Fordham Urban Law Journal

Volume 47
Number 4 *Symposium: Urban Intelligence and the Emerging City*
Article 2

2020

Smarter Cities or Bigger Brother? How the Race for Smart Cities Could Determine the Future of China, Democracy, and Privacy

John Wagner Givens

Debra Lam

SMARTER CITIES OR BIGGER BROTHER? HOW THE RACE FOR SMART CITIES COULD DETERMINE THE FUTURE OF CHINA, DEMOCRACY, AND PRIVACY

John Wagner Givens[*] *& Debra Lam*[**]

---

[*] Associate Professor, School of Government and International Affairs, Kennesaw State University. Thank you to everyone involved in the 2019 *Fordham Urban Law Journal* Cooper–Walsh Colloquium as well as Heather Pincock for her helpful comments and support.

[**] Managing Director, Smart Cities and Inclusive Innovation, Georgia Institute of Technology. Thank you to the Office of the Executive Vice President of Research at Georgia Tech and the Georgia Smart Partners: Georgia Power, Atlanta Regional Commission (ARC), Association County Commissioners of Georgia, Georgia Centers for Innovation, Georgia Chamber, Georgia Department of Community Affairs, Georgia Municipal Association, Metro Atlanta Chamber, and Technology Association of Georgia, Georgia Planning Association, and the Global City Teams Challenge.

INTRODUCTION

Since at least the early twentieth century, when the emergence of the automobile saved cities from being buried under the manure produced by their horse-based transportation system, technologies have emerged to help solve the unique problems faced by rapidly growing cities.[1] Yet, as with the automobile, no matter how rapid and seemingly miraculous a technological solution, it will create its own set of problems that need to be addressed. For a little over a decade, smart city technology has been promising to cure a wide variety of cities' transportation, financial, environmental, and social ills.[2] But unresolved concerns about smart city technology, especially relating to privacy, are increasingly delaying the development and implementation of these technologies in democracies.

To explore the themes and issues outlined above, this Article takes a comparative approach to the challenges that smart cities face. Specifically, we compare how concerns about smart city technology play out in wealthy democracies[3] and contrast this with the relatively unchallenged rollout of that technology in the People's Republic of China. These wealthy democracies are further divided into the European Union, where government regulation is stronger, and North America, where smart cities have faced less regulation, but perhaps, as a result, more popular resistance.[4]

Part I of this Article reviews the rise of cities and smart city technology. We assess the (over)promise of the technology and

---

1. *See* Elizabeth Kolbert, *Hosed*, NEW YORKER (Nov. 9, 2009), https://www.newyorker.com/magazine/2009/11/16/hosed [https://perma.cc/9PSE-V88K].

2. *See* Teena Maddox, *Smart Cities: A Cheat Sheet*, TECHREPUBLIC (July 16, 2018), https://www.techrepublic.com/article/smart-cities-the-smart-persons-guide/ [https://perma.cc/G5G6-KYFL].

3. This focus on wealthy democracies is a product of where the leading companies selling smart city technology are currently based. *See These Are the Top Ten Companies That Build Smart Cities*, SMART CITY HUB (Apr. 5, 2017), https://smartcityhub.com/technology-innnovation/the-top-ten-companies-that-build-smart-cities/ [https://perma.cc/8SET-H73X].

4. *See generally* Mario Weber & Ivana Podnar Žarko, *A Regulatory View on Smart City Services*, 19 SENSORS (BASEL) 415, 416 (2019). *See also* Michael M. Losavio et al., *The Internet of Things and the Smart City: Legal Challenges with Digital Forensics, Privacy, and Security*, 1 SECURITY & PRIVACY 1, 6 (2018).

examine the increasing pushback and skepticism that smart city projects and related technology have attracted. In Part II, we turn our attention to the case of China, examining four different uses of smart city technology: Alibaba's City Brain, the monitoring of Xinjiang, the social credit system, and other uses of facial recognition technology. Part II then draws overall lessons from these Chinese cases.

Part III of this Article considers possibilities for improving the use, regulation, and development of smart city technology in wealthy democracies. First, we consider the important role surveillance intermediaries could play in protecting privacy. Second, we look at the European Union and its General Data Protection Regulation (GDPR). Third, we ask whether it is, at this point, possible for companies based in democracies to catch up with the development of Chinese smart city technology. Fourth, we look at how and where competition for smart city technology could play out in the rest of the world.

Part IV provides recommendations about a possible way forward in the development of smart cities that would protect privacy and engender public trust and support.

I. SMART CITIES

Rapid global urbanization driven by overall population increase and rural-to-urban migration is expected to reach 60% of the world's population by 2030, and 68% by 2050.[5] Across the world, urbanization has been closely tied with lower overall poverty rates, higher educational levels, and higher living standards. It is the main reason people choose to move to cities: the lure of higher-paying jobs and greater opportunities. McKinsey projects that the top 100 global cities by economic growth will contribute 35% of the world's GDP growth from 2007 to 2025.[6] Cities are seen as engines of progress, improved services, and technological advancement.

However, city development also produces unintended negative effects. For example, cities are major contributors to climate change.

---

5. U.N. DEP'T OF ECON. & SOC. AFFAIRS, POPULATION DIV., WORLD URBANIZATION PROSPECTS 2018: HIGHLIGHTS, at 5, U.N. Doc. ST/ESA/SER.A/421, Sales No. E19.XIII.6 (2019).

6. RICHARD DOBBS ET AL., MCKINSEY GLOB. INST., URBAN WORLD: MAPPING THE ECONOMIC POWER OF CITIES 1 (2011), https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Urbanization/Urban%20world/MGI_urban_world_mapping_economic_power_of_cities_full_report.ashx [https://perma.cc/9M6G-8ZCF].

While they house 55% of the world's population[7] on only 2% of the Earth's surface, cities consume 78% of the world's energy and produce more than 60% of the world's greenhouse gases.[8] City residents' reliance on fossil fuels to drive their cars, heat their homes, and run their factories worsen air and water quality and harm wildlife and its habitats.[9] According to the World Health Organization (WHO), more than 80% of urban inhabitants are exposed to levels of air pollution above WHO limits which, in turn, increases the risk of stroke, heart disease, and other chronic and acute respiratory diseases especially for elderly, youth, and marginalized groups.[10] Globally, urban areas have, on average, 50% less species richness[11] than intact natural habitats.[12] As Dr. Eric Strauss, executive director of the Center for Urban Resilience at Loyola Marymount University-Los Angeles, notes: "When you have an intact animal diversity, you control those zoonatic diseases without having to use as much pesticide."[13] More frequent and severe extreme weather, such as hurricanes, heat waves, and drought, have not only damaged infrastructure and food economies but have also widened socio-economic inequality between those who have the resources and physical strength to withstand it, and those who do not.[14] The urban poor often live in areas of greatest risk (for example, older homes in

---

7. Hannah Ritchie & Max Roser, *Urbanization*, OUR WORLD IN DATA (Sept. 2018), https://ourworldindata.org/urbanization [https://perma.cc/3SB4-QTAG].

8. *Cities and Pollution Contribute to Climate Change*, UNITED NATIONS, https://www.un.org/en/climatechange/cities-pollution.shtml [https://perma.cc/ZS9P-UETT] (last visited Jan. 22, 2020).

9. *Urban Threats*, NAT'L GEOGRAPHIC, https://www.nationalgeographic.com/environment/habitats/urban-threats/ [https://perma.cc/778L-4LZA] (last visited Feb. 18, 2020).

10. *WHO Global Urban Ambient Air Pollution Database*, WORLD HEALTH ORG. (2016), http://www.who.int/phe/health_topics/outdoorair/databases/cities/en/ [https://perma.cc/T9SP-XYSR].

11. Species richness is the number of different species in an ecosystem. J.A. Veech, *Measuring Biodiversity*, *in* ENCYCLOPEDIA OF THE ANTHROPOCENE 287–95 (Dominick Dellasala & Michael I. Goldstein eds., 2018).

12. German Center for Integrative Biodiversity Research, *Urban Growth Causes More Biodiversity Loss Outside of Cities*, EUREKALERT! (Dec. 9, 2019), https://www.eurekalert.org/pub_releases/2019-12/gcfi-ugc120619.php [https://perma.cc/2DWY-73DC].

13. Steve Holt, *Where Do Urban Animals Go When Their Habitats Disappear?*, CITYLAB (Nov. 16, 2017), https://www.citylab.com/environment/2017/11/where-do-urban-animals-go-when-their-habitats-disappear/546002/ [https://perma.cc/3YRQ-654Q].

14. *See generally* Kimberley Thomas et al., *Explaining Differential Vulnerability to Climate Change: A Social Science Review*, WILEY INTERDISC. REV. CLIMATE CHANGE, Nov. 5, 2018.

flood zones) and have fewer resources (such as home and health insurance), information, and financial networks to avoid, prepare for, and address those risks.[15]

A. The Rise of Smart Cities

The problems that have accompanied urbanization have forced many to rethink how we build and maintain cities. Cities can still be an overall positive force, and proactive city leaders are increasingly galvanized to create change. Mayors from all over the world are coming together to share ideas and solutions over their common urban problems.[16] Despite differences in development levels, politics, and geographies, cities are increasingly expected to do more with fewer financial resources,[17] poor infrastructure,[18] and an aging workforce.[19] For example, Indianapolis requires ten times the current budget to achieve basic fair conditions for roads,[20] typical of many cities. As Zach Adamson, a member of the Indianapolis City-County Council's Public Works Committee, noted, "The city is always behind, there is not enough revenue to cover our needs."[21]

Organizations like the C40,[22] Rockefeller Foundation,[23] and Bloomberg Philanthropies[24] have become bastions of mayoral

---

15. *See* S. Nazrul Islam & John Winkel, *Climate Change and Social Inequality* 6 (U.N. Dep't of Econ. & Soc. Affairs, Working Paper No. 152, 2017).

16. *See About Us*, GLOBAL COVENANT MAYORS FOR CLIMATE & ENERGY, https://www.globalcovenantofmayors.org/about/ [https://perma.cc/5R77-E9AD] (last visited Feb. 18, 2020).

17. *See* Michael Maciag, *What Are Cities Spending Big On? Increasingly, It's Debt.*, GOVERNING (Sept. 2017), https://www.governing.com/topics/finance/gov-legacy-cities-bills-debt.html [https://perma.cc/3Q9D-XXQW].

18. *See America's Infrastructure Grade*, ASCE's 2017 INFRASTRUCTURE REP. CARD, https://www.infrastructurereportcard.org/americas-grades/ [https://perma.cc/5GSK-VV34] (last visited Feb. 18, 2020).

19. *See* Michael Maciag, *The "Silver Tsunami" Has Arrived in Government*, GOVERNING (May 31, 2016), https://www.governing.com/topics/mgmt/gov-government-retirement-survey-center-state-local.html [https://perma.cc/V744-G86Z].

20. John Tuohy, *Indy's Streets Are So Bad, Making Them 'Fair' Would Take 10 Times the Current Budget*, INDIANAPOLIS STAR (Feb. 15, 2018), https://www.indystar.com/story/news/2018/02/15/indys-streets-so-bad-making-them-fair-would-take-10-times-current-budget/324044002/ [https://perma.cc/XWL5-XB6M].

21. *Id.*

22. *About C40*, C40 CITIES, https://www.c40.org/about [https://perma.cc/BY3D-NRL5] (last visited Feb. 18, 2020).

23. *About Us*, ROCKEFELLER FOUND., https://www.rockefellerfoundation.org/about-us/ [https://perma.cc/K7AS-A3DD] (last visited Feb. 18, 2020).

collaboration and have heightened the sense of urgency and opportunity for cities to be transformative. These coalitions have tried to take best practices and innovations from industry, both in process and in outcome, and seed them in cities. Michael Bloomberg, former mayor of New York City, naturally brought his managerial style and industry expertise from running New York City, where he was famous for saying, "In God we trust. Everyone else bring data."[25]

Industry, in turn, witnessed its own technological breakthroughs and was eager to proselytize their solutions and increase their sales, markets, and influence by working with and selling to cities. IBM, for example, promised a "smarter planet and a new strategic agenda for progress and growth."[26] Cisco solutions claim that it "encapsulates a new way of thinking about how communities are designed, built, managed, and renewed to achieve social, economic, and environmental sustainability."[27] Start-ups, small and medium-sized enterprises (SMEs), and consultancies naturally joined, each offering their own solutions and analysis to support cities.

It is this confluence of urgency and expectation in cities, and the increased ability with industry-led solutions and optimism, that birthed smart cities.[28] By 2025, the smart cities market is estimated to be worth $2.4 trillion.[29] The convergence is also resulting in more flexible and diverse jobs that are newly created or replacing lower-skilled jobs.[30] McKinsey estimates that 15% of our global

---

24. *About Us*, BLOOMBERG PHILANTHROPIES, https://www.bloomberg.org/about/ [https://perma.cc/6ULP-YSPL] (last visited Feb. 18, 2020).

25. *Bye-Bye, Bloomberg*, ECONOMIST (Nov. 2, 2013), https://www.economist.com/united-states/2013/11/02/bye-bye-bloomberg [https://perma.cc/A525-MTE9].

26. *IBM Builds a Smarter Planet*, IBM, http://www.ibm.com/smarterplanet/us/en/ [https://perma.cc/SGC6-KYWN] (last visited Jan 22, 2020).

27. Seungho Yoo, *Songdo: The Hype and Decline of World's First Smart City*, *in* SUSTAINABLE CITIES IN ASIA 153 (Federico Caprotti & Li Yu eds., 2017).

28. *See generally* Mircea Eremia et al., *The Smart City Concept in the 21st Century*, 181 PROCEDIA ENGINEERING 12 (2017).

29. *See* Pramod Borasi, *Smart Cities Market by Functional Area (Smart Governance & Smart Education, Smart Energy, Smart Infrastructure, Smart Mobility, Smart Healthcare, Smart Building, and Others): Global Opportunity Analysis and Industry Forecast, 2018–2025*, ALLIED MARKET RES. (Nov. 2018), https://www.alliedmarketresearch.com/smart-cities-market [https://perma.cc/S6JZ-KJRJ].

30. *See* James Manyika & Kevin Sneader, *AI, Automation, and the Future of Work: Ten Things to Solve For*, MCKINSEY GLOBAL INST. (June 2018), https://www.mckinsey.com/featured-insights/future-of-work/ai-automation-and-the-future-of-work-ten-things-to-solve-for [https://perma.cc/N9DA-BC8N].

workforce, or 400 million workers, could be displaced by automation from 2016–2030.[31] However, the same McKinsey analysis shows an "additional labor demand of between 21 percent to 33 percent of the global workforce (555 million and 890 million jobs) to 2030, more than offsetting the numbers of jobs lost."[32] Many of the new jobs created are ones we currently have a hard time imagining and are based on emerging technology that is becoming part of our built environment. For example, Accenture estimates that the fifth-generation wireless technology (5G) rollout could create 3 million direct U.S. jobs and an additional 2.2 million jobs that support the 5G economic ecosystem.[33]

B. The Overpromise of Smart Cities

Nothing could be a clearer sign of the hype that surrounds the smart city than the multitude of definitions for "smart city" that exist; the term is most frequently used without any clear or consistent definition in mind. In an article for the *Journal of Urban Technology*, Vito Albino, Umberto Berardi, and Rosa Maria Dangelico collected 23 distinct definitions of smart cities from authoritative sources.[34] Liviu-Gabriel Cretu provides a useful breakdown of the two major trends in smart city thinking: "(1) smart cities should do everything related to governance and economy using new thinking paradigms and (2) smart cities are all about networks of sensors, smart devices, real-time data and ICT integration in every aspect of human life."[35]

In this Article, we eschew a specific definition in favor of considering examples and technologies that are included in projects or articles that brand themselves as being about smart cities. If we were to exclude these for not fitting a narrower and more precise definition of smart city, we risk missing how less-related technology

---

31. *Id.*

32. *Id.*

33. Urvashi Verma, *5G Rollout to Create 3 Million New Jobs, Adding $500 Billion to the US Economy*, CONNECTED REAL EST. MAG. (Sept. 26, 2019), https://www.connectedremag.com/das-in-building-wireless/5g-rollout-to-create-3-million-new-jobs-adding-500-billion-to-the-us-economy/ [https://perma.cc/A42J-F337].

