SMART CITIES AND DEMOCRATIC VULNERABILITIES

// **BETH KERLEY,** PROGRAM OFFICER, INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES, NATIONAL ENDOWMENT FOR DEMOCRACY

INTRODUCTION

From the most established democracies to the "digital totalitarian" setting of the People's Republic of China (PRC), **"smart city" projects are transforming municipal governance**. Definitions of this broad term for municipal-level digitalization vary widely, sometimes encompassing relatively simple projects such as launching digital portals for public agencies or offering free public Wi-Fi.

Many smart city initiatives, however, **leverage the capacity of the Internet of Things (IoT) and artificial intelligence (AI)–powered analytics tools to monitor trends in urban life, identify challenges, and inform or even automate the provision of services**—from heating and waste management to public safety. Such initiatives promise increased efficiency and could even provide new opportunities for public engagement in municipal governance. Yet current approaches to these projects may be sidelining democratic deliberation and fueling authoritarian practices instead.[1]

Most current smart city projects promise in some way to streamline urban governance through the ongoing **collection and analysis of large volumes of data**. In an experimental "Smart Village" in South Korea, residents are sharing data collected by smart watches and smart home devices in exchange for rent-free living.[2] Saudi Arabia has been touting its plans for a vertically stacked city called "The Line" that will draw on "residents' smartphones, their homes, facial recognition cameras, and a host of other sensors" to "feed information back to the city and help it predict user needs."[3] In the PRC—which as of January 2020 is already home to more than eight-hundred smart city projects—the U.S.-China Economic and Security Review Commission has observed, "[It] is clear . . . that the CCP [Chinese Communist Party] intends to use multiple smart city technologies to substantially augment and even revolutionize its mass surveillance capabilities."[4] In more democratic settings, the surveillance potential of smart cities can lead to pushback: a planned Sidewalk Labs initiative in Toronto featuring heated streets and computer vision-enabled cameras was cancelled in 2020 amid both economic woes and a lawsuit over "data surveillance."[5]

DEFINING THE CHALLENGE

Smart cities are a sometimes underappreciated part of a broader narrative in which digital tools once expected to put political participation within easy reach are also proving to be powerful instruments of manipulation and control. They underscore that this trajectory involves not only the sphere of online discourse but also governance processes and the physical world.

Digital tools once expected to put political participation within easy reach are also proving to be powerful instruments of manipulation and control.

The democracy risks around smart cities span multiple fronts and include the *authoritarian actors* frequently involved in their design and operation; the *opaque and irregular processes* by which they come into being; and the *data-collection capacities* they create. Both individually and in combination, these risks threaten to erode rule-of-law norms. They also produce privacy hazards with the potential to fuel discrimination, enable political manipulation, and chill civic participation. On all these fronts, risks can be exacerbated by pre-existing illiberal trends or weaknesses in oversight institutions.

Although the PRC's development and export of "smart city" tools together with the Sidewalk Labs case may have received the greatest share of attention, smart cities are a global phenomenon. In particular, these projects are a major presence in what Steven Feldstein described in a recent report for the International Forum for Democratic Studies as **"swing states"**: "partly open political settings where key liberal-democratic guardrails are weakened or absent in ways that could heighten the appeal of authoritarian digital models."[6] These and other political settings marked by democratic backsliding are fertile grounds for the development of the authoritarian potential inherent in technologies that involve an unprecedented monitoring of daily life.

Autocratic actors

With regard to *actors*, the PRC's leading role in smart city exports has alarmed democracy advocates. **China has made smart cities-related technologies (including cloud computing, big data, and IoT) a top-level priority** and exported such tools to more than a hundred countries.[7] At home, these projects

A Huawei CCTV camera installed in Suvarnabhumi Airport in Bangkok, Thailand.

fit within a wider web of technical and institutional practices for **integrating information from different sources in the service of social control**.[8] As Samantha Hoffman relates, smart city projects can fuse "the everyday provision of basic publics goods" with "the projection of authoritarian power." She explains, "[F]or instance, a smart electricity meter can improve the accuracy, transparency, and reliability of readings, to the benefit of the utility and its customers. For police, the data from that same meter can help to detect 'abnormal' behaviors indicative of 'illegal' gatherings."[9]

Thus, one major question around PRC-sponsored smart city projects concerns whether, when other governments purchase these technologies from vendors such as Huawei, the digital authoritarian model will come along for the ride. On this front, it is noteworthy that **Huawei "Safe Cities"—a security-focused spinoff of the smart cities concept** that features surveillance systems such as "command centers, CCTV cameras, intelligent video surveillance, facial and license plate recognition technology, crowd monitoring, situational awareness detection, noise monitoring or detection, abandoned object detection, and social media monitoring"—are spreading globally, particularly in countries classified as "Not Free" or "Partly Free" by Freedom House.[10]

Even if the PRC's surveillance systems end up working somewhat differently outside the highly specific social and institutional authoritarian frameworks in which they are embedded at home,[11] they may still end up strengthening autocrats or undermining democratic governance in a range of other ways.

Authorities in Beijing may gain access to sensitive host country data through **surreptitious "backdoors,"** as recently observed in a law enforcement database in Pakistan.[12] Even "legitimately" collected data could **help PRC state entities to hone their propaganda** and other tools for manipulating foreign societies, as Samantha Hoffman has persuasively argued.[13] Security-centric smart city projects together with PRC know-how could encourage governments in closed or semi-closed settings to **intensify their monitoring of political opponents**; Huawei technicians were found to have assisted with such activity in Uganda and Zambia.[14] Finally, growing dependence on PRC digital infrastructure could in turn provide Beijing with new and dangerous **leverage over the politics of importing countries**.[15]

Good governance hazards

At the same time, it bears noting that some *procedural concerns* are common to both PRC smart city projects and those involving vendors based in democracies. In the essays that follow, Roukaya Kasenally—scrutinizing a Huawei Safe City project in Mauritius—and Bárbara Simão and Blenda Santos—examining the multi-vendor smart city landscape in Brazil—similarly stress the challenge of opacity. Authorities are frequently disinclined to disclose information about the contracts through which they procure smart city technologies. This reluctance is particularly worrisome when those contracts involve high-level deals with PRC vendors that **circumvent standard public procurement procedures**, as we observe in cases from Mauritius to Serbia.[16] But the problem is not exclusive to these cases.

> Authorities are frequently disinclined to disclose information about the contracts through which they procure smart city technologies.

Opacity can also be linked to a **failure to solicit community input** or conduct appropriate human rights impact assessments for smart city projects, as Simão and Santos document. If officials commissioning these projects do not prioritize input from below, the package deals offered by private vendors can instead end up setting public agendas. In such circumstances, these projects can amount, in Bianca Wylie's words, to "the outsourcing of public governance to a for-profit actor."[17]

The specter of mass surveillance

These procedural shortcomings are particularly concerning because smart city projects create new *capacities*, especially in the surveillance domain, that could **amplify unaccountable government and corporate power** at the expense of public engagement. Many smart city projects include controversial facial recognition tools overtly designed for surveillance, nominally to fight crime. Yet as Simão and Santos note, smart city initiatives in fields such as education or connectivity also tend to involve the **collection, or provision to vendors, of large volumes of personal data**.

Where frameworks to guide the handling of this data are absent or inadequate, there is little guarantee that it will not be leveraged in ways that are discriminatory or enable political manipulation. As Kasenally observes in Mauritius, even when data protection frameworks are formally in place, national-security clauses may give executive branch officials considerable unilateral discretion over data handling. In backsliding democracies where those same officials have a record of engaging in practices that violate civil liberties or trample on checks and balances, this situation is cause for concern.

Moreover, data collection in smart cities presents something more serious than simply the series of independent, project-level risks associated with each new smart streetlight or energy meter. In the PRC, we can already observe how **digital platforms for "data fusion"** enable the integration of different data streams—drawn from both digital spaces such as WeChat accounts and physical ones such as streets monitored by facial-recognition cameras—to monitor individuals and predict social trends.[18] Such practices are used to their most devastating effect in the Integrated Joint Operations Platform that flags potentially "dangerous" individuals to police in Xinjiang.[19]

Across all three fronts, **underlying weaknesses in democratic institutions aggravate the risks of smart city projects**. Where checks and balances are weak and decisions are made behind closed doors by a small circle of elites, officials may be likelier to underestimate—or simply discount—the dangers of entanglement with vendors based in autocracies. They may also have fewer incentives to assess the human rights impacts of projects at the design stage or implement appropriate data protection safeguards. Feldstein's research on digital repression has shown "a strong relationship between curtailments of political liberties and subsequent government abuse of surveillance technologies." This tendency could produce a vicious feedback loop linking smart city risks to democratic backsliding.[20]

Underlying weaknesses in democratic institutions aggravate the risks of smart city projects.

DIGITALIZATION