Monica P. Wallace, Assemblymembers Wallace and Zebrowski Introduce Legislation to Protect Consumer Data from Internet Service Providers (Apr. 13, 2017), http://nyassembly.gov/mem/Monica-P-Wallace/story/74506/ [https://perma.cc/8PH4-5JMB].

390. Assemb. B. 7191, 2017 Leg., 239th Legis. Sess. (N.Y. 2017); S.B. 5603, 2017 Leg., 239th Legis. Sess. (N.Y. 2017) ("A telecommunications or [internet service provider] that has entered into a franchise agreement, right-of-way agreement, or other contract with the State of New York or any political subdivision thereof, or that uses facilities that are subject to such agreements, even if it is not a party to the agreement, shall not collect nor disclose personal information from a customer resulting from the customer's use of the telecommunications or internet service provider without express written approval from the customer.").

391. *Id.*

392. *See* Transcript of Hearing of N.Y.C. Council Comm. on Tech. 21 (Oct. 16, 2017). Chairperson James Vacca said: "We in this Council have enacted much legislation about transparency. I'm here 12 years. Much of our legislation has been about transparency." *Id.*

393. N.Y.C. Local Law No. 49 (2018).

394. April 2017 Council Hearing, *supra* note 178, at 44–46 (discussing ways to change how the city can award franchise agreements with privacy in mind).

chairperson also asked about the repealed FCC regulations.[395] City officials noted that even though LinkNYC is not technically an internet service provider, its privacy policy is stronger than what the now-rescinded FCC regulations would have mandated.[396] Officials also said they "will continue to implement strict privacy policies for public wi-fi directly provided by the City, such as LinkNYC."[397] The de Blasio administration has also shown a willingness to engage with residents to decide how they want to deploy smart city technology in their own communities. For example, the city began a series of planning meetings in March 2017 in the Brownsville neighborhood of Brooklyn to see how its residents would want to deploy smart city technologies.[398]

B. Greater Transparency Empowers Both Judicial and Public Oversight

With the ability to consider changing technology and weigh societal expectations of privacy, the power to do more to protect New Yorkers' privacy, and the political will to do so, how can DoITT and elected city officials best enforce those goals? The patchy, shifting nature of judicial pronouncements in this area presents a danger of paralysis in the face of uncertainty. But the city can use its experience with the changing LinkNYC privacy policy—and the spirit of its other smart city initiatives—to make sure the kiosks' mission of closing the digital divide for the city's disadvantaged communities is realized without subjecting those same users to intrusive surveillance. Franchisees like LinkNYC should be required to reveal exactly what kind of information they are collecting and explain it clearly in a place where citizens can see it and the city council can review it. This transparency is a central tenet of New York's and other municipalities' smart city initiatives, is palatable to technology

---

395. *Id.* at 22, 42.

396. *Id.* at 42–43.

397. Press Release, City of N.Y. Dep't of Info. Tech. & Telecomm., Joint Statement from Department of Information Technology and Telecommunications Commissioner Anne Roest and Chief Technology Officer Miguel Gamiño on the Repeal of Federal Internet Privacy Protections (Apr. 5, 2017), http://www1.nyc.gov/site/doitt/about/press-releases/joint-statement-doitt-commissioner-roest-and-cto-gamino-on-repeal-of-federal-internet-privacy-protections.page [https://perma.cc/GTG2-WY8D]; *see also* April 2017 Council Hearing, *supra* note 178, at 22, 42.

398. Press Release, City of New York, Mayor de Blasio Brings NYC's First Neighborhood Innovation Lab for Smart City Technologies to Brownsville (Mar. 20, 2017), http://www1.nyc.gov/office-of-the-mayor/news/159-17/ mayor-de-blasio-brings-nyc-s-first-neighborhood-innovation-lab-smart-city-technologies-to [https://perma.cc/WXX3-XR4W].

companies like LinkNYC, enhances judicial oversight, and can be embedded directly in the franchise agreements themselves.

First, revealing more information about the data collected by the kiosks comports with the stated goals of municipal open data and other smart city initiatives, as well as New York City's own stated goals. City officials have already signaled that they want to protect privacy in the increasingly connected city. An example of this is the city's "Internet of Things" guidelines,[399] which cover numerous devices connected to the internet that make smart city programs work.[400] Even though the guidelines have been joined by twenty other cities,[401] they are voluntary. The city has also expressed its desire to fill the gap left by the now-rescinded federal data privacy regulations.[402] New York City officials have said that, "where possible," they want to "leverage" franchise agreements to improve privacy protections for New Yorkers.[403]

Furthermore, advocates of open municipal data argue that it creates a "better understand[ing of] government decision-making, expand[s] knowledge of government services and transactions, and improve[s] access to government processes and decision-makers."[404] That openness facilitates community engagement that can also ensure that surveillance technology is not imposed on communities, but is instead deployed with their support and for their ultimate benefit.[405] For example, surveillance technology can be used to deter not only crime, but also racial profiling and police brutality.[406] But LinkNYC

---

399. *About*, CITY OF N.Y.: GUIDELINES FOR THE INTERNET OF THINGS, https://iot.cityofnewyork.us/about/ [https://perma.cc/SD6J-C5ZR].

400. *Id.*

401. Press Release, City of New York, Leading U.S. Cities Partner on Guidelines for Smart Cities (Sept. 26, 2016), https://iot.cityofnewyork.us/wp-content/uploads/2016/09/PressRelease-SmartCityGuidelines-9-26-2016.pdf [https://perma.cc/X3KF-Y7YC].

402. Ryan McCauley, *New York City, Seattle Enlist in Fight to Preserve Internet Privacy for Residents*, GOV'T TECH. (May 4, 2017), http://www.govtech.com/dc/articles/New-York-City-Seattle-Enlist-in-Fight-to-Preserve-Internet-Privacy-for-Residents.html [https://perma.cc/K737-YSTP]; *see also* April 2017 Council Hearing, *supra* note 178, at 41–43.

403. April 2017 Council Hearing, *supra* note 178, at 17.

404. *Open Cities*, SUNLIGHT FOUND., https://sunlightfoundation.com/policy/open-cities/ [https://perma.cc/2DU9-RXA4].

405. I. Bennett Capers, *Crime, Surveillance, and Communities*, 40 FORDHAM URB. L.J. 959, 977–89 (2013).

406. *Id.* at 978–84.

does not currently explain how law enforcement may use data from the kiosks.[407]

Second, private partners like LinkNYC have demonstrated that they are amenable to such transparency. LinkNYC adopted a more-protective privacy policy without pulling out of the franchise agreement or reducing its ambitions and goals. Quite the opposite: the companies behind LinkNYC have already expanded it to London[408] and have plans to launch in other cities,[409] though locals in other cities are also concerned about the privacy implications.[410] Other revenue-restricting requirements, including prohibitions on certain types of advertising, are already embedded within the franchise agreement.[411] If the city is concerned about providing Wi-Fi without saddling the city with the costs, the LinkNYC experience shows that vendors are still eager to provide digital services to the city even if they must guarantee New Yorkers more robust privacy protections.[412]

Furthermore, other technology companies who may bid on future smart city initiatives are themselves quite aggressive about revealing information about government surveillance occurring on their networks. Technology companies such as Twitter, Google, Cisco, Facebook, and others release aggregated data about how many and what types of requests law enforcement officials have made for user

---

407. Brandon A. Brooks & Alexis Schrubbe, *The Need for a Digitally Inclusive Smart City Governance Framework*, 85 UMKC L. REV. 943, 949 (2017).

408. For example, similar kiosks are now in London. *See Urban Partnerships: Cities*, INTERSECTION, https://www.intersection.com/urban-partnerships/cities/ [https://perma.cc/T34S-QZ3A].

409. *E.g.*, Anthony Noto, *Phone Booth Wi-Fi Provider Intersection Clinches $150 Million in Funding*, N.Y. BUS. J. (Nov. 8, 2017), https://www.bizjournals.com/newyork/news/2017/11/08/phone-booth-wifi-provider-intersection-clinches.html [https://perma.cc/BEK2-4H9B]; Natalie Wong, *Google Sister Company to Build Digital District from Scratch in Toronto*, BLOOMBERG TECH. (Oct. 17, 2017), https://www.bloomberg.com/news/articles/2017-10-17/alphabet-unit-to-build-digital-district-from-scratch-in-toronto [https://perma.cc/9YG5-AF4R].

410. Claire Sasko, *Are Philly's New Wi-Fi Kiosks Going to Spy on You?*, PHILA. MAG. (Nov. 3, 2017), http://www.phillymag.com/news/2017/11/03/philly-new-wifi-kiosks-privacy/ [https://perma.cc/PM46-MCQ5].

411. LinkNYC Franchise Agreement, *supra* note 136, at 30.

412. *See Internet Society Conference*, *supra* note 130, at 22:30 (remarks of Benjamin Dean); *see also* Jan Whittington, *Remembering the Public in the Race to Become Smart Cities*, 85 UMKC L. REV. 925, 929 (2017) (suggesting that cities can use their own financial leverage to impose restrictions on data usage and collection when contracting with third parties); Jesse W. Woo, *Smart Cities Pose Privacy Risks and Other Problems, but that Doesn't Mean We Shouldn't Build Them*, 85 UMKC L. REV. 953, 969 (2017) ("Cities should remember that [they] [sic] have tremendous market power in negotiating contracts.").

data.[413] Technology companies actually pushed for permission from the government to publish the data.[414] They have also sued when the government has tried to prevent them from publishing the reports.[415] These "transparency reports"[416] are not perfect,[417] but they do reveal to the public how much the government is accessing data—not unlike the transparency goals that New York City has already codified in its open data law.[418] Transparency about government data requests is also helpful to the companies' bottom lines.[419] In addition, some large technology companies have fought legal battles with the government over releasing user data, such as Google's stance on the encryption of its smartphones[420] and Microsoft's fight to protect user data stored overseas.[421] Technology companies' willingness to fight

---

413. *See generally* CISCO, TRANSPARENCY REPORT, https://www.cisco.com/c/en/us/about/trust-center/validation/report.html [https://perma.cc/6A7U-QNMM]; FACEBOOK, GOVERNMENT REQUESTS REPORT, https://govtrequests.facebook.com/ [https://perma.cc/7J4H-4DFE]; GOOGLE, REQUESTS FOR USER INFORMATION, https://transparencyreport.google.com/user-data/overview [https://perma.cc/2JLR-7T4S]; TWITTER, INFORMATION REQUESTS, https://transparency.twitter.com/en/information-requests.html [https://perma.cc/B7EH-FMX9]. *See also* Rainey Reitman, *Who Has Your Back? Government Data Requests 2017*, ELEC. FRONTIER FOUND. (July 10, 2017), https://www.eff.org/who-has-your-back-2017 [https://perma.cc/4QYQ-U9PV] (discussing policies at various technology companies).

414. Nick Bilton, *Tech Companies Offer Update on Government Data Requests*, N.Y. TIMES: BITS BLOG (Feb. 3, 2014), https://bits.blogs.nytimes.com/2014/02/03/tech-companies-release-government-data-requests/ [https://perma.cc/KD3D-FJQ3].

415. *See, e.g.*, Twitter, Inc. v. Sessions, 263 F. Supp. 3d 803, 816–17 (N.D. Cal. 2017) (finding that the federal government must face a lawsuit over Twitter's push to release data about national security requests in its transparency reports).

416. *See generally* Wendy Everette, *"The FBI Has Not Been Here [Watch Very Closely for the Removal of This Sign]": Warrant Canaries and First Amendment Protection for Compelled Speech*, 23 GEO. MASON L. REV. 377, 381–83 (2016).

417. Ryan Budish, *What Transparency Reports Don't Tell Us*, THE ATLANTIC (Dec. 19, 2013), https://www.theatlantic.com/technology/archive/2013/12/what-transparency-reports-dont-tell-us/282529/ [https://perma.cc/UGM6-MPMX].

418. 2012 N.Y.C. Local Law No. 11 § 1 (codified as amended at N.Y.C. ADMIN. CODE §§ 23-501 to 23-503 (2018)).

419. Joshua Kopstein, *Silicon Valley's Surveillance Cure-All: Transparency*, NEW YORKER (Oct. 1, 2013), http://www.newyorker.com/tech/elements/silicon-valleys-surveillance-cure-all-transparency [https://perma.cc/VV9D-T4NL] (describing non-U.S. companies canceling contracts with U.S.-based technology companies after revelations of spying by the National Security Agency).

420. For an overview of the debate, see Alina Selyukh & Camila Domonoske, *Apple, the FBI and iPhone Encryption: A Look at What's at Stake*, NAT'L PUB. RADIO (Feb. 17, 2016), https://www.npr.org/sections/thetwo-way/2016/02/17/466796705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake [https://perma.cc/2NAB-G9UX].

421. *See* Microsoft Corp. v. United States, 829 F.3d 197, 201–02 (2d Cir. 2016) (finding that a government warrant could not force Microsoft to turn over customer

these battles and reveal government access to their users' data suggests that New York City can likely require the same thing from vendors without losing any interest from potential bidders.

Finally, proactively revealing information about law enforcement use of new technology is better at protecting privacy than court action alone; judicial oversight of the Fourth Amendment limits on massive and surreptitious data collection is only possible if the government is transparent about what data it is collecting and how. The use of "stingray" cell-site simulators is a prime example. Law enforcement bent over backwards to keep their use of the devices secret, and faced the ire of judges for doing so.[422] Their use began to be regulated and curtailed only after their use was more widely known.[423] Keeping their use secret for so long impaired the judiciary's constitutional oversight role.[424]

In addition, Edward Snowden's revelations about the National Security Agency's bulk data collection programs also show how secrecy limits the judiciary's effectiveness at overseeing law enforcement searches aided by powerful technology.[425] When civil liberties groups sued over legislation that authorized the agency's activities, the U.S. Supreme Court said they did not have standing to sue because any potential injury was, at that point, speculative.[426] But after Snowden's revelations showed the extent of those programs, and how members of the groups challenging them would be impacted, the Second Circuit said they could bring a challenge to the programs in

---

data held at an overseas facility), *cert. granted sub nom.* United States v. Microsoft Corp., 138 S. Ct. 356 (U.S. Oct. 16, 2017) (No. 17-2).

422. Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, BALT. SUN (Nov. 18, 2014, 7:32 PM), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-officer-contempt-20141117-story.html [https://perma.cc/957B-EKXR] (describing state prosecutors' decision to withdraw evidence possibly obtained from a cell-site simulator after a judge threatened to hold a detective in contempt if he did not explain how the evidence was obtained).

423. *See* discussion *supra* Section II.C.

424. Bates, *supra* note 309, at 1.

425. *See, e.g.*, David D. Cole, *After Snowden: Regulating Technology-Aided Surveillance in the Digital Age*, 44 CAP. U. L. REV. 677, 686–88 (2016) (describing how courts and the pubic pushed back on the National Security Agency programs only after they became public); Matt Hamblen, *Snowden Leaks Furor Still Spilling Over into Courts*, COMPUTERWORLD (Feb. 8, 2016, 12:02 PM), https://www.computerworld.com/article/3030661/data-privacy/snowden-leaks-furor-still-spilling-over-into-courts-and-4th-amendment-debate.html [https://perma.cc/R2YJ-MXBD] ("[Snowden's] revelations have prompted a broader discourse, especially among legal scholars, over the potentially invasive nature of big data cybersurveillance tools.").

426. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401–02 (2013).

court.[427] The limits imposed by justiciability doctrines like standing and the opaqueness of the technology at issue will slow any judicial response to abuses and limit the judiciary's effectiveness at addressing these concerns.

C. Privacy Protections Should Be a Prerequisite to a City Contract or Franchise

The city should require its franchisees and contractors to adhere to binding, enforceable privacy principles as a condition of receiving or maintaining a franchise or contract. Such a requirement will help protect New Yorkers' privacy while also giving them the benefit of smart city initiatives. The city can use its government contracting power as leverage to influence the contours of its own surveillance policy.[428] Contractors have financial and other incentives to make the data they collect to others, but they also want to access lucrative municipal markets through franchise that cities control.[429] New York could achieve its own objectives by applying its existing local policies that control data sharing and management to its franchisees, bringing surveillance policy back in line with local priorities.[430]

Such steps could be taken when the city awards new franchises. Existing city regulations demonstrate that the city can embed privacy protections into the franchising process from the start. The city already requires vendors to comply with other standards. Vendors

---

427. ACLU v. Clapper, 785 F.3d 787, 801 (2d Cir. 2015) (noting that "[a]ppellants here need not speculate that the government has collected, or may in the future collect, their call records"); *see also id.* at 802 ("There is no question that an equivalent manual review of the records, in search of connections to a suspect person or telephone, would confer standing even on the government's analysis. That the search is conducted by a machine might lessen the intrusion, but does not deprive appellants of standing to object to the collection and review of their data.").

428. *See* Woo, *supra* note 412, at 969 (discussing how Seattle renegotiated its contracts with a vendor to prevent the sale of traffic location data collected by sensors); *see also* Jan Whittington et al., *Push, Pull, and Spill: A Transdisciplinary Case Study in Municipal Open Government*, BERKELEY TECH. L.J. 1899, 1947–51 (2015) (discussing findings of an assessment of the privacy provisions of Seattle's vendor contracts); *cf.* Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595, 1598, 1601–04 (2016) (discussing how the vast sums of money that the federal government has given to local law enforcement agencies to purchase equipment have realigned cities' surveillance policies with federal goals, and how cities can bring them back into line with local priorities).

429. *See* Whittington, *supra* note 412, at 929.

430. *Cf.* Crump, *supra* note 428, at 1660–61 (suggesting a realignment of police decisions with local policy choices by implementing such measures as requiring police to adhere to privacy policies and empowering a chief privacy officer); Whittington, *supra* note 412, at 929 (suggesting that cities impose restrictions on data usage and collection when contracting with third parties).

must make sure passwords are secure and comply with the city's open data regulations.[431] The city charter also requires franchisees to recognize their workers' unions.[432]

The RFP that led to LinkNYC also established requirements of potential bidders, and future RFPs can make privacy protections a requirement, too. Whoever took over the payphone franchises had to conduct environmental reviews, adhere to the requirements of the Americans with Disabilities Act, follow building codes, permit free 911 calling, and indemnify the city, among many other requirements.[433] Numerous siting requirements, explaining how big or intrusive the physical structures can be on city streets, were also part of the RFP.[434] The RFP even made it harder for contractors to win the franchise if they did not agree to the so-called "Macbride principles," which date from 1991 and relate to alleged employment discrimination in Northern Ireland.[435]

Future bidders could be told that they will be judged in part on how well they will protect users from the possibility of mass surveillance. The city's RFP contained a number of other provisions explaining how their bids would be judged. Bidders were told that they would be evaluated on their legal, technical, business, and financial experience with running Wi-Fi and telephone networks in urban environments,[436] as well as the "adequacy" of their software and information-sharing protocols.[437] Perhaps most relevant, proposals would be rated on how they would "ensure that the public receives the maximum benefits available under the Franchise and that the benefits are shared equitably throughout the City."[438]

The final franchise agreement itself also has numerous requirements. For example, it requires the kiosks to provide encrypted connections to secure users' data.[439] It even contains restrictions on advertising, prohibiting the kiosks from displaying ads for tobacco products.[440] Adding privacy protections to the franchise

---

431. *Technical Vendor Resources*, N.Y.C. DEP'T OF TECH. & TELECOMM., https://www1.nyc.gov/site/doitt/business/technical-vendor-resources.page [https://perma.cc/6BTQ-VJ63].

432. *See* N.Y. CITY CHARTER § 363(h)(6) (2004).

433. RFP, *supra* note 115, at 35–36.

434. *Id.* at 43–44.

435. *Id.* at 54.

436. *Id.* at 23.

437. *Id.* at 24.

438. *Id.*

439. Jean-Pharuns, *supra* note 171.

440. LinkNYC Franchise Agreement, *supra* note 136, at 30.

agreement can follow a similar form to those requirements that are already in place.

The city should therefore incorporate such transparency requirements directly into franchise agreements. New York has no shortage of private partners who should adhere to these principles. Besides LinkNYC, the city has other technology-focused franchises, including for Wi-Fi in the subways[441]; for telecommunications companies to place their equipment on poles for street lights, traffic lights, and utilities[442]; and some voice and data equipment along city streets.[443]

Those requirements should include an explicit description of what data is collected and allow New Yorkers to see their own data. The privacy policy should only be amended through an open, public process overseen and approved by the DoITT and the city council.[444] Teeth should be added to the agreements so violations can be challenged either by private litigation[445] or by automatically withholding revenue from the franchisee or not renewing its franchise. Indeed, the city has taken some steps, albeit tentative, in this direction. In November 2017, the city requested information about how it could roll out broadband to all New Yorkers' homes.[446] In its request, the city explicitly asked for those submitting information to explain how their suggestions would protect New

---

441. *Mobile Subway Stations Franchises*, N.Y.C. DEP'T OF INFO. TECH. & TELECOMM., http://www1.nyc.gov/site/doitt/business/mobile-subway-stations-franchises.page [https://perma.cc/C32N-A6XA].

442. *Mobile Telecom Franchises*, N.Y.C. DEP'T OF INFO. TECH. & TELECOMM., http://www1.nyc.gov/site/doitt/business/mobile-telecom-franchises.page [https://perma.cc/U42H-9ZQA].

443. *Information Service Franchises*, N.Y.C. DEP'T OF INFO. TECH. & TELECOMM., http://www1.nyc.gov/site/doitt/business/information-services-franchises.page [https://perma.cc/CF6G-LJ97].

444. Buttar & Kalia, *supra* note 175; *cf.* Crump, *supra* note 428, at 1656–57 (suggesting more involvement by local officials when accepting federal grants for surveillance technologies).

445. Jennifer Shkabatur, *Transparency With(out) Accountability: Open Government in the United States*, 31 YALE L. & POL'Y REV. 79, 133–34 (2012) (describing citizen suits as one method to bring enforceability to municipal transparency initiatives).

446. Mara Gay, *New York City Wants New Ideas on Providing Internet Access*, WALL ST. J. (Nov. 14, 2017), https://www.wsj.com/articles/new-york-city-wants-new-ideas-on-providing-internet-access-1510635662 [https://perma.cc/4TDL-E83B]; Press Release, City of N.Y. Mayor's Office of the Chief Tech. Officer, Mayor's Office of the Chief Technology Officer Issues Request for Information on Citywide Broadband Deployment (Nov. 15, 2017) [hereinafter RFI Press Release], http://www1.nyc.gov/site/forward/news/press-release-rfi.page [https://perma.cc/MPH6-8S9U].

Yorkers' privacy.[447] The city plans to use the suggestions it receives to shape a formal request for proposals about in-home broadband.[448] By going further to make its privacy principles binding and enforceable, the city could achieve one of its smart city goals of government accountability and protect its citizens' privacy at the same time.[449]

CONCLUSION

Using procurement and contractual control to ensure New Yorkers' privacy rights is the most effective way to vindicate the city's twin goals of closing the digital divide and making New York a "smart city." Judicial responses are too slow and muddled, and courts' views often clash with public opinion. Cities are not powerless; their leverage over local contractors sets a norm that can adapt to changing technology. Requiring greater transparency about vendors' data collection and punishing violators would advance the city's policies, ensure that LinkNYC fulfills its goal of making New York City "smarter" and more equitable, and would be acceptable to technology companies that are already pushing for more openness about law enforcement's use of their networks. Greater transparency also allows courts and policymakers to respond when actions go beyond the scope of the Fourth Amendment[450] or the public's expectations of privacy.[451] LinkNYC has not been immune from

---

447. Mayor's Office of the Chief Tech. Officer for the City of N.Y., NYC Connected: Request for Information, Page 5F (Nov. 14, 2017), https://app.wizehive.com/appform/display/nycconnectedrfi/11 [https://perma.cc/NP3R-W8XR] ("Privacy: The City places a high priority on protecting the rights of New Yorkers to control their sensitive personal data as they access the internet. Please share your suggestions regarding privacy practices that could be included in your potential participation in the City's pursuit of its policy goals.").

448. RFI Press Release, *supra* note 446.

449. *See, e.g.*, 2012 N.Y.C. Local Law No. 11 § 1 (codified as amended at N.Y.C. ADMIN. CODE §§ 23-501 to 23-503 (2018)) (finding that the city's open data portal "will make the operation of city government more transparent, effective and accountable to the public"); *Privacy + Transparency*, CITY OF N.Y.: GUIDELINES FOR THE INTERNET OF THINGS, https://iot.cityofnewyork.us/privacy-and-transparency/ [https://perma.cc/M7U8-UH63] ("The City is committed to being open and transparent about the 'who, what, where, when, why and how' of data collection, transmission, processing and use.").

450. *Cf. supra* Sections II.C, III.B (discussing how challenges to cell-site simulators and NSA activities were only possible once people actually knew that those programs and technologies existed and that they were being used to surveil Americans without their knowledge).

451. *See* discussion *supra* Section II.E.

unanticipated consequences.[452] Shrouding LinkNYC in secrecy, however, makes it difficult for New Yorkers "to accept what they are prohibited from observing."[453] The kiosks can see just about everything that New Yorkers are doing. It is time for New Yorkers to see everything that the kiosks are doing, too.

---

452. Calder & O'Neill, *supra* note 162.

453. *Cf.* "People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing." ACLU v. Clapper, 785 F.3d 787, 828 (2d Cir. 2015) (Sacks, J., concurring) (quoting Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 572 (1980)) (discussing advantages of open court proceedings).