34. *See* Vito Albino et al., *Smart Cities: Definitions, Dimensions, Performance, and Initiatives*, 22 J. URB. TECH. 3, 6–8 (2015). The earliest definition collected comes was published by R.E. Hall in 2000 and is fairly typical: "A city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rails, subways, airports seaports, communications, water, power, even major buildings, can better optimize its resources, plan its preventive maintenance activities, and monitor security aspects while maximizing services to its citizens." *Id.* at 6.

35. Liviu-Gabriel Cretu, *Smart Cities Design Using Event-Driven Paradigm and Semantic Web*, 16 INFORMATICA ECONOMICĂ 57, 57 (2012).

and examples get brought into the discourse on smart cities. Two examples from the subsequent Section, Quayside's wooden construction and the Facebook data breaches, illustrate how concepts that might not fit many definitions of smart city technology nevertheless may be held back by (in the case of the former) or contribute to (in the case of the latter) the pushback against smart cities.

Smart city solutions were originally seen as a way to solve many of the problems plaguing cities. With better technology and mastery of data analytics, cities could become more efficient at providing basic services like waste and recycling collection,[36] identifying potholes,[37] and abating pests and rats.[38] The technologies were also supposed to tackle larger problems like public safety and traffic congestion. McKinsey estimates that smart mobility applications (including smarter public transit, self-driving electric vehicles, ride-hailing, and car, bicycle, and scooter-sharing)[39] have the potential to cut commuting times for developing cities by 15% to 20%.[40]

However, almost as soon as smart city technologies began to be applied, it became apparent that the technology-driven approach of smart cities was insufficient to achieve cities' goals; sensors designed to notify drivers of free parking spots or public charging stations for electric vehicles needed trained staff for installation and maintenance.[41] While there were common problems, the one technology solution fits all approach was not effective — tech

---

36. *See* Donald Cambelin, *Smarter Waste for the Smart City*, COMPOLOGY (Sept. 19, 2017), http://compology.com/blog/smarter-waste-for-the-smart-city [https://perma.cc/5NW6-FND6].

37. *See* Theodora S. Brisimi et al., *Sensing and Classifying Roadway Obstacles in Smart Cities: The Street Bump System*, 4 IEEE ACCESS 1301, 1302 (2016).

38. *See* Linda Poon, *Will Cities Ever Outsmart Rats?*, CITYLAB (Aug. 9, 2017), https://www.citylab.com/solutions/2017/08/smart-cities-fight-rat-infestations-big-data/535407/ [https://perma.cc/PH9G-B2TU].

39. *See* Eric Hannon et al., *An Integrated Perspective on the Future of Mobility*, MCKINSEY GLOBAL INST. (Oct. 2016), https://www.mckinsey.com/business-functions/sustainability/our-insights/an-integrated-perspective-on-the-future-of-mobility [https://perma.cc/CRC4-HTV9].

40. *See* Jonathan Woetzel et al., *Smart City Technology for a More Liveable Future*, MCKINSEY GLOBAL INST. (June 2018), https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/smart-cities-digital-solutions-for-a-more-livable-future [https://perma.cc/TMT2-S9MR].

41. *See* Marcos Martínez Euklidiadas, *Smart Cities That Failed along the Way*, SMART CITY LAB (Nov. 26, 2019), https://www.smartcitylab.com/blog/urban-environment/smart-cities-that-failed-along-the-way/ [https://perma.cc/KK28-FK68].

companies and vendors were driven by the sales of their products and services, rather than by development, such that it became a race to have their technology adopted by as many cities as possible for domain supremacy.[42] Cities purchased smart city technology falsely thinking that technology alone would make the city smart with limited knowledge in the application and usage of the technology, and left unsure of the exact problem they were trying to solve with its implementation.[43] Smart city technology also widened inequalities within and between cities among those with the technology, connectivity, and knowledge to use it — and those without it. For example, while Flint, Michigan's water supply systems continued to deteriorate and poison its residents,[44] 200 miles away in South Bend, Indiana, Mayor Pete Buttigieg's administration was able to work with the University of Notre Dame to install sensors under manhole covers and implement a smart sewer system.[45]

The smart cities backlash created new thinking about technology and its relationship with city development. Smart cities became best thought of not as an end state, but a continuous improvement process that allows cities and communities of all sizes to pursue the most suitable integration of technology and data to increase their quality of life. It concentrates on the local context and meeting the community where they are, as well as creative problem-solving with an enhanced toolkit that includes technology, data, as well as policy and financing solutions. Smart cities, such as Smart Columbus,[46] Chicago's City Tech,[47] and Dallas Innovation Alliance,[48] are utilizing this kind of

---

42. *See* Laura Bliss, *2018 Was the Year of the Smart City Skeptic*, CITYLAB (Dec. 27, 2018), https://www.citylab.com/transportation/2018/12/smart-city-uber-google-facebook-technology-startup-solutions/579025/ [https://perma.cc/VRE8-NDH5].

43. *See* Ben Green, *Cities Are Not Technology Problems: What Smart Cities Companies Get Wrong*, METROPOLIS (Mar. 4, 2019), https://www.metropolismag.com/cities/ben-green-smart-enough-city/ [https://perma.cc/L8RE-WEBE].

44. *See* Melissa Denchak, *Flint Water Crisis: Everything You Need to Know*, NAT'L RESOURCE DEF. COUNCIL (Nov. 8, 2018), https://www.nrdc.org/stories/flint-water-crisis-everything-you-need-know [https://perma.cc/UP2N-LP7H].

45. Debra Lam & John Wagner Givens, *Small and Smart: Why and How Smart City Solutions Can and Should Be Adapted to the Unique Needs of Smaller Cities*, 12 NEW GLOBAL STUD. 21, 31–32 (2018).

46. *See We Are Smart, Columbus*, SMART COLUMBUS, https://smart.columbus.gov/about [https://perma.cc/9QDA-78QL] (last visited Feb. 18, 2020).

47. *See About City Tech*, CITY TECH, http://www.citytech.org/about-overview [https://perma.cc/X6A6-M85T] (last visited Feb. 18, 2020).

empowering, people-centric framework, with new types of solutions and public-private partnerships. Funded by public and private grants,[49] the efforts include Multimodal Trip Planning Applications and common transportation payment systems,[50] and developing demand management opportunities to reduce freight delivery congestion[51] and open data initiatives.[52] Yet, even more rapid than the progress of smart city thinking and projects has been the backlash against smart city technology, which we consider in the next Section.

C. Smart City Skepticism

"CityLab," *The Atlantic*'s publication devoted to the future of cities, declared 2018 the year of the smart city skeptic.[53] Their run-down of the challenges that smart cities face included both meaningful setbacks to an important smart city project as well as more general and less immediate concerns, such as how the rise of autonomous vehicles might change city planning. The problems described were distressingly familiar, with violations of data privacy topping of the list. Singled out was the revelation that Facebook had given its business partners access to personal data, exempting them from its own privacy rules. In total, Facebook provided 150 companies, including Netflix and Spotify, access to user data that included users' private messages.[54]

In some ways, it is misleading to name the above Facebook example, and other similar violations of online privacy, as a setback for smart cities. Because the collection and analysis of data is at the core of smart cities, every blow toward citizen trust in data collection, analysis, and storage may ultimately have a significant impact on

---

48. *See About DIA*, DALLAS INNOVATION ALLIANCE, http://www.dallasinnovationalliance.com/what-we-do [https://perma.cc/C4P8-3RWQ] (last visited Feb. 18, 2020).

49. *See, e.g.*, *We Are Smart, Columbus*, *supra* note 46.

50. *See Multi-Modal Trip Planning Application & Common Payment System*, SMART COLUMBUS, https://smart.columbus.gov/projects/multi-modal-trip-planning-application [https://perma.cc/KWG6-6A5Z] (last visited Feb. 21, 2020).

51. *See City Solutions*, CITY TECH, http://www.citytech.org/city-solutions [https://perma.cc/H3PD-6J5S] (last visited Feb. 21, 2020).

52. *See Dallas OpenData*, CITY OF DALLAS, https://www.dallasopendata.com/ [https://perma.cc/G46Q-A4EK] (last visited Feb. 21, 2020).

53. Bliss, *supra* note 42.

54. Gabriel J. X. Dance et al., *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html [https://perma.cc/FJY7-HT4N].

public goodwill, which smart city projects in democracies must rely on to progress. Indeed, this Article will show that it is precisely these types of concerns that are likely to impede the development of smart cities in democracies and ultimately allow the People's Republic of China (PRC) to control the future of smart city technology.

Setbacks to smart city efforts may come in the form of revelations that damage general public opinion about emerging technologies rather than events that are specific to the development of any actual smart city projects. Another major source of concern for smart city advocates and skeptics is that many smart city solutions were not as close at hand as previously thought.[55] For example, after years of predictions that autonomous vehicles (AVs) were just over the horizon, stalled development and a fatal accident have suggested that self-driving cars are decades away, not years.[56] AVs are more closely related to smart cities than social media, but would not necessarily hold back the other aspects of smart cities projects. Here again, China seems to have an advantage. As this Article demonstrates, Chinese citizens are less skeptical of new technologies, irrespective of how deeply flawed they may be.[57]

Closer still to the core of smart city strategies, car-, bike-, and scooter-sharing services have also come under increased scrutiny.[58] Evidence that ridesharing exacerbates, rather than improves both traffic and carbon emissions — serious problems that smart cities are

---

55. *See* Bliss, *supra* note 42.

56. Neal E. Boudette, *Despite High Hopes, Self-Driving Cars Are 'Way in the Future'*, N.Y. TIMES (July 17, 2019), https://www.nytimes.com/2019/07/17/business/self-driving-autonomous-cars.html [https://perma.cc/TDF7-KDCW].

57. Paul Mozur, *Wild about Tech, China Even Loves Robot Waiters That Can't Serve*, N.Y. TIMES (July 21, 2018), https://www.nytimes.com/2018/07/21/technology/china-future-robot-waiters.html [https://perma.cc/3TE3-2ZSD].

58. *See* Ziru Li et al., An Empirical Analysis of On-Demand Ride Sharing and Traffic Congestion 5 (Sept. 25, 2016) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843301 [https://perma.cc/B62N-PP6E]; Daniel Castro, *E-Scooter Bans Show Cities Are Hesitant to Embrace Innovation*, GOV'T TECH. (Mar. 2019), https://www.govtech.com/opinion/E-Scooter-Bans-Show-Cities-Are-Hesitant-to-Embrace-Innovation.html [https://perma.cc/2TH6-TEDF]; Luz Lazo, *Dockless Bike, Scooter Firms Clash with U.S. Cities Over Regulations*, WASH. POST (Aug. 4, 2018), https://www.washingtonpost.com/local/trafficandcommuting/dockless-bike-scooter-firms-clash-with-us-cities-over-regulations/2018/08/04/0db29bd0-9419-11e8-a679-b09212fb69c2_story.html [https://perma.cc/RNW4-2RS7]; Jane Lee, *Bike-Sharing Companies Face an Uphill Ride in U.S.*, REUTERS (Mar. 16, 2018), https://www.reuters.com/article/us-usa-bikesharing/bike-sharing-companies-face-an-uphill-ride-in-u-s-idUSKCN1GS0YX [https://perma.cc/X5EZ-QCV5].

meant to ameliorate — may be mounting.[59] Micromobility solutions such as bike- and e-scooter-sharing services have faced criticism over blocking sidewalks, breaking traffic ordinances, increasing emergency room visits, and causing accidents.[60] Cities, including West Hollywood, California, Nashville, Tennessee, and Winston-Salem, North Carolina, have forced e-scooter-sharing services out of their cities; other local governments, among them Columbia, South Carolina, and Davis, California passed preemptive scooter-sharing bans.[61] Meanwhile, cities such as Atlanta, Georgia have pushed operators out with regulations, including high impound fees and a ban on night use.[62] Yet, e-scooters remain popular and can likely help reduce carbon emissions.[63] Most issues arise not from inherent problems in the technology, concept, or appeal, but in a lack of both physical and legal infrastructure.[64] Laws and regulations that apply to e-scooters are often unclear, and cities and scooter companies appear to be tacitly acknowledging, if not encouraging, rule-breaking by scooter riders. Mandates to wear helmets, stay off of sidewalks, and read voluminous terms and conditions are "more honored in the

---

59. *See* Lauren Alexander & Marta González, Assessing the Impact of Real-Time Ridesharing on Urban Traffic using Mobile Phone Data 9 (2015) (unpublished presentation, Massachusetts Institute of Technology) (on file with University of Maryland, Baltimore County), https://userpages.umbc.edu/~nroy/courses/fall2018/cmisr/papers/Real-time-Ridesharing_Alexander.pdf [https://perma.cc/S7GU-289P]; Gregory D. Erhardt et al., *Do Transportation Network Companies Decrease or Increase Congestion?*, SCI. ADVANCES, May 8, 2019, at 4–6, https://advances.sciencemag.org/content/advances/5/5/eaau2670.full.pdf [https://perma.cc/5LHB-689C]. Yet, other studies have found conflicting results. *See* Li et al., *supra* note 58.

60. Castro, *supra* note 58.

61. *Id.*; Emily Maher, *Davis Bans Electric Scooter Companies, for Now*, KCRA (Oct. 30, 2018), https://www.kcra.com/article/davis-bans-electric-scooter-companies-for-now/24461579 [https://perma.cc/LK8L-TM6W].

62. Raisa Habersham, *Lime Scooters Leaving Atlanta, Cites 'Significant' Scooter Impound Fees*, ATLANTA J. CONST. (Jan. 9, 2020), https://www.ajc.com/news/local/lime-scooters-leaving-atlanta-cites-significant-scooter-impound-fees/0xL0NUZa2aDs2pt0eQ6JQI/ [https://perma.cc/2PNJ-3NLP].

63. *See* Joseph Hollingsworth et al., *Are E-Scooters Polluters? The Environmental Impacts of Shared Dockless Electric Scooters*, 14 ENVTL. RES. LETTERS 1, 9 (2019).

64. *See* John Frazer, *With the Help of Regulators, Micromobility Will Be Poised for a Massive Surge in Adoption*, FORBES (June 13, 2019), https://www.forbes.com/sites/johnfrazer1/2019/06/13/with-the-help-of-regulators-micromobility-will-be-poised-for-a-massive-surge-in-adoption/ [https://perma.cc/F49F-A4JE].

breach than in the observance."[65] In this sense, e-scooters neatly embody the current state of most smart cities technology — an emerging technological solution lacking sufficient regulatory, legal, and physical infrastructure, and heavily dependent on public opinion for its continued existence and expansion.

Most ominously for smart city advocates, however, is the fact that the largest smart city project in North America has come under heavy public criticism. The Toronto Quayside project by Sidewalk Labs (a subsidiary of Alphabet, Google's parent company), which was supposed to be the first neighborhood built "from the internet up,"[66] experienced several major setbacks.[67] First, the board of Waterfront Toronto, the organization administering the project, experienced a series of public resignations and firings related to concerns over Quayside.[68] Saadia Muzaffar, a member of Waterfront Toronto's Digital Strategy Advisory Panel, levied a very public resignation, citing "a blatant disregard for resident concerns about data and digital infrastructure."[69] Second, the Canadian Civil Liberties Association filed a suit against Waterfront Toronto in addition to the governments of Toronto, Ontario, and Canada.[70] The suit alleges that the "Quayside Agreements empower Sidewalk Labs and others to effect historically unprecedented, non-consensual, inappropriate

---

65. Jesse Halfon, *A Lawyer Explains Why Electric Scooter Laws Don't Work*, CITYLAB (June 28, 2019), https://www.citylab.com/perspective/2019/06/electric-scooters-dockless-regulations-liability-helmet-laws/592861/ [https://perma.cc/B346-9DXU].

66. Henry Grabar, *Building Googletown*, SLATE (Oct. 25, 2017), http://www.slate.com/articles/technology/metropolis/2017/10/sidewalk_labs_quayside_development_in_toronto_is_google_s_first_shot_at.html [https://perma.cc/5MA6-4UEV].

67. *See* Dan Bilefsky, *Toronto's City of Tomorrow Is Scaled Back Amid Privacy Concerns*, N.Y. TIMES (Oct. 31, 2019), https://www.nytimes.com/2019/10/31/world/canada/toronto-google-sidewalk.html [https://perma.cc/54XD-WRP5].

68. Josh O'Kane, *Ontario Government to Fire Three Waterfront Toronto Directors Over Sidewalk Labs Partnership*, GLOBE & MAIL (Dec. 7, 2018), https://www.theglobeandmail.com/canada/toronto/article-ontario-government-to-fire-three-waterfront-toronto-directors-over/ [https://perma.cc/FFJ2-XEZH]; Jordan Pearson, *Toronto Advisor Resigns Over Data Concerns with Google's Smart City Project*, VICE: MOTHERBOARD (Oct. 4, 2018), https://www.vice.com/en_us/article/3km74w/google-smart-city-in-toronto-advisor-resigns-data-privacy [https://perma.cc/9CKJ-KDWJ].

69. Pearson, *supra* note 68.

70. *CCLA v. Waterfront Toronto, et. al: Public Court Documents to Date*, CANADIAN C.L. ASS'N (June 24, 2019), https://ccla.org/quayside-project-application-documents/ [https://perma.cc/76AK-CWN4].

mass-capture surveillance and [the] commoditization of personal data of individuals who live in, work in or visit Quayside."[71] As a result of the popular backlash, the Quayside project has been significantly scaled back.[72]

To a certain extent, the setback of some smart cities technology and projects, like burdensome regulations on micromobility solutions and truncations to the Quayside project, was the inevitable result of a bubble of excitement and hype that was unsustainable and bound to burst. Yet, many of these specific problems are far from inevitable and are primarily issues tied to public opinion. Concerns about smart city technology, especially as related to privacy, should not be as damaging as they first appear and should be surmountable for two major reasons.

First, most of the setbacks related to smart city technology are centered around privacy concerns that, while important, reflect only a subset of smart city technologies. From wooden building construction to public transit optimization, to smart sewers and trashcans, many of the technologies with the most potential are uncontroversial. They raise few, if any, privacy concerns, especially if designed correctly from the outset. Returning to the example of South Bend, Indiana, the installed sensors under manhole covers dramatically increased the efficiency of water management in their sewers and allowed them to forgo expensive infrastructure upgrades.[73] As with any technology that attaches internet-enabled sensors to objects, many pieces of smart city technology are part of the Internet of Things (IoT). But sensors installed inside trashcans or under manhole covers generally do not present privacy concerns or a security danger if hacked. Projects can disentangle uncontroversial smart cities technologies such as improved construction techniques and materials, increased energy efficiency, and less-problematic sensors. Projects that focus on timber construction, optimizing bus routes, and unobjectionable sensors can advance while leaving behind technologies that rely on facial recognition, collecting personal data from smartphones, and

---

71. James McLeod, *Civil Liberties Group Sues to Quash Sidewalk Labs Project, with Final Master Plan Due Within Weeks*, FIN. POST (Apr. 17, 2019), https://business.financialpost.com/technology/civil-liberties-group-sues-to-quash-sidewalk-labs-project-with-final-master-plan-due-within-weeks [https://perma.cc/7Y56-QN72].

72. Bilefsky, *supra* note 67.

73. Greg Swiercz, *Sensors Help Combat Sewer Problems in South Bend, Ind.*, GOV'T TECH. (Feb. 15, 2017), http://www.govtech.com/fs/Sensors-Help-Combat-Sewer-Problems-in-South-Bend-Ind.html [https://perma.cc/5Q6U-73MR]; *supra* note 45 and accompanying text.

other sources. Even if privacy concerns related to personal data cannot be overcome, it should be possible to move forward with many innovations, which raise fewer objections.

Second, privacy issues around smart cities arise primarily from concern over what private companies, such as Google's Sidewalk Labs, will do with the potentially tremendous quantity, and unprecedented quality, of data that smart city infrastructure allows them to collect.[74] Considering the high costs and technology involved in most smart city projects, private companies are probably an inevitable part of advancing smart cities. In the United States, repeated revelations about how large technology companies collect, store, use, and abuse our data has damaged the public's trust.[75] Yet, stricter laws and enforcement in the European Union have led to a higher level of public trust that private companies will handle their data appropriately — and face repercussions if they do not.[76] While it would be an uphill battle, companies and governments in North America need to help improve attitudes toward smart city technology by building a successful track record of protecting people's data, thereby making the public more willing to trust smart cities with increased data collection. Increased trust that data is sufficiently protected will ultimately increase people's trust in the companies collecting such data, as well as the government's regulation of these companies.

Increased skepticism over and pushback to even fairly straightforward applications of smart cities technologies seems likely to delay the development and implementation of smart cities in democracies. In a liberal democracy with a robust rule of law, new technology that interacts with the public sphere, as most smart city technology does, requires at least a reasonable amount of public acceptance of the new technology. This trust can be built with

---

74. *See generally* Zaheer Allam, *The Emergence of Anti-Privacy and Control at the Nexus between the Concepts of Safe City and Smart City*, 2 SMART CITIES 96 (2019); Ellen P. Goodman & Julia Powles, *Urbanism under Google: Lessons from Sidewalk Toronto*, 88 FORDHAM L. REV. 457 (2019); Rob Walker, *Privacy, Equity, and the Future of the Smart City*, Lincoln Inst. of Land Pol'y: Land Lines Mag., January 2019.

75. *See* Kim Hart, *Americans Don't Trust Tech Companies on Data Privacy*, AXIOS (Apr. 23, 2018), https://www.axios.com/distrust-social-media-firms-to-protect-privacy-survey-8b95db51-f137-46e3-a239-a5f304f0ac1b.html [https://perma.cc/97A4-QDF9].

76. Luc Burgelman, *Council Post: GDPR and the Trusted Framework for Data Privacy*, FORBES (June 21, 2018, 9:00 AM), https://www.forbes.com/sites/forbestechcouncil/2018/06/21/gdpr-and-the-trusted-framework-for-data-privacy/ [https://perma.cc/C6D2-W7M9].

increased transparency, education, and open dialogue, which the public values but is ultimately a time-consuming process. The idea that deliberative processes in democracies would delay development that otherwise could rapidly move ahead has been seen in previous instances — as has the fact that the PRC often ignores these concerns and speeds ahead. For example, in 2008, *The Economist* noted that "it took as long to conduct a public inquiry into the proposed construction of Heathrow's Terminal Five as it took to build Beijing's new airport terminal from scratch."[77] Because the concerns raised by smart cities are newer and more complex, the time gap between development in democracies and China is likely to be, and become, even wider.

Privacy concerns can hold up the development of smart city projects in part because many smart city innovations are popularly seen as making a relatively small contribution, or even as providing a frivolous luxury. Yet, delays in the development of smart cities projects are potentially incredibly damaging for two reasons. First, some of the problems that smart cities help address, especially climate change,[78] are so acute that there is little time to lose. Second, if companies in the United States and other democracies are substantially delayed in their development of smart cities projects, this will only increase the advantage of companies that are based in the PRC, which will then increase the use of Chinese smart cities technology across the world.[79] As this Article argues, the technology developed and sold by PRC-based companies is likely to lack basic privacy protections, empower authoritarians, and perhaps even make countries who utilize the technology vulnerable to the PRC.

D. Privacy Challenges for Smart Cities

Because almost any definition of smart cities involves the effective collection and use of data to improve city governance and services,

---

77. *China's Infrastructure Splurge — Rushing on by Road, Rail and Air*, ECONOMIST (Feb. 14, 2008), https://www.economist.com/briefing/2008/02/14/rushing-on-by-road-rail-and-air [https://perma.cc/DRW9-FC4S].

78. *See* Andrew Howard, *Do Only "Smart Cities" Have the Answer?*, SCHRODERS (July 21, 2017), https://www.schroders.com/en/insights/economics/do-only-smart-cities-have-the-answer/ [https://perma.cc/JP2B-KRA9].

79. Allison Graham, *China Is Pulling Ahead of North America on Smart Cities*, BELFER CTR. FOR SCI. & INT'L AFF. (July 10, 2019), https://www.belfercenter.org/publication/china-pulling-ahead-north-america-smart-cities [https://perma.cc/FUR2-G2AP].

concerns about data and privacy are inevitable and imminently reasonable. According to Lilian Edwards, Professor of E-Governance at the University of Strathclyde, the key security challenges faced by smart cities are: (1) a lack of meaningful consent; (2) private data collected from public interactions; (3) privatization of both infrastructure and data; (4) repurposing data from the IoT; and (5) storage of data in the cloud.[80] There is no perfect solution to these problems; a balance needs to be struck between protecting people's data and using data for the public good, from fighting climate change to improving city services. The costs in terms of lost privacy and other concerns need to be balanced with the lost opportunity cost of *not* implementing these technologies. Giving up on technologies that help fight climate change or provide better public transit and other city services to underserved neighborhoods may be too high a price to pay to protect certain types of personal data. More important than any specific solution to these challenges is the need for ongoing dialogue about how to handle data in an inclusive, consistent, and transparent manner, which will, in turn, facilitate meaningful trust among the public.

Public backlash against smart city projects has the potential to derail even uncontroversial elements of smart cities. The Quayside project, for example, intends to take unprecedented steps by using wood as its primary building material for buildings up to 35 stories.[81] Because concrete is a major contributor to carbon dioxide emissions, and wood is renewable, lighter, and an excellent way of storing excess carbon, the Quayside project could pilot innovation by making a major contribution towards climate change reduction.[82] However, while Sidewalk Labs tried to highlight its innovative wood construction, both the public and its own advisory panel pushed back against the project based on other privacy concerns[83] regarding how data would be collected and used by a private company.[84] Saadia

---

80. *See* Lilian Edwards, *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective*, 2 EUR. DATA PROT. L. REV. 28, 28 (2016).

81. Kira Barrett, *Sidewalk Labs Is Building a Smart City Entirely of Mass Timber. What Could Go Wrong?*, SMART CITIES DIVE (Aug. 5, 2019), https://www.smartcitiesdive.com/news/sidewalk-labs-mass-timber-CLT-buildings-green-materials-waterfront-toronto-construction/560045/ [https://perma.cc/5J75-8D6U].

82. *Id.*

83. Pearson, *supra* note 68.

84. Leyland Cecco, *"Surveillance Capitalism": Critic Urges Toronto to Abandon Smart City Project*, GUARDIAN (June 6, 2019), https://www.theguardian.com/cities/2019/jun/06/toronto-smart-city-google-project-privacy-concerns [https://perma.cc/F2RH-RK5M].

Muzaffar, a member of Waterfront Toronto's Digital Strategy Advisory Panel who resigned, described the problem with the public consultation process. She argued that instead of addressing privacy concerns, "time was spent [by Waterfront Toronto] . . . talking about buildings made of wood and the width of one-way streets, things no one has contested or expressed material concern for in this entire process."[85] If Sidewalk Labs and other companies spearheading smart cities efforts[86] cannot create strategies to overcome concerns about their projects, especially related to privacy, then even the popular elements of their plans might be abandoned — or at least significantly delayed. The cost to society and the planet in terms of lost opportunity could be significant. The opportunities that such delays present to Chinese companies, on the other hand, which have less concern for privacy and transparency, could be even larger.[87]

II. CHINA

Part II examines the development of smart city technology in the PRC. We give particular attention to four cases: Alibaba's City Brain, the monitoring of Xinjiang, China's social credit system, and other uses of facial recognition technology. Finally, we summarize and draw conclusions based on what these fairly different applications of technology tell us as a whole.

Across a variety of industries that include smart cities and related technologies, China's companies are increasingly competitive with their counterparts from North America, out-innovating them in a variety of fields, from artificial intelligence to 5G.[88] Several factors help make China a world-leader in smart cities: First, the tremendous size of the Chinese market, in terms of both population and GDP.[89] Second, the state uses strategic investment, tax incentives, and a variety of other inducements and policies to support Chinese companies, seeking to make the PRC a world-wide leader in technology and innovation. The "Made in China 2025" initiative has formalized these policies into a prominent national campaign aimed

---

85. Pearson, *supra* note 68.

86. *See These Are the Top Ten Companies That Build Smart Cities*, *supra* note 3 (listing the top companies that help build smart cities).

87. *See infra* Section III.C.

88. *See* Graham, *supra* note 79.

89. Anja Kielmann, *Chinese Tech Companies Are Leading the New Global Innovation Revolution*, DRUM (Nov. 14, 2019), https://www.thedrum.com/opinion/2019/11/14/chinese-tech-companies-are-leading-the-new-global-innovation-revolution [https://perma.cc/7E3A-YNBR].

at making China a global technological superpower and costing the state at least hundreds of billions of dollars.[90] Third, the state further assists Chinese companies by blocking foreign firms from operating in spaces that it deems "sensitive," especially search and social media. Prominent examples include the blocking of Facebook, Google, and Twitter.[91] This not only allows China greater control over industries and applications it deems "sensitive," but has allowed other Chinese technology companies to fill a space that American firms otherwise dominate in most of the world. Fourth, and most important to our argument, Chinese companies enjoy an advantage when it comes to smart cities technology because they face relatively little need to deal with issues related to privacy, public opinion, or other concerns about the implementation of new technology. Chinese companies working in conjunction with the state can power ahead in implementing technology with little concern for public opinion and even less worry about legal or political setbacks of the kind Quayside faced.

The PRC's rapid rise to dominance in several high technology fields, especially renewable energy, provides an instructive example for the possible future of many smart city technologies. Beginning in the 1990s, China invested heavily in renewable energy with a particular focus on photovoltaic panels (PVs). In total, the Chinese state may have contributed as much as $47 billion to build its solar manufacturing industry.[92] The results were even more impressive. "Between 2008 and 2013, China's fledgling solar-electric panel industry dropped world prices by 80 percent."[93] China leapfrogged previous market leaders — the United States, Germany, and Japan — not only in production but also in patents. Its current market dominance in the industry seems, at least for the time being, unassailable.

It is often claimed that the Chinese are more likely to embrace new technology than people in other countries, especially wealthy democracies, because the population as a whole is less distrusting of it. "'Chinese are much more willing to try something new just

---

90. MAX J. ZENGLEIN & ANNA HOLZMANN, EVOLVING MADE IN CHINA 2025 8 (2019).

91. Paige Leskin, *Here Are All the Major US Tech Companies Blocked Behind China's 'Great Firewall'*, BUS. INSIDER (Oct. 10, 2019), https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5 [https://perma.cc/GE2Z-EDT8].

92. John Fialka, *Why China Is Dominating the Solar Industry*, SCI. AM. (Dec. 16, 2016), https://www.scientificamerican.com/article/why-china-is-dominating-the-solar-industry/ [https://perma.cc/A5CN-LUS8].

93. *Id.*

because it looks cool,' said Andy Tian, Chief Executive of Beijing-based Asia Innovations Group, which runs mobile applications. 'It sounds superficial. It is superficial. But that's the driver of progress [in the PRC] in a lot of cases.'"[94] This general enthusiasm for technology may help overcome concerns about privacy and other issues. Some data likewise suggests that Chinese consumers are more comfortable with a variety of technologies likely to figure into smart city projects.[95] In the most extreme cases, Chinese and Americans take the opposite view of technology. A survey by OC&C Strategy Consultants found that 70% of Americans say that they would not trust an autonomous vehicle, while 72% of Chinese said they would.[96] Yet, not all results are clear cut, and the causes and nature of Chinese attitudes towards privacy and technology is worth further examination.

In 2018, the CEO of Baidu, China's biggest search engine, publicly stated: "I think Chinese people are more open or less sensitive about the privacy issue. If they are able to trade privacy for convenience, for safety, for efficiency, in a lot of cases they're willing to do that."[97] The comments reflected a reasonably common point of view but were also met with significant public criticism. When it comes to online privacy, the gap between Chinese and Western attitudes is less extreme but still appears to be significant. A 2019 survey by Ipsos Group found that only 11% of Chinese were very concerned about their online privacy, compared to 26% of respondents in the United States.[98] The overall numbers of those who were concerned or very concerned were similar at 68% and 78% respectively.[99] Chinese lack of concern seems even more dramatic because it puts China in similar

---

94. Mozur, *supra* note 57.

95. *See* Gil Press, *Would You Trust a Self-Driving Car? 70% of Americans Say 'No,' 72% of Chinese Say 'Yes'*, FORBES (Dec. 16, 2019), https://www.forbes.com/sites/gilpress/2019/12/16/would-you-trust-an-autonomous-vehicle-70-of-americans-say-no-72-of-chinese-say-yes/ [https://perma.cc/VTN5-HZ3L].

96. *Id.*

97. Xinmei Shen, *Chinese Internet Users Criticize Baidu CEO for Saying People in China Are Willing to Give Up Data Privacy for Convenience*, S. CHINA MORNING POST (Mar. 28, 2018), https://www.scmp.com/tech/big-tech/article/3028402/chinese-internet-users-criticize-baidu-ceo-saying-people-china-are [https://perma.cc/99BM-NAWP].

98. IPSOS PUB. AFFAIRS, CTR. FOR INT'L GOVERNANCE INNOVATION, INTERNET SECURITY, ONLINE PRIVACY & TRUST 8 (2019), https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%201%20%26%202%20Internet%20Security%2C%20Online%20Privacy%20%26%20Trust.pdf [https://perma.cc/HAB5-FKYN].

99. *Id.*

territory, primarily with wealthy and well-run democracies such as Japan, Germany, and Sweden.[100] Countries more similar to China, in terms of development and political system, tended towards the other end of the scale; in Egypt, India, Nigeria, South Africa, Mexico, Korea, Brazil, and Tunisia, over 40% reported being very concerned about online privacy.[101] That China looks more like well-run wealthy democracies than developed countries hints at a theme that will be examined later in this Article: for a middle-income authoritarian regime, China seems to be uniquely capable and trusted by its own people.[102]

As China becomes wealthier, better-educated, and more tech-savvy, it is possible that attitudes towards online privacy are shifting. Both the Ipsos poll and a report by Kantar China Insights, a media consultancy, suggest that concern about personal privacy online is growing.[103] There is even evidence that the Chinese state is responding to increasing concerns about online data privacy.[104] China's new e-commerce law, which took effect in 2019, contains important provisions for protecting the privacy of consumers.[105]

How any given Chinese person or the country as a whole feels about sacrificing privacy may matter less when the state and powerful tech companies act as though Chinese care little about privacy. Ordinary Chinese people have relatively little control over the rapidly growing use of a wide variety of technologies with the serious potential to infringe on their privacy.[106] In meaningful ways, Chinese

---

100. *See id.*

101. *Id.*

102. *See infra* Section II.E.

103. *See* IPSOS PUBLIC AFFAIRS, *supra* note 98; Guo Min (郭敏), *2017 Kaidu Zhongguo Shejiaomeiti Yingxiang Baogao* (2017 凯度中国社交媒体影响报告), KANTAR (June 6, 2017), https://cn.kantar.com/媒体动态/社交/2017/2017凯度中国社交媒体影响报告/ [https://perma.cc/AYH4-2TQC].

104. *See* Winston Wenyan Ma, *China Is Waking Up to Data Protection and Privacy. Here's Why That Matters*, WORLD ECON. FORUM (Nov. 12, 2019), https://www.weforum.org/agenda/2019/11/china-data-privacy-laws-guideline/ [https://perma.cc/HP8P-US72].

105. *See* Sara Xia, *Implications of China's E-Commerce Law*, AMCHAM SHANGHAI (Apr. 7, 2019), https://www.amcham-shanghai.org/en/article/implications-chinas-e-commerce-law [https://perma.cc/39AY-2FWM].

106. *See* "Cha Pingjun," *Zhongguoren budebu Yong Yinsi Jiaohuan Bianlixing* (中国人不得不用隐私交换便利性。), WECHAT OFFICIAL ACCTS. PLATFORM (微信公众平台) (Mar. 26, 2018), http://mp.weixin.qq.com/s?__biz=MzA5NDc1NzQ4MA==&mid=2653328398&idx=1&sn=f0b7524eddf6b86aa2b4a14bfba0f690&chksm=8b9b8309bcec0a1f5a2910a44befac

citizens have already been forced to accept technology[107] that many in developed democracies remain skeptical of or even openly resist.[108] In major Chinese cities, mobile phone-based payment systems, like Alipay and WeChat Pay, are so pervasive that using cash or credit cards falls between inconvenient and impossible, even for low-value face-to-face transactions like buying a bottle of water. Similarly, WeChat (Weixin) — an application that serves messaging, payment, and many other functions — is so ubiquitous that it is difficult to live a normal life or conduct business without it.[109] It is possible, therefore, that to the extent the Chinese do have laxer attitudes about potential privacy-infringing technology, this is a consequence of an environment where there is relatively little choice but to opt into such technology, irrespective of overriding privacy concerns. Additionally, the market dominance of a few national champions with close ties to the state gives consumers few choices in terms of competing providers that might take their privacy more seriously.[110]

The advantage that Chinese companies have as a result of being able to largely ignore privacy concerns and many other regulatory hurdles is clear to Chinese companies, the state that supports them, and their competitors.[111] In the words of Dong Tao, Vice Chairman for Greater China at Credit Suisse Private Banking Asia Pacific, "I'm not saying Chinese companies are better than American companies, I'm not saying Chinese engineers are better than American engineers. What will make China be big in AI and big data is: China has no serious law protecting data privacy."[112] As the following Sections show, these advantages allow for Chinese companies to be involved in projects that companies in Europe or North America could not even contemplate.

---

b09b781e71dcc62f3df7cc516006f64c8a19b5d3ba688d#rd [https://perma.cc/P7Q8-RB23].

107. *See* Shen, *supra* note 97.

108. PEW CHARITABLE TRS., ARE AMERICANS EMBRACING MOBILE PAYMENTS? (2019), https://www.pewtrusts.org/-/media/assets/2019/10/mobilepayments_brief_final.pdf [https://perma.cc/Q2Y6-QX5N].

109. *See* Audrey Jiajia Li, *Learning to Survive Without WeChat*, N.Y. TIMES (Sept. 20, 2018), https://www.nytimes.com/2018/09/20/opinion/learning-to-survive-without-wechat-in-china.html [https://perma.cc/4NFH-6QML].

110. *See* "Cha Pinjun," *supra* note 106.

111. *See* Yen Nee Lee, *China Will Win the A.I. Race, According to Credit Suisse*, CNBC (Mar. 22, 2018), https://www.cnbc.com/2018/03/22/credit-suisse-china-will-win-the-ai-race-due-to-lack-of-serious-laws-on-data-protection.html [https://perma.cc/5R3A-NADX].

112. *Id.*

It is unclear, however, if all the advantages that Chinese companies currently enjoy will last. Perhaps precisely because it is not a democracy, the Chinese state is very sensitive to public opinion.[113] Its supportive attitude of companies that care little for its citizens' privacy may change if the state becomes seriously concerned that attitudes of average Chinese people are shifting to more closely match the higher levels of concern visible in other middle-income countries. This would be similar to improvements made in air quality that China experienced as a result of public backlash against high-levels of air pollution, helping to shift the government's previously laissez-faire attitude about heavy polluters.[114]

In the Sections below, this Article considers three of the PRC's largest-scale and most Orwellian uses of data in the public sphere, as well as several smaller-scale examples of the use of facial recognition technology in the PRC.

A. City Brain

If Sidewalk Lab's Quayside project is the ambitious but problematic poster child for smart cities in wealthy democracies, it pales in comparison to China's most important smart city project, Alibaba's City Brain.[115] According to Xian-Sheng Hua of Alibaba Group's DAMO Academy (Academy for Discovery, Adventure, Momentum, and Outlook):

> City Brain is an end-to-end system whose goal is to glean irreplaceable values from big city data, specifically from videos, with

---

113. *See* Jidong Chen et al., *Sources of Authoritarian Responsiveness: A Field Experiment in China*, 60 AM. J. POL. SCI. 383, 383–84 (2016); Jonathan Hassid, *China's Responsiveness to Internet Opinion: A Double-Edged Sword*, 44 J. CURRENT CHINESE AFF. 39, 39–68 (2015).

114. *See* Meir Alkon & Erik H. Wang, *Pollution Lowers Support for China's Regime: Quasi-Experimental Evidence from Beijing*, 80 J. POL. 327, 327–31 (2018); Ling Li et al., *Public Participation in Achieving Sustainable Development Goals in China: Evidence from the Practice of Air Pollution Control*, 201 J. CLEANER PRODUCTION 499, 499–506 (2018); Xiaowen Zhang, *The Reemerging Concern Over Air Pollution in China: The Smog of the State's Efforts to Guide Public Opinion*, 23 J. CHINESE POL. SCI. 519, 519–20 (2018).

115. Xian-Sheng Hua, *The City Brain: Towards Real-Time Search for the Real-World*, *in* THE 41ST INTERNATIONAL ACM SIGIR CONFERENCE ON RESEARCH AND DEVELOPMENT IN INFORMATION RETRIEVAL 1343–44 (2018) [hereinafter Hua, *Towards Real-Time Search*]; *see* Xiansheng Hua et al., *The City Brain: Practice of Large-Scale Artificial Intelligence in the Real World*, 1 IET SMART CITIES 1, 1 (2019) [hereinafter Hua et al., *Practice of Large-Scale AI*]; *see also* Abigail Beall, *In China, Alibaba's Data-Hungry AI Is Controlling (and Watching) Cities*, WIRED (May 30, 2018), https://www.wired.co.uk/article/alibaba-city-brain-artificial-intelligence-china-kuala-lumpur [https://perma.cc/ZG7G-WPU8].

> the assistance of rapidly evolving AI technologies and fast-growing computing capacity. From cognition to optimization, to decision-making, from search to prediction and ultimately, to intervention, City Brain improves the way we manage the city, as well as the way we live in it.[116]

In short, City Brain appears to be an effort to collect, consolidate, analyze, and implement as much data relevant to city functions as digitally possible.

Currently, City Brian has five major applications: (1) monitoring city "vital signs" such as traffic across multiple modes of transport; (2) monitoring for public security purposes; (3) improving traffic on a micro-level (controlling traffic lights and transit routes and departures); (4) route optimization for emergency response vehicles; and (5) assisting with urban planning.[117] According to Alibaba, "utilizing comprehensive real-time city data, City Brain holistically optimizes urban public resources by instantly correcting defects in urban operations. This has led to numerous breakthroughs in urban government models, service models, and industrial development."[118] As with Quayside and other smart cities projects in wealthy democracies, many of the most beneficial applications of the technology, such as optimizing traffic, emergency services, and public transport, are likely to be popular and are relatively unobjectionable from a privacy standpoint. The public security applications, however, are a very different matter.

In a way, City Brain is the logical conclusion of an effort that started on the other side of the world when the United Kingdom installed four closed-circuit cameras in Trafalgar Square in 1960.[119] Since then, the United Kingdom has led the world as one of the most surveilled countries, with a total of around 5.9 million closed-circuit television cameras.[120] While the amount of video collected is enormous, however, the system is old, "a muddle of more than a

---

116. Hua, *Towards Real-Time Search*, *supra* note 115.

117. Hua et al., *Practice of Large-Scale AI*, *supra* note 115, at 1.

118. *City Brain: Empower Cities to Think with Data-Driven Governance*, ALIBABA CLOUD, https://www.alibabacloud.com/et/city [https://perma.cc/QDA8-M4KM] (last visited Dec 19, 2019).

119. *See* Jess Young, *A History of CCTV Surveillance in Britain*, SWNS (Jan. 22, 2018), https://stories.swns.com/news/history-cctv-surveillance-britain-93449/ [https://perma.cc/34KU-R8VM].

120. David Barrett, *One Surveillance Camera for Every 11 People in Britain, Says CCTV Survey*, TELEGRAPH (July 10, 2013), https://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html [https://perma.cc/SY8B-GK96].

thousand video formats, poor quality footage and manual processing."[121] The footage is used primarily as a tool for review by specially trained police to use after an incident has already taken place. "In the aftermath of the London riots in August 2011 police scoured through more than 200,000 hours of CCTV to identify suspects. Around 5,000 offenders were found by trawling through the footage, after a process that took more than five months."[122] While meaningful efforts to modernize, improve, and automate at least parts of the United Kingdom's dilapidated system are underway, the process will be expensive and lengthy. As the United Kingdom advances these efforts, it has already experienced pushback about the use of facial recognition and biometric tracking information that the CCTV network would need to become more automated and produce data in real-time.[123] In particular — with the details of the United Kingdom's post-Brexit relationship with Europe still to be worked out — the United Kingdom's use of these technologies will face meaningful constraints in the form of the European Union's General Data Protection Regulation (GDPR), which this Article will later examine.[124]

City Brain's public security functions are essentially trying to recreate the efforts of the London police in 2011, but with automation, programming City Brain to work in real-time, and even make predictions. This level of surveillance may have already, or may not, surpass that of regimes like Communist East Germany[125] or, indeed, Mao-era China.[126] But even if it does not, City Brain efforts offer massive advantages in terms of efficiency and precision. At the time of its collapse, East Germany had more than 260,000 people, or

---

121. James Temperton, *One Nation Under CCTV: The Future of Automated Surveillance*, WIRED (Aug. 17, 2015), https://www.wired.co.uk/article/one-nation-under-cctv [https://perma.cc/NCR2-G8KY].

122. *Id.*

123. *See* Shannon Togawa Mercer & Ashley Deeks, *'One Nation Under CCTV': The U.K. Tackles Facial Recognition Technology*, LAWFARE (May 7, 2018), https://www.lawfareblog.com/one-nation-under-cctv-uk-tackles-facial-recognition-technology [https://perma.cc/E4V4-MGFM].

124. *See id.*; *see also infra* Section III.B.

125. John Torpey, *From Surveillance Communism to Surveillance Capitalism and Beyond*, FORBES (Nov. 8, 2019), https://www.forbes.com/sites/johntorpey/2019/11/08/from-surveillance-communism-to-surveillance-capitalism-and-beyond/ [https://perma.cc/TZ3K-7JLS].

126. Mao-era China involved exceptionally high levels of surveillance. *See* Elizabeth Economy, *China's Neo-Maoist Moment*, FOREIGN AFF. (Oct. 1, 2019), https://www.foreignaffairs.com/articles/china/2019-10-01/chinas-neo-maoist-moment [https://perma.cc/P5SU-ZYWF].

2% of its population, working full or part-time for its secret police.[127] The comparable figure for the PRC would be approximately 28 million, about four times the number of civil servants currently working in China.[128] City Brain would seem to be able to provide a similar level of surveillance at a tiny fraction of the cost. Additionally, according to Alibaba's researchers, the technology is both much faster and much better at identifying people than a human; they claim that the system was able to locate people in security footage from a single photo, even if that photo was from behind.[129] This identification technology has many worthy applications, from preventing terrorist attacks and mass shootings to finding missing children. Nevertheless, the potential for an authoritarian regime that could identify and track the comings and goings of every individual in a city in real-time is staggering and perhaps not that far off. The further the technology spreads beyond China, the more authoritarians or potential authoritarians could have access to this surveillance of unprecedented efficiency and effectiveness.

As with many smart cities or big data projects, City Brain collects and stores large amounts of data on the cloud.[130] The storage of such large amounts of potentially sensitive data poses challenges — even for companies in jurisdictions that are more concerned with data security and privacy. But large Chinese technology companies' lack of concern with privacy, and their close relationship with the state, make these concerns even more serious.[131] Without a government regulating the collection, storage, and protection of data and with little fear of retribution from a state heavily invested in its success, Alibaba — or any company in a similar position — has little reason to take adequate measures to secure its data and systems. Even fairly basic smart traffic control systems offer a prime target for hackers,[132]

---

127. *Can Technology Plan Economies and Destroy Democracy?*, ECONOMIST (Dec. 18, 2019), https://www.economist.com/christmas-specials/2019/12/18/can-technology-plan-economies-and-destroy-democracy [https://perma.cc/EDL7-968M].

128. Cai Shenkun (蔡慎坤), *Shouci Pilu Gongwuyuan Zongshu You Shei Xin?* (首次披露公务员总数有谁信？), EPOCH TIMES (大纪元) (June 26, 2016), http://www.epochtimes.com/gb/16/6/26/n8037944.htm [https://perma.cc/E5US-7D96].

129. *See* Hua et al., *Practice of Large-Scale AI*, *supra* note 115, at 10.

130. *See id.*

131. Louise Lucas, *China Government Assigns Officials to Companies Including Alibaba*, FIN. TIMES (2019), https://www.ft.com/content/055a1864-ddd3-11e9-b112-9624ec9edc59 [https://perma.cc/RC5V-KL3J].

132. *Id.*

and as one of the most ambitious systems ever conceived, City Brian provides an expansive attack surface area.

Concern that Alibaba and those that buy its smart cities products will not take the security of its data seriously is more than theoretical. In 2019, John Wethington of data security firm Condition:Black discovered that a sizable Chinese smart city database was easily accessible online, not even protected by a password.[133] Although the owner of the data was not explicit, it "made several references to the tech giant's artificial intelligence-powered cloud platform, City Brain, but Alibaba later denied its platform was used."[134] When the content of the database became clear, it not only raised concerns that such a large and sensitive dataset was going unprotected but also revealed the worrying scope of the data being collected and stored.

The unprotected data Wethington found was produced by the continual monitoring of "residents around at least two small housing communities in eastern Beijing, the largest of which is Liangmaqiao, known as the city's embassy district."[135] The data is collected through various means, most notably cameras enabled with facial recognition software. Using the data, it would be possible to construct a picture of an individual's coming and goings. It also identified the ethnicity of individuals, a worrying prospect given China's recent record of targeting Muslims for repression,[136] but also in many other contexts.[137] More concerning still, the data collected by cameras and processed by facial recognition software was linked to government records, including national identification card numbers and police records.[138] This clue also makes it likely that the Alibaba customer to whom the data belonged was a Chinese local government.[139] In a similar breach in January 2020, City Brain data from the Chinese cities of Luzhou and Hangzhou were uncovered.[140]

---

133. *See* Zack Whittaker, *Security Lapse Exposed a Chinese Smart City Surveillance System*, TECHCRUNCH (May 3, 2019), https://techcrunch.com/2019/05/03/china-smart-city-exposed/ [https://perma.cc/49H7-9JFX].

134. *Id.*

135. *Id.*

136. *See infra* Section II.B.

137. *See generally* James Leibold, *Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement*, 29 J. CONTEMP. CHINA 46 (2020) (discussing the surveillance of, and targeted repression against, Uyghur communities in the Xinjiang region of China).

138. Whittaker, *supra* note 133.

139. *See id.*

140. Lee Johnstone, *Smart Cities with Not-So-Smart Security — Again!*, DATABREACHES (Jan. 14, 2020),

Yet the worrying implications of City Brain's public security features and overall concerns about data collection and security are easy to overlook in favor of the tremendous potential of its other functions. Alibaba claims that its system is able to integrate data from map tools, traffic police microblog accounts, and videos to optimize traffic lights, taxi dispatch, and public transportation to reduce traffic, improve emergency vehicle response times, and reduce public transit delays.[141] The system was purported to be highly effective in its test city of Hangzhou, a major metropolis in China's silicon valley. After City Brain was given control of 104 traffic lights in one district of the city, traffic was reduced by 15% in the first year.[142] Additionally, in Hangzhou, ambulance response times dropped by 50%, and the accuracy of real-time traffic incident detection reached 95%.[143] In Shanghai, optimizing traffic light timing dropped travel time by 8% and roadway congestion by 15%.[144] Better still for traffic-clogged metropolises, researchers claimed that in Suzhou, in Jiangsu Province, "dynamic adjustment of bus departure time increased the number of people taking buses by 17%."[145] If these kinds of improvements are substantiated and reproducible in other contexts, cities around the world will and should be clamoring to get their own City Brains.

While the scope and scale of City Brain are impressive, it is the possibility for the rapid spread of the system that makes it perhaps the most important smart cities technology on the planet. A system that provides cities some relief from congestion without major infrastructure spending could be incredibly tempting even for a wealthy democracy that takes transparency and data privacy seriously. For the rapidly growing and increasingly congested cities of the developing world (the four cities with the world's worst traffic are Mumbai, Bogota, Lima, and New Delhi),[146] many of which have limited legal and democratic constrains, the appeal of City Brain may

---

https://www.databreaches.net/smart-cities-with-not-so-smart-security-again/ [https://perma.cc/LAF8-UFMZ].

141. *City Brain: Empower Cities to Think with Data-Driven Governance*, *supra* note 118.

142. Beall, *supra* note 115.

143. Hua et al., *Practice of Large-Scale AI*, *supra* note 115.

144. *Id.*

145. *Id.*

146. Niall McCarthy, *The World's Worst Cities for Traffic Congestion [Infographic]*, FORBES (June 5, 2019), https://www.forbes.com/sites/niallmccarthy/2019/06/05/the-worlds-worst-cities-for-traffic-congestion-infographic/ [https://perma.cc/2AGF-D3FX].

be irresistible. City Brain is already being deployed in cities across China, including Xiong'an New Area (near Beijing and Tianjin), Chongqing, Macau, Guangzhou, Shanghai, Hangzhou, and Suzhou.[147] Beyond China, Malaysia's capital, Kuala Lumpur, has already signed a contract to implement City Brain,[148] and if things go according to plan, this will be only the tip of the iceberg. Alibaba claims it "is already working with 120,000 developers and 2700 academic institutes and businesses from 77 countries and regions."[149]

Utility notwithstanding, there are good reasons to believe that the Chinese state can and will take advantage of the incredible data gathering power of City Brain. According to Christopher Ashley Ford, Assistant Secretary of State for International Security and Non-Proliferation at the United States Department of State:

> Firms such as Huawei, Tencent, ZTE, Alibaba, and Baidu have no meaningful ability to tell the Chinese Communist Party "no" if officials decide to ask for their assistance . . . . Such aid may not necessarily occur routinely, but it certainly can occur — and presumably will — whenever the Party considers this useful and cares to demand it.[150]

That the Chinese state will be able to use City Brain and similar technologies to help it monitor and control its citizens, therefore, is a virtual certainty. Yet, as City Brain spreads to cities across the globe, it is possible that the Chinese state will use its influence on Alibaba and other companies to gain an equal level of access in any and every city that implements Chinese smart city technology. This fear echoes and amplifies the existing concerns about the spread of Huawei's 5G technology, which are considered below.[151]

Further legitimate fears arise from concerns that as this technology spreads, City Brain-like systems might be built and controlled by purely private interests. In the words of John Wethington:

---

147. Hua et al., *Practice of Large-Scale AI*, *supra* note 115, at 10.

148. Zen Soo, *Alibaba Helps Malaysia Implement Smart City Programme*, S. CHINA MORNING POST (Jan. 29, 2018), http://www.scmp.com/tech/china-tech/article/2131006/chinas-alibaba-helps-malaysia-implement-smart-city-programme [https://perma.cc/Q6PA-H5R9].

149. Beall, *supra* note 115.

150. Christopher Ashley Ford, U.S. Asst. Sec'y of State, Huawei and Its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications, Remarks at the Multilateral Action on Sensitive Technologies (MAST) Conference (Sept. 11, 2019) (transcript available at https://www.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/ [https://perma.cc/CF5H-MYSV]).

151. *See infra* Section III.C.

> [I]t's not difficult to imagine the potential for abuse that would exist if a platform like this were brought to the U.S. with no civilian and governmental regulations or oversight . . . while businesses cannot simply plug in to FBI data sets today it would not be hard for them to access other state or local criminal databases and begin to create their own profiles on customers or adversaries.[152]

The potential for the private use and abuse of this data could be even greater in developing nations where governments would have less technical and regulatory ability or inclination to pushback against wealthy and powerful companies, most of which would be based in other countries.

B. Monitoring Muslims

China's Western provinces, especially Xinjiang, have long been areas discontented with PRC rule, which is both a cause and a result of repression against Muslim minorities.[153] The region has a long but troubled relationship with Beijing, with the Qing and subsequent Republican governments often only loosely controlling the region.[154] This culminated in a strong nationalist movement and even a brief period of independence in the 1930s and 1940s.[155] Since the rise of the PRC, however, Beijing has exerted increasingly tighter control over the region.[156] After 9/11, the PRC used the threat of Islamic terrorism to justify its repression, yet most of the discontent has surfaced in the form of ethnic riots, such as a major outbreak in the summer of 2009.[157]

The repression has stepped up since 2017, with at least 800,000 Muslims being detained in "re-education" camps.[158] In some ways,

---

152. Whittaker, *supra* note 133.

153. *See* James Griffiths, *China's Paranoia and Oppression in Xinjiang has a Long History*, CNN (Oct. 13, 2018), https://www.cnn.com/2018/10/11/asia/xinjiang-reeducation-muslim-china-intl/index.html [https://perma.cc/T79W-J4S5]. *See also generally* R. Harris, *Repression and Quiet Resistance in Xinjiang*, 118 CURRENT HIST. 276 (2019); Liselotte Odgaard & Thomas Galasz Nielsen, *China's Counterinsurgency Strategy in Tibet and Xinjiang*, 23 J. CONTEMP. CHINA 535, 535–55 (2014).

154. Griffiths, *supra* note 153.

155. *Id.*

156. *Id.*

157. *Id.*

158. Ishaan Tharoor, *The Cone of Silence Around China's Muslim 'Gulags'*, WASH. POST (Jan. 9, 2019), https://www.washingtonpost.com/world/2019/01/09/cone-silence-around-chinas-muslim-gulags/ [https://perma.cc/2VG8-DE34]. While it is hard to know much for certain about the methods or goals of the re-education camps, the general concept seems to

this is just a particularly extreme phase in ongoing cycles of repression. In 2010, for example, Beijing essentially turned off the internet in Xinjiang for ten months.[159] What makes this round of repression different and important for considering the future of smart cities is that the detentions and repression seem to be quietly supported by a sophisticated and massive effort to use data collection to target and sustain it.

In early 2018, Human Rights Watch (HRW), an international NGO, downloaded a smartphone application designed for use by Chinese officials in Xinjiang. The application is part of China's Integrated Joint Operations Platform (IJOP), an overarching system of mass surveillance in Xinjiang, and seems to have been created by a major Chinese military contractor. The goal of this effort seems to be an unprecedented level of surveillance and control of everyone in the province. Working with a Berlin-based security company to decipher and reverse engineer the application, HRW was able to assemble a picture of a remarkably data-intensive program of mass surveillance underway in Xinjiang.[160]

The IJOP, in large part, appears to be an effort to assemble every piece of information the government can learn about residents of Xinjiang, but what makes it so unprecedented is the overwhelming number of data sources the application can draw on.[161] Starting in 2017, authorities in Xinjiang began collecting biometrics, including DNA samples, fingerprints, iris scans, and blood types of all residents in the region between the ages of 12 and 65.[162] Additional information collected includes height, religious dress, beard length, electricity and gas usage, package deliveries, use of a home's back

---

be to de-radicalize, Sinicize, and generally compel Chinese Muslims (especially from the Uighur ethnic group) to accept Beijing's rule.

159. Edward Wong, *After Long Ban, Western China Is Back Online*, N.Y. TIMES (May 14, 2010), https://www.nytimes.com/2010/05/15/world/asia/15china.html [https://perma.cc/2S3K-FP4J].

160. Dholakia Nazish & Wang Maya, *Interview: China's 'Big Brother' App*, HUM. RTS. WATCH (May 1, 2019), https://www.hrw.org/news/2019/05/01/interview-chinas-big-brother-app [https://perma.cc/GNK2-FJQR].

161. MAYA WANG, HUMAN RIGHTS WATCH, CHINA'S ALGORITHMS OF REPRESSION: REVERSE ENGINEERING A XINJIANG POLICE MASS SURVEILLANCE APP 17 (2019), https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance [https://perma.cc/XU2F-3KRZ].

162. *China: Minority Region Collects DNA from Millions*, HUM. RTS. WATCH (Dec. 13, 2017), https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions [https://perma.cc/79AC-F7XT].

versus the front door, movements around cities and the province, police records, addresses, vehicle registration, as well as details on trips abroad.[163]

The breadth of the data collected is even more staggering once the detail of the information becomes clear. Information on packages, for example, includes not only basic information on the sender, intended recipient, and delivery company but also includes who received the package upon delivery, the date and time, X-rays, and photos of it.[164] Information on gas and electricity usage is presumably drawn from utility companies and financial information from banks, both of which are partially — if not completely — state-owned.[165] Information on the sending and delivery of packages is added and must come, at least in part, from private delivery companies. Cameras equipped with facial recognition, cross-referenced with existing government biometric data, provide much of the most important information on a person's comings and goings.[166] Physical checkpoints have been set up all over Xinjiang to check IDs, often in conjunction with facial recognition. Additionally, these checkpoints seem to have been quietly equipped with "data doors," special machines that detect and log the MAC addresses and IMEI numbers of any phones that pass through the checkpoint.[167] Similarly, the IJOP application seems to pick up and log wireless signals and their security features (a process called "wardriving").[168] While this level of data collection would certainly be ripe for a legal challenge elsewhere, even in China, it seems likely that the IJOP violates relatively limited restrictions on state surveillance.[169] Yet, mounting a legal or political challenge to the system would almost certainly be both dangerous and futile. While many actions of the local Chinese

163. WANG, *supra* note 161, at 17.

164. *Id.*

165. *See* XIAOTING ZHENG ET AL., PEOPLE'S REPUBLIC OF CHINA: DO PRIVATE WATER UTILITIES OUTPERFORM STATE-RUN UTILITIES? iv (2016), https://www.adb.org/publications/prc-private-water-utilities-outperform-state-run-utilities [https://perma.cc/UW3E-XK47]; Matthew Miller, *China's Banks Embrace Communist Party Committees in Risk Crackdown*, REUTERS (June 27, 2018, 1:48 AM), https://www.reuters.com/article/us-china-banks-party-idUSKBN1JN0XN [https://perma.cc/U8XD-CPQ9].

166. WANG, *supra* note 161.

167. *Id.*

168. Benjamin D. Kern, *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 101, 104 n.7 (2004).

169. WANG, *supra* note 161.

state can successfully and safely be challenged in court,[170] more politically sensitive cases, especially those relating to ethnic minorities, are beyond the pale. Taking such a case to court could lead to a wide variety of repressive responses from the state against both plaintiffs and their lawyers, including criminal prosecution.[171]

Once assembled, the information collected by the IJOP is used to identify "suspicious" individuals or situations.[172] Given the incredible breadth and depth of data available to it, the IJOP is surprisingly mechanistic in determining which individuals or situations are worthy of further scrutiny.[173] Instead of the big-data-worthy algorithms we might expect, the application seems to use "simple conditional statements — *if a, then b* (for example, if the person who drives the car is not the same as the person to whom the car is registered, then investigate this person)."[174] Having identified a person or situation for further review, the application then prompts low-level local officials to investigate. A pair of mock examples from HRW's reverse engineering of the application provides a sense of how the application is meant to function. The first example shows the extent to which investigations are prompted purely by when and where people are picked up by automated surveillance, such as facial recognition systems and data doors. This seems to work in combination with conclusions drawn from algorithms that glean characteristics like ethnicity and religiosity based on personal appearance: "suspicious person Zhang San, whose address is Xinjiang Urumqi, ID number 653222198502043265, phone number 18965983265. That person has repeatedly appeared in inappropriate locations, and he displays [or his clothing shows] strong religiousness." A second example shows how the application prompts officials to collect more data: "Suspicious person Maimaiti Muhemuti, who originally lives in Xinjiang's Urumqi, ID number

---

170. *See generally* John Wagner Givens, *Sleeping with Dragons? Politically Embedded Lawyers Suing the Chinese State*, 31 WIS. INT'L L.J. 101 (2013).

171. AMNESTY INT'L, AGAINST THE LAW: CRACKDOWN ON CHINA'S HUMAN RIGHTS LAWYERS DEEPENS 3 (2011), https://www.amnesty.org/download/Documents/28000/asa170182011en.pdf [https://perma.cc/6U9P-BSVZ]; *China: Torture and Forced Confessions Rampant amid Systematic Trampling of Lawyers' Rights*, AMNESTY INT'L (Nov. 12, 2015), https://www.amnesty.org/en/latest/news/2015/11/china-torture-forced-confession/ [https://perma.cc/M2R7-8A59]; Jonathan Kinkel & William Hurst, *Review Essay — Access to Justice in Post-Mao China: Assessing the Politics of Criminal and Administrative Law*, 11 J. EAST ASIAN STUD. 467, 478 (2011).

172. WANG, *supra* note 161.

173. *Id.*

174. *Id.* at 19.

653222198502043215, phone number 13803021458. Report time: 2017-09-25 14:01:53 [Mission] text: Please carefully investigate whether he still lives in Urumqi and investigate his family situation."[175] While this overall program of mass surveillance is overseen by the Public Security Bureau (the local police), personnel from other government agencies, state-owned enterprises, and public institutions have also been used to surveil people.[176] Surveillance may also include extended home visits,[177] which in 2017 amounted to an attempt to put one million government officials in the homes of Xinjiang residents.[178]

Visits by the prompted officials are meant to produce yet more information, which seems to be the main purpose of the IJOP application.[179] Officials are urged to add varied information to the IJOP through the application, from text and drop-down menus to audio and photos.[180] The investigation can also include "a phone search for software, network tools, or content that is problematic."[181] Fifty-one network tools are flagged as suspicious, including tools for circumventing online censorship, such as Virtual Private Networks (VPNs), and apps that allow for encrypted communication, like WhatsApp and Viber.[182] The surveillance does not end with the targeted minorities.

> The app also scores government officials on their performance in fulfilling tasks and is a tool for higher-level supervisors to assign tasks to, and keep tabs on the performance of, lower-level officials. The IJOP application, in part, aims to control government officials to ensure that they are efficiently carrying out the government's repressive orders.[183]

---

175. *Id.* at 29.

176. *Id.* at 18.

177. *China: Visiting Officials Occupy Homes in Muslim Region*, HUM. RTS. WATCH (May 13, 2018), https://www.hrw.org/news/2018/05/13/china-visiting-officials-occupy-homes-muslim-region [https://perma.cc/H9PT-PMCD].

178. *Xinjiang Qidong Minzu Tuanjie "Jieqin Zhou" Baiwan Ganbu Zhigong Fenpi Xia Jiceng* (新疆启动民族团结"结亲周"百万干部职工分批下基层), ZHONGYANG TONGZHANBU WANGZHAN (中共中央统一战线工作部) (Dec. 19, 2017), http://www.zytzb.gov.cn/tzb2010/S1824/201712/029ea48103254b359c754152e005c302.shtml [https://perma.cc/2HYM-TMH2].

179. WANG, *supra* note 161.

180. *Id.*

181. Nazish & Maya, *supra* note 160.

182. WANG, *supra* note 161, at 2.

183. *Id.* at 3.

While IJOP is likely to stay limited to Xinjiang or perhaps other minority-heavy areas of China, for the time being, the authoritarian possibilities its example hints at are terrifyingly Orwellian.

C. Social Credit System

Although it is currently only peripherally related to core smart city functions and extensively covered in both popular and academic publications, no discussion about data security in the PRC could be complete without a brief mention of China's rapidly expanding social credit systems (SCS). The "Planning Outline for the Construction of a Social Credit System," released in 2014 by the State Council (the PRC's chief administrative authority), provides an authoritative direction on what the PRC seeks to accomplish with SCS.[184]

> [The plan] focused on the creation of the underlying information infrastructure that would be required for the system's successful rollout. It systematically provided for standardized means to record credit-related information in different sections of the administration, databases to store this information at the central and local levels, the establishment of credit reporting mechanisms to enable public access to the information, as well as information sharing processes in order to counter the siloing of data within the bureaucracy.[185]

This data is then used to implement a system of rewards and punishments implemented with implications for interactions with both the state and the market. Black (bad) and red (good) lists would be created to punish and reward people.[186] Being on the blacklist could result in serious consequences for an individual, and even their family who might find themselves "unable to purchase high-speed train tickets, fly on an airplane, or send [their] kids to a private school."[187] Despite assertions to the contrary, especially in the popular press, what does not seem to be present in the creation of the SCS are the types of big data algorithmic analyses that are at work in the City Brain project.[188] Essentially, the SCS appears to be a far broader and more authoritarian use of the types of credit rating

---

184. Rogier Creemers, China's Social Credit System: An Evolving Practice of Control 13 (May 22, 2018) (unpublished manuscript) (on file with Leiden University), https://www.ssrn.com/abstract=3175792 [https://perma.cc/2Q64-GXZB].

185. *Id.*

186. *Id.*

187. Louise Matsakis, *How the West Got China's Social Credit System Wrong*, WIRED (July 29, 2019), https://www.wired.com/story/china-social-credit-score-system/ [https://perma.cc/DY2D-AA8Q].

188. Creemers, *supra* note 184, at 13, 22.

systems that are already common in wealthy democracies.[189] Aside from substantial data collection, therefore, the applicability and comparability of the SCS to smart cities are relatively small.

The evidence suggests that rather than finding SCSs to be a dystopian violation of personal privacy as they are invariably conceived of in Western media, they are extremely popular among average Chinese. Evidence from a 2018 cross-regional online survey by Genia Kosta of the Freie Universität Berlin found remarkably high levels of support for social credit systems. While 48.9% of respondents said they strongly approved of the schemes and 31.1% said they somewhat approved, less than 1.5% said they disapproved of such schemes. Older, male, higher-income, more educated, and urban respondents showed higher levels of support.[190] These findings may seem surprising, but supplementary "interviews show that citizens perceive SCSs not as an instrument of surveillance, but as an instrument to improve the quality of life and to close institutional and regulatory gaps, leading to more honest and law-abiding behavior in society."[191]

The difference between public perception of the SCS in China and its depiction in the Western media can largely be explained by the remarkably high levels of trust that Chinese people have in their state. According to Edelman, the world's biggest public relations firm by revenue, the Chinese have the highest level of trust in their government of the 26 countries they surveyed, with a score of 86 out of 100.[192] Other empirical work has long shown high levels of trust and support for the Chinese state.[193] This explanation is borne out by other findings of the survey; 77% of respondents expected the central government to be the most responsible user of personal data. Provincial (48%) and municipal governments (42%) were also seen as relatively trustworthy, and even state-owned companies (27%) were

189. Christopher Curley, *Many Countries Don't Use Credit Scores Like the US — Here's How They Determine Your Worth*, BUS. INSIDER (Aug. 20, 2018), https://www.businessinsider.com/credit-score-around-the-world-2018-8 [https://perma.cc/B72D-NL3Q].

190. Genia Kostka, *China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval*, 21 NEW MEDIA & SOC'Y 1565, 1588 (2019).

191. *Id.*

192. EDELMAN, 2019 EDELMAN TRUST BAROMETER: GLOBAL REPORT 41 (2019), https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Global_Report.pdf [https://perma.cc/8EUB-QBFD].

193. *See generally* Lingnan He & Dali L. Yang, *The Enigma of Political Trust in China*, 15 TAIWAN J. DEMOCRACY 87 (2019).

viewed as far more trustworthy than private companies (8%).[194] The conclusion, yet again, seems to be that, to date, average Chinese are comparatively comfortable with the collection, analysis, and use of data, especially when controlled by the state.

D. Other Applications of Facial Recognition Technology

While the other applications of smart city-related technology explored in this Section are large-scale projects, a few smaller examples of uses of facial recognition technology in China help us understand how far down the path to ubiquity important surveillance technology has traveled. The examples also give color to how unconcerned the state and even private companies are with uses of technology that many citizens of democracies might see as Orwellian.

China has slowly been rolling out new anti-jaywalking systems that use cameras, LED screens, and facial recognition to identify, fine, and shame jaywalkers. At very busy intersections, cameras on traffic lights take pictures of jaywalkers, use facial-recognition software to identify them, and subsequently issue them fines as well as post their pictures and identifying details on screens mounted on the traffic lights.[195] The technology amusingly misfired when it named a well-known Chinese businesswoman, Dong Mingzhu, as a jaywalker after recognizing her photograph from an advertisement on the side of a bus.[196] Furthermore, in a pilot program at a public toilet in Beijing, facial recognition is used to combat toilet paper thieves by dispensing only two feet of toilet paper to any given person within nine minutes.[197]

Chinese have little choice but to consent to systems like the anti-jaywalking traffic lights, though they could attempt to disguise their faces when they cross. Yet, even when given a choice, the average Chinese seem relatively willing to "opt-in" to facial recognition even when the payoff seems vanishingly low. In some Chinese airports, terminals offer the minor convenience of allowing

---

194. Kostka, *supra* note 190, at 1587–88.

195. Liu Zhen, *Shanghai Introduces Facial Recognition to Halt Jaywalkers*, S. CHINA MORNING POST (July 3, 2017), https://www.scmp.com/news/china/society/article/2101061/shanghai-adopts-facial-recognition-system-name-shame-jaywalkers [https://perma.cc/F9MN-DYE8].

196. *Chinese AI Caught Out by Face in Bus Ad*, BBC (Nov. 27, 2018), https://www.bbc.com/news/technology-46357004 [https://perma.cc/5ZDB-CZXR].

197. Javier C. Hernández, *China's High-Tech Tool to Fight Toilet Paper Bandits*, N.Y. TIMES (Mar. 20, 2017), https://www.nytimes.com/2017/03/20/world/asia/china-toilet-paper-theft.html [https://perma.cc/DMC3-42DX].

travelers to check their flight details by presenting their face to a camera equipped with facial recognition software.[198] Some of KFC's 6000 outlets in China[199] have even experimented with facial recognition systems for ordering food, and though the idea does not seem to have taken off, it also did not seem to spark any serious resistance.[200] Facial recognition-based payment systems, however, are quickly gaining popularity. In Henan's capital of Zhengzhou, nearly 200,000 commuters opted to authorize facial recognition-based payments to use the local subway.[201]

There does seem to be a limit, however, on the uses of facial recognition that average Chinese citizens, or at least netizens, will tolerate. For example, in January 2020,

> the urban management department of Suzhou, a city of six million people in Anhui Province, sparked outrage online when it published surveillance photos taken by street cameras of seven residents wearing pajamas in public along with parts of their names, government identification numbers and the locations where their "uncivilized behavior" had taken place.[202]

While the government's battle against public pajamas and other "uncivilized behavior" has been an ongoing issue for over a decade in China, this use of facial recognition quickly attracted national criticism and caused Suzhou officials to apologize.

---

198. Jennings Brown, *Creepy Airport Face Scans Like China's Aren't Just Coming to America — They're Already Here*, GIZMODO (Mar. 25, 2019), https://gizmodo.com/creepy-airport-face-scans-like-chinas-arent-just-coming-1833547407 [https://perma.cc/7TSE-AQ7R].

199. Harrison Jacobs, *KFC Is Most Popular Fast Food Chain in China — Here's What It's Like*, BUS. INSIDER (Mar. 8, 2019), https://www.businessinsider.com/most-popular-fast-food-chain-in-china-kfc-photos-2018-4 [https://perma.cc/2DQU-Q6BH].

200. Amy Hawkins, *KFC China Is Using Facial Recognition Tech to Serve Customers — But Are They Buying It?*, GUARDIAN (Jan. 11, 2017), https://www.theguardian.com/technology/2017/jan/11/china-beijing-first-smart-restaurant-kfc-facial-recognition [https://perma.cc/V2YT-VVW9].

201. Sarah Dai, *China's Subways Embrace Face-Scan Payments Despite Privacy Concerns*, S. CHINA MORNING POST (Dec. 4, 2019), https://www.scmp.com/tech/apps-social/article/3040398/chinas-subways-embrace-facial-recognition-payment-systems-despite [https://perma.cc/ALN4-4SNU].

202. Amy Qin, *Chinese City Uses Facial Recognition to Shame Pajama Wearers*, N.Y. TIMES (Jan. 21, 2020), https://www.nytimes.com/2020/01/21/business/china-pajamas-facial-recognition.html [https://perma.cc/BFV4-JVNW].

E. Lessons from the Chinese Case

While the technologies and applications assessed in these cases are very different, each of them is essentially about the collection and use of data that, at least in theory, can be applied to smart cities. It should be immediately evident that many of these examples fall afoul of Edwards' key security issues.[203] None of the systems explored above, with perhaps the minor exception of the airport facial recognition system, provide any meaningful opportunity for opting out or providing consent. All these systems, but especially City Brain and the IJOP, create privately-held data linked specifically to individuals from "public" interactions that are as simple as walking down the street, making it very different than London's CTV security footage. All the systems seem to involve private contractors who may have access to the data, though admittedly a lack of information and transparency makes this issue difficult to assess fully. Much of the data fed into these systems, especially City Brain, is repurposed from the Internet of Things.[204] Finally, as was vividly demonstrated by Wethington, once collected data is stored on the cloud, little thought is given to its security.

Beyond these clear failures to solve or even engage with privacy challenges, there are common themes that emerge from China's projects, which help inform our comparison with wealthy democracies. First, there is little concern on almost any level about what data is collected, how it is stored, for how long, and who has access to it. Second, while wealthy democracies wring their hands about privacy and other issues,[205] China and its private sector are powering ahead and at a staggering rate. Third, there is little transparency about how any of these projects or technologies are advancing; this is unsurprising given that there seems to be relatively little demand for transparency from political or legal systems or even public opinion. Fourth, the amount of data being collected and used in these projects is staggering. With the vital exception of City Brain, however, there seems to be a lack of the big data analytical techniques and sophisticated algorithms of the kind we might expect and indeed has sometimes been (mis)reported. It is possible that this

---

203. *See supra* Section I.D.

204. *See* WANG, *supra* note 161; Hua et al., *Practice of Large-Scale AI*, *supra* note 115.

205. Hannah Williams, *Why the UK Is Playing Catch up with China in the Smart City Race*, COMPUTERWORLD (Nov. 12, 2019), https://www.computerworld.com/article/3453024/why-the-uk-is-playing-catch-up-with-china-in-the-smart-city-race.html [https://perma.cc/BJ3Z-7WYM].

more sophisticated analysis is coming, perhaps as part of the expansion of City Brain. But it is also possible that given the level of data available and the applicable goals, more sophisticated analysis is simply unnecessary. Google, Facebook, and Amazon may need cutting edge data analytics to help fill in the blanks about user age, gender, religion, marital and family status, and other attributes. Still, the Chinese State will already know any one of these data points as a certainty. Lastly, average Chinese, with the notable exception of targeted minority groups, are generally willing to accept obviously authoritarian uses of the PRC's rapidly increasing data collection. Chinese appear to overwhelmingly support a social credit system that is universally disparaged abroad.[206] They are apparently willing to accept facial recognition even for the minor convenience of paying subway fare or getting their flight information. This may seem surprising in the West, and yet it makes sense given the high level of trust most citizens have in the Chinese state. Given, however, that this trust is largely built on the state's record of overseeing the largest and most dramatic spurt of development in human history (performance legitimacy)[207] and that trust in government usually suffers during a downturn (performance theory),[208] it is likely that trust in the state would suffer from a serious economic downturn. While the details of how and when this might happen are unclear, the possibility concerns the Chinese state and may be one of the reasons for its ramping up of surveillance and other repressive capacities.

Before indulging in dystopian speculation about the depth and power of China's digital authoritarianism, it is important to have some reasonable perspective. On a trip to Shanghai in May 2019, one of this Article's authors could not help but notice that people paid little attention to face recognition-equipped traffic lights. Instead, a much more obvious conflict was going on between Shanghai's police and residents being ticketed for unregistered electric scooters or riding bicycles on the sidewalk. These conflicts could be seen played out all over Shanghai, but always in person and often with long, drawn-out arguments between the public security officers and people

206. *See generally* Kostka, *supra* note 190.

207. *See generally* Hongxing Yang & Dingxin Zhao, *Performance Legitimacy, State Autonomy and China's Economic Miracle*, 24 J. CONTEMP. CHINA 64 (2015). *See also* Yuchao Zhu, *"Performance Legitimacy" and China's Political Adaptation Strategy*, 16 J. CHINESE POL. SCI. 123 (2011).

208. *See generally* Yunsoo Lee, *The Great Recession, Government Performance, and Citizen Trust*, 25 J. INT'L & AREA STUD. 57 (2018).

being fined.[209] What is more, the e-scooter crackdown seems to extend only to a handful of China's largest cities.[210] Within smaller, less-developed cities, these types of violations still generally go almost completely unnoticed. The PRC's dreams of complete surveillance and control are vast,[211] and the progress is rapid, but in many areas, state capacity and the monitoring and control of society still lags what is common in wealthy democracies.[212] In the contemporary PRC, policing society still happens face to face.

III. DEMOCRATIC ALTERNATIVES TO THE CHINA MODEL

In this Article, we argue that China's rapid advancement in smart cities technology should be a wakeup call to democracies. But the fact that it has forged ahead so quickly also means that the China Model offers vivid examples that other democracies can learn from — although in most cases, China provides an example that democracies should avoid, rather than follow. This Part contrasts the Chinese example with the development of smart city technology in wealthy democracies. In particular, we examine the potential role of surveillance intermediaries and consider the role of Europe's data privacy law and potential U.S. parallels. Further, we evaluate if and how wealthy democracies can compete with Chinese smart city technology. Finally, we consider what China's rapid advancement in smart cities and democracies' lagging response means in the rest of the world.

China's smart city technologies offer almost no transparency or consent in terms of the collection, use, or storage of data. Additionally, when asked, private companies will not resist the

---

209. Wu Linhua (邬林桦), *Shanghai Jingfang Zaici Kaizhan Quanshi Jizhong Daji Zhengzhi Xingdong: Chachu Jiaoyu Feijidongche, Xingren Weifa Jin 4 Wan Qi* (上海警方再次开展全市集中打击整治行动：查处教育非机动车, 行人违法近4万起), SHANGHAI OBSERVER (上观) (Apr. 13, 2019), https://www.shobserver.com/news/detail?id=144666 [https://perma.cc/4J42-B64M].

210. Kenneth Tan, *1,000RMB Fines Will Be Issued for Unregistered E-Bikes from May 1*, TIME OUT BEIJING (Apr. 22, 2019), http://www.timeoutbeijing.com/features/Blogs-Beijing_News/170781/1,000RMB-fines-will-be-issued-for-unregistered-e-bikes-from-May-1.html [https://perma.cc/VB7E-2BUC].

211. Adam Greenfield, *China's Dystopian Tech Could Be Contagious*, ATLANTIC (Feb. 14, 2018), https://www.theatlantic.com/technology/archive/2018/02/chinas-dangerous-dream-of-urban-control/553097/ [https://perma.cc/7L4M-2GF8].

212. Hanna Bäck & Axel Hadenius, *Democracy and State Capacity: Exploring a J-Shaped Relationship*, 21 GOVERNANCE 1, 2 (2008).

state.[213] Samantha Hoffman, a visiting academic fellow at the Mercator Institute for China Studies, explained that "Under [China's] Cyber Security Law, the personal data a company collects can be protected from misuse by the company . . . that same data, however, is not protected from the government. This isn't contradictory in Chinese law, even if it is according to Western norms."[214] In short, China can serve as a vivid demonstration of a system in which the state and private companies fail to check one another in the collection and use of data.

Another serious issue in China is the lack of choice between companies that may collect personal information. In no small part, this is due to a close collaboration between the private sector and the state. Private companies like Huawei and Alibaba maintain and value close relationships with the state; other technology companies, including all cellular network providers, are state-owned. Additionally, foreign competitors that might offer a more privacy-friendly alternative are censored or banned from certain sectors.[215]

Democracies advancing smart cities technology should ensure they give their citizens more choice. Many applications of smart cities technology make use of public data in some way. That said, it is difficult for even a relatively educated and wealthy consumer who cares a great deal about data privacy to move away from a jurisdiction with weak privacy protections to one that takes data security more seriously. By contrast, shifting between providers of other types of products involved in collecting and using smart cities data could be much easier. In many cases, consumers can shift between ride-hailing apps, smartphone makers, internet providers, and other service providers in a few minutes and at no cost. One lesson for smart city designers, therefore, could be to ensure that consumers and residents are provided as much choice as possible when using private or third-party products to interact with smart city infrastructure.

A. Surveillance Intermediaries

Because of the high technological bar and investment needed for large scale smart cities projects, it is probable that nearly all will

---

213. Lucas, *supra* note 131; William Yang, *How Much Do Chinese People Care About Privacy?*, DEUTSCHE WELLE (Apr. 12, 2018), https://www.dw.com/en/how-much-do-chinese-people-care-about-privacy/a-43358120 [https://perma.cc/U6BX-M8WD].

214. Yang, *supra* note 213.

215. Leskin, *supra* note 91.

involve private partners. As we have seen in the Chinese case, this can create potential problems and an added layer of complexity when trying to protect privacy. Yet, we argue it could also create opportunities for helping to protect data and privacy better and limit the abuse of smart cities technology.

Tech companies in wealthy democracies could play a vital role in protecting personal data from the state. In part, this could and should be a result of legal restrictions that prevent companies from collecting, keeping, or sharing certain kinds of data. But market incentives can also induce companies to take privacy more seriously. Companies can create significant value for their brands by cultivating a reputation for keeping its customers' data secure. While most consumers are probably more worried about malicious actors, evidence that a company can and will protect data from the state can be important to many, from small-government conservatives in the United States to citizens of developing countries with worrisome records on civil liberties. Imagine if customers in Russia, Kazakhstan, Vietnam, Cuba, Venezuela, or Iran had a choice between Chinese technology they could be relatively sure would allow the state access to their data, and a company based in a democracy with strict data privacy protection, which consumers could be relatively sure would do its best to pushback against state snooping. This possibility is not theoretical: in repeatedly and very publicly refusing to unlock iPhones for the American federal government, Apple has proven both the strength of its encryption and the depth of its commitment to privacy protection. The volume, and more importantly, the nature of the publicity that this incident generated for Apple could not be bought at any price.[216]

Current U.S. law and the policies of big tech firms seriously limit the extent to which technology firms can push back against government requests for data. The third-party doctrine, as applied in *United States v. Miller*[217] and *Smith v. Maryland*,[218] holds that voluntarily providing information to a third party forfeits any privacy interest in that information.[219] The inability of private companies to

---

216. *See generally* Amitai Etzioni, *Apple: Good Business, Poor Citizen?*, 151 J. BUS. ETHICS 1 (2018); Katie Benner, *Barr Asks Apple to Unlock Pensacola Killer's Phones, Setting Up Clash*, N.Y. TIMES (Jan. 13, 2020), https://www.nytimes.com/2020/01/13/us/politics/pensacola-shooting-iphones.html [https://perma.cc/B72D-NL3Q].

217. 425 U.S. 435, 433 (1976).

218. 442 U.S. 735, 749 (1979).

219. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2008).

push back against U.S. law enforcement is evidenced by the remarkable quantity of data major technology companies provide to the government. By 2019, "Facebook said it produced data for 88% of U.S. government requests, and that a majority of them, 47,457, were under the 'legal process' category that includes search warrants, subpoenas and court orders."[220] These requests extend to a large number of technology companies and have been rising dramatically.[221]

Existing jurisprudence also helps point towards possible legal solutions to how to protect personal data better. For example, *United States v. Jones* raised the possibility of a constitutional difference between short- and long-term surveillance.[222] In a concurring opinion, Justice Samuel Alito wrote:

> Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.[223]

Justice Sotomayor's separate concurring opinion picked up on similar themes.[224] Years later, the implications of IoT enabled surveillance and just how far long term and even retroactive surveillance could be taken were addressed in *Carpenter v. United States*. Writing for the majority, Chief Justice Roberts opined:

> With access to CSLI [cell site location information], the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices [sic] of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States — not just those belonging to persons who might happen to come under investigation — this newfound tracking capacity runs against

---

220. Catherine Thorbecke, *Facebook Says Government Requests for User Data Have Reached All-Time High*, ABC NEWS (Nov. 13, 2019), https://abcnews.go.com/Business/facebook-government-requests-user-data-reached-time-high/story?id=66981424 [https://perma.cc/WA8V-NHPX].

221. Eyragon Eidam, *Law Enforcement Agencies' Requests for Facebook Data Continue to Rise*, GOV'T TECH. (May 3, 2017), https://www.govtech.com/social/Law-Enforcement-Agencies-Requests-for-Facebook-Data-Continue-to-Rise.html [https://perma.cc/WA3S-HPF5].

222. 565 U.S. 400, 412 (2012).

223. *Id.* at 430 (Alito, J., concurring) (citing United States v. Knotts, 460 U.S. 276 (1983)).

224. *Id.* at 413–18 (Sotomayor, J., concurring).

> everyone. Unlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when. Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may — in the Government's view — call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.[225]

Companies can and should create more streamlined systems that collect less data, anonymize it, or delete it more quickly. Currently, American mobile providers store customers' location data collected for between one year (Verizon) and seven years (AT&T).[226] There seems little justification for keeping this data, especially un-anonymized, other than selling it to third parties, which has come under congressional and popular scrutiny.[227] Strong legal restrictions on both selling data and keeping it for extended periods would help companies resist state demands for data. Companies cannot be made to produce data they never collected, no longer have, or cannot link to specific individuals.

Building on the logic established in *Jones* and *Carpenter*, the United States could structure its data privacy around a short- versus long-term distinction. Personal data could be used to optimize traffic, emergency response routes, public transit, and a wide variety of other city services, but could be legally required to be deleted within hours or even minutes.

If the United States is to become an exemplar of data privacy to be emulated and to disperse high standards along with its smart cities technology globally, it will need newer, smarter, and tougher laws. In this regard, the European Union is already far ahead of the United States. In the next Section, we examine a case that shows how Europe's General Data Protection Regulation (GDPR) can and has empowered surveillance intermediaries to push back against the local state. We will also show how California's new privacy law is bringing the United States into line with these same standards.

---

225. Carpenter v. United States, 138 S.Ct. 2206, 2218 (2018).

226. Scar de Courcier, *Cellular Provider Record Retention Periods*, FORENSIC FOCUS (Apr. 18, 2017), https://articles.forensicfocus.com/2017/04/18/cellular-provider-record-retention-periods/ [https://perma.cc/HS2V-ENSW].

227. Alfred Ng, *Senators Call for Investigation of Phone Companies Selling Location Data*, CNET (Jan. 10, 2019), https://www.cnet.com/news/senators-call-for-investigation-on-phone-companies-selling-location-data/ [https://perma.cc/9BWD-DQB8].

B. Europe

Thanks to the GDPR, the European Union, composed of nearly 30 sovereign nations, can be seen as having a more comprehensive, coherent, and consistent privacy policy than the United States.[228] There are several reasons for this. In part, it is the result of the strong federal nature of the United States, which has also hurt advancements in other areas of innovation that generally benefit from strong government support. For example, policy fragmentation and lack of clear national leadership were two of the reasons that the United States was surpassed by the PRC and the European Union in the development of renewable energy, where a "patchwork of state-level approaches creates complexity, instills uncertainty, and inhibits opportunities to optimize resource allocation."[229]

Yet the U.S. federal structure also offers opportunities for specific jurisdictions, especially populous ones, to lead the way by setting higher standards than the federal government or other states. Sometimes this is merely states fulfilling their roles as "laboratories of democracy."[230] When a state or city sets a higher minimum wage, it provides an example that other states or the federal government may or may not choose to emulate.[231] But when a particularly populous state sets strict standards that certain products must meet, companies often choose to meet this higher standard with products offered throughout the United States or even the world. For example, California's emissions and fuel standards for automobiles are "benchmarks set in the Golden State [that] ripple through the rest of the country and can even shape the global market."[232] For this

---

228. Tony Romm et al., *Europe, Not the U.S., Is Now the Most Powerful Regulator of Silicon Valley*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/business/technology/europe-not-the-us-is-now-the-most-powerful-regulator-of-silicon-valley/2018/05/25/f7dfb600-604f-11e8-8c93-8cf33c21da8d_story.html [https://perma.cc/BFV2-D454].

229. Kelly Sims Gallagher, *Why & How Governments Support Renewable Energy*, 142 DAEDALUS 59, 73 (2013).

230. G. Alan Tarr, *Laboratories of Democracy? Brandeis, Federalism, and Scientific Management*, 31 PUBLIUS 37, 40–41 (2001).

231. *See* Andrew Branch, *Wages of Federalism,* WORLD MAG. (Feb. 21, 2014), https://world.wng.org/2014/02/wages_of_federalism [https://perma.cc/X4KL-X6GW]; Matthew Zeitlin, *Seattle's Minimum Wage Was the Highest in the Nation. Here's What Happened.*, VOX (July 22, 2019), https://www.vox.com/the-highlight/2019/7/13/20690266/seattle-minimum-wage-15-dollars [https://perma.cc/Z9G5-JW32].

232. Umair Irfan, *Trump's Fight with California over Vehicle Emissions Rules Has Divided Automakers*, VOX (Nov. 5, 2019),

reason, the best hope for near-term improvements in privacy regulations in the United States comes in the form of the California Consumer Privacy Act (CCPA), the strictest privacy law in the United States, which came into effect in January 2020.[233] The CCPA will have a nation-wide, and to a lesser extent, global impact not only because of California's large population and lucrative markets but because over half of the United States' and over a quarter of the world's 20 largest tech companies are headquartered in California.[234]

The CCPA will set the de facto national standard for privacy for the foreseeable future. It will, therefore, begin to bring the United States into line with the privacy principles enshrined in Europe's GDPR. More specifically, those principals are lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality (security); and accountability.[235] Taken together as the standard for Europe and the de facto standard for the United States, the GDPR and CCPA could give companies in wealthy democracies a relatively clear global standard. When combined, the United States and the European Union represent a market of around 800 million people and a GDP that is still far larger than the PRC's. This could give companies developing smart cities technologies in wealthy democracies a market big enough for them to compete with Chinese companies. Additionally, Chinese companies will need to meet these same standards, at least in the United States and European Union, lest they forgo many of the world's largest markets. In order to capitalize on these opportunities, efforts should be taken to harmonize the privacy regimes among democracies as much as possible.

While the impact of the CCPA is still uncertain, the GDPR, which has applied since May 25, 2018, has already had a substantial impact.[236] The idea that private service providers might push back against government overreach with smart cities data might initially seem optimistic, yet this is exactly what the GDPR has helped some surveillance intermediaries to do. Brøndby IF, a football club based in the outskirts of Copenhagen, uses facial recognition software to prevent known troublemakers from attending matches in the team's

---

https://www.vox.com/policy-and-politics/2019/11/5/20942457/california-trump-fuel-economy-auto-industry [https://perma.cc/N6ME-8YEF].

233. ERIC GOLDMAN, INTERNET LAW CASES & MATERIALS 357–64 (2019).

234. *Global 500*, FORTUNE, https://fortune.com/global500/2018/ [https://perma.cc/QB7Y-PH9T] (last visited Jan 17, 2020).

235. Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).

236. Burgelman, *supra* note 76.

stadium.[237] Brøndby's system marks one of the first private large-scale uses of facial recognition software after the GDPR came into effect.[238] In compliance with the GDPR, the facial recognition system is used to enter those from the watchlist into the system only on game day and is deleted at the end of the day. The system is kept separate from the internet, and a cross-check is used to avoid false positives.[239]

The value of strict data privacy laws being passed and enforced on private systems and the contrast with the Chinese case examined above should be clear. Less clear is the extent to which such laws could and should enable private companies to push back against possible overreach from other parts of the state. Mickel Lauritsen, Brøndby's security chief, says that local police have asked him to use the team's facial recognition system to assist in an investigation, but that he was obligated to refuse by the terms of their regulatory permission.[240] There are signs that these clear rules, when strictly enforced, facilitate public trust. In the words of one football fan, "You can't do anything in Denmark without getting the proper approval. So it's not being misused, I don't think. You can't do that in Denmark."[241]

An arrangement like the strict European approach to privacy, however, may be difficult or impossible to replicate in the United States. For one thing, it is relatively easy for Europe to be strict or even punitive against technology companies in both legislation and enforcement because none of the world's largest tech companies are based in Europe. Yet the CCPA should provide some hope here as well: if California can move to reign in its large tech firms like Apple, Alphabet, and Facebook, perhaps the rest of the country will be willing to follow. Nevertheless, even if the legislation and tough enforcement prove forthcoming, it is not clear that public opinion will follow. China and most governments in Europe, especially Northern Europe, have long enjoyed higher levels of trust among their people.[242] This is unlikely to be easy or fast to reproduce in the U.S.

---

237. Sidsel Overgaard, *A Soccer Team in Denmark Is Using Facial Recognition to Stop Unruly Fans*, NAT'L PUB. RADIO (Oct. 21, 2019), https://www.npr.org/2019/10/21/770280447/a-soccer-team-in-denmark-is-using-facial-recognition-to-stop-unruly-fans [https://perma.cc/MUV9-XN8H].

238. *Id.*

239. *Id.*

240. *Id.*

241. *Id.*

242. *See* EDELMAN, *supra* note 192, at 41.

context and is another reason that more market-based solutions to data privacy issues might be a more practical choice in the United States.

C. Can Democracies Compete with the PRC's Smart City Technology?

In this Article, we argue that wealthy democracies must push forward with the development of smart cities for two reasons. First, smart cities can provide meaningful benefits not only to the residents of wealthy democracies, such as in improving traffic but also to the world, like combatting climate change. Second, if wealthy democracies and their corporations do not offer the world smart cities technologies that allow for some measure of privacy, democracy, and personal freedom, then non-democratic countries and their corporations will offer them smart cities technologies that do less to address these concerns.

The idea that China could beat out wealthy democracies in smart cities technology has a strong precedent. The most relevant example is the current state of and debates about 5G technology and its deployment around the globe.[243] Beginning wide-scale deployment in 2019, 5G is a fifth-generation wireless technology that offers much faster data on digital cellular networks. Huawei, a Chinese company with close links to the Chinese state, is the world leader in 5G technology. The United States has repeatedly voiced security concerns about Huawei's close relationship to the Chinese state and that using their technology could give Beijing unprecedented access to, and even control over, other countries' communication technology. In the words of a report published by the NATO Cooperative Cyber Defence Centre of Excellence:

> Chinese companies are not only subsidised by the Chinese government but also legally compelled to work with its intelligence services. Whether the risk of such collaboration is real or perceived, the fear remains that adopting 5G technology from Huawei would introduce a reliance on equipment which can be controlled by the Chinese intelligence services and the military in both peacetime and crisis.[244]

There are alternatives to Huawei's technology available from companies, such as Nokia, Ericsson, and Samsung, that are based in

---

243. KADRI KASKA ET AL., HUAWEI, 5G AND CHINA AS A SECURITY THREAT 4 (2019).

244. *Id.*

liberal democracies.[245] Yet, Huawei advertises its technology as not only cheaper to purchase, but lighter, easier, faster, and cheaper to install, cheaper to maintain, and more energy-efficient.[246] Because of these advantages and despite the warnings from the United States and NATO, some of the wealthiest nations in the world, including Switzerland and Saudi Arabia, are opting for Huawei's technology.[247] The calculus for poorer developing nations is likely to be even simpler and inevitable.[248] A massive and rapid change will need to occur if Huawei is not to dominate the world's cellular networks in the near future.

In no small part, Huawei's success in 5G technology is the result of strong support from the Chinese state.

> A Wall Street Journal review of Huawei's grants, credit facilities, tax breaks and other forms of financial assistance details for the first time how Huawei had access to as much as $75 billion in state support as it grew from a little-known vendor of phone switches to the world's largest telecom-equipment company — helping Huawei offer generous financing terms and undercut rivals' prices by some 30%, analysts and customers say.[249]

As security concerns related to the rollout of Huawei-powered 5G networks grow, the United States is finally reacting. In January 2020, a bipartisan group of U.S. senators introduced legislation that would provide over $1 billion for the development of 5G alternatives to Huawei.[250] Yet, with funding a fraction the size of what Huawei received, and 5G technology already being implemented, the initiative seems like far too little, far too late. Just as 5G technology gives insight into potential Chinese dominance of smart cities, it

---

245. Fiona Leake, *The U.S. Must Provide Alternatives to Huawei 5G Tech in 2020*, 5GRADAR (Dec. 23, 2019), https://www.5gradar.com/news/the-us-must-provide-alternatives-to-huawei-5g-tech-in-2020 [https://perma.cc/AF6C-SN4S].

246. Steve McCaskill, *Huawei: We Make It Cheaper and Simpler to Deploy 5G*, TECHRADAR (Feb. 22, 2019), https://www.techradar.com/au/news/huawei-we-make-it-cheaper-and-simpler-to-deploy-5g [https://perma.cc/GM6H-XUN7].

247. Elise Thomas, *Huawei and 5G: What Are the Alternatives?*, STRATEGIST (Mar. 8, 2019), https://www.aspistrategist.org.au/huawei-and-5g-what-are-the-alternatives/ [https://perma.cc/R3SZ-2KMQ].

248. *Id.*

249. Chuin-Wei Yap, *State Support Helped Fuel Huawei's Global Rise*, WALL ST. J. (Dec. 25, 2019), https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736 [https://perma.cc/2ZYE-VZW7].

250. Lauren Feiner, *Senators Propose Pumping Over $1 Billion into 5G Alternatives to China's Huawei*, CNBC (Jan. 14, 2020), https://www.cnbc.com/2020/01/14/senators-propose-over-1-billion-for-5g-alternatives-to-chinas-huawei.html [https://perma.cc/LQV7-DQ6U].

echoes China's success in previous races for technology, especially renewable energy.[251]

What makes these examples truly worrying from the perspective of smart cities is that China beat wealthy democracies in the development of technologies such as 5G and solar panels, even though these technologies are not subject to nearly the same level of concern, complexity, and negative public onion as many smart cities technologies.

D. Battlegrounds for the Meaning of Smart Cities?

City Brain is already being implemented in Malaysia's most populous metropolis.[252] This points to Southeast Asia as the probable location of the first battleground in the contest of smart city technology between the PRC and democracies. Geographically, the countries of Southeast Asia are relatively close to China. Most have large ethnic Chinese communities that have traditionally worked in business and may maintain business ties to China.[253] Southeast Asian countries also have relatively similar levels of development to China,[254] and relatively positive attitudes towards the PRC, at least compared to other Asian countries like India, Japan, and South Korea.[255] They also have generally more authoritarian and less democratic tendencies.[256] These last two factors could be important for minimizing public opinion pushback against projects that could give not only their countries' leaders but Chinese companies and even the Chinese state, the key to ubiquitous surveillance of their cities.

---

251. *See supra* Part II.

252. Soo, *supra* note 148.

253. Alle Neuigkeiten von Schlegel und Partner, *Southeast Asia: The True Extent of Chinese Influence*, SCHLEGEL UND PARTNER (May 11, 2015), https://www.schlegelundpartner.com/cn/news/suedost-asien-china/u/1126/ [https://perma.cc/4PKU-7F6M].

254. *Report for Selected Countries and Subjects*, INT'L MONETARY FUND (Oct. 2018), https://www.imf.org/external/pubs/ft/weo/2018/02/weodata/weorept.aspx?pr.x=82&pr.y=6&sy=2017&ey=2018&ssd=1&sort=country&ds=.&br=1&c=512 [https://perma.cc/74AU-9NBL].

255. Kat Devlin, *5 Charts on Global Views of China*, PEW RES. CTR. (Oct. 19, 2018), https://www.pewresearch.org/fact-tank/2018/10/19/5-charts-on-global-views-of-china/ [https://perma.cc/59B6-3MWX].

256. MONTY G. MARSHALL & KEITH JAGGERS, UNIV. OF MD., POLITY IV PROJECT, (2013); LEE MORGENBESSER, THE RISE OF SOPHISTICATED AUTHORITARIANISM IN SOUTHEAST ASIA (2020); *The Rise of Sophisticated Authoritarianism in South East Asia*, GRIFFITH ASIA INST. (Sept. 23, 2019), https://blogs.griffith.edu.au/asiainsights/the-rise-of-sophisticated-authoritarianism-in-south-east-asia/ [https://perma.cc/SBS9-KNPE].

Southeast Asia is not unique, however, in their increasingly overflowing and traffic-clogged cities, which are badly in need of improved infrastructure and services.[257] Even if Chinese tech companies do not find Southeast Asia to be fertile ground for their smart cities technology, as Alibaba seems to hope, other regions like the Middle East and North Africa, Central Asia, Sub-Saharan Africa, and even Latin America all offer likely opportunities because they suffer from many of the same problems arising from rapid urbanization.[258]

None of this is to suggest, however, that people, companies, or governments in developing countries outside China lack agency. A country like India with a huge population and an already impressive technology sector could still emerge as to equal or even outmatch the smart city technology developed in China and wealthy democracies.

IV. RECOMMENDATIONS AND THE WAY FORWARD

While we recognize that smart city efforts like Quayside face serious and unanswered questions about data and digital infrastructure, we argue three major reasons why democracies must continue to develop smart cities technology with all deliberate speed. First, many of the questions about data privacy and digital infrastructure can only be answered through real working examples of smart cities technology. Some projects may fail to produce results. Others may end up being viewed as not responsive enough to terms and concerns related to data protection. Yet, if there is any lesson to be drawn from the experiences of the digital revolution, it is that both experiences of failure and the creation of successful models are necessary for smart cities to continue to advance. Smart cities developers may have to "move fast and break things" (Facebook's motto until 2014),[259] especially if they are to catch up with their Chinese competitors.

---

257. Gharad Bryan et al., *Cities in the Developing World* (Nat'l Bureau of Econ. Res., Working Paper No. 26390, 2019).

258. *See generally* WORLD BANK & INT'L MONETARY FUND, GLOBAL MONITORING REPORT 2013: RURAL-URBAN DYNAMICS AND THE MILLENNIUM DEVELOPMENT GOALS (2013), http://documents.worldbank.org/curated/en/720451468171242999/pdf/759570BR0SECM20Official0Use0Only090.pdf [https://perma.cc/Q5SE-QTHV].

259. The Quantified VC, *Move Fast and Break Things Is Not Dead*, MEDIUM (Sept. 15, 2018), https://medium.com/swlh/move-fast-and-break-things-is-not-dead-8260b0718d90 [https://perma.cc/BL5E-QRCZ].

Second, smart cities projects have the potential to be important parts of the solution to pressing global issues such as climate change and inequality. Many of the technologies with the most potential to address these problems are the least objectionable. Smart cities should not be only about the shiniest technology and fastest processors. Instead, they should take data seriously and focus on those technologies that offer the most advantage the most efficiently — even if that is something as simple as wood construction.

Third, if democracies do not develop and regulate their own smart cities technology, the spread of PRC-based technology will go largely unchallenged. Democracies should not let the great be the enemy of the good. Some compromises and sacrifices of data privacy may be necessary to strike a balance and move smart cities technologies forward before China gains an advantage in smart cities that is insurmountable. Temporary concessions to Google over a project like Quayside could be rolled back relatively easily by democratic governments. Cities-worth of cameras feeding into Alibaba's servers will, conversely, be far harder to undo.

Finally, we offer two major recommendations that we believe could help in the development of smart cities in the democratic world. First, massive government investment in smart cities to help counter the tremendous sums that the PRC has already poured into their smart cities' efforts. This must be done before it is too late, as demonstrated by the example of 5G or solar technology. Second, clear and transparent laws protecting users and residents must be implemented and enforced. Violations need to be announced and punished transparently and publicly. These laws also need to empower private companies to refuse government requests for data. The laws should be harmonized within countries and even across as many democracies as possible. Only this will provide a more or less unified market that is bigger than China's market.

In reality, it may be too late for some technologies and projects to catch up with City Brain in the near term. Every wasted opportunity, however, moves farther away from the prospect of cities that are not only smart but also transparent and respectful of individuals' data.

CONCLUSION

This Article generally assumes that smart cities technology is coming, whether academics, governments, lawyers, judges, or citizens like it or not. Even if companies in wealthy democracies do not develop or implement certain types of technology for legal, political, commercial, or ethical reasons, companies in other countries, like the

PRC, will happily sell and implement their smart city technologies. Indeed, Section II.A discussed how this is already happening.

This Article considers how contrasting approaches to smart cities has and will impact smart city development, and how the technologies will be adopted outside of the PRC and wealthy democracies. It is imperative for established democracies, and the companies based in them, to continue to move forward with smart cities technology development and implementation. Further, they should use smart city technology with the most rigorous standards of transparency and oversight possible. Because smart city technology will continue to spread, particularly to the developing world where the will and ability to guard against its abuse is lower, wealthy democracies must push forward with the development of smart cities, both to create technology with better built-in safeguards and to develop and normalize rolling best practices for data privacy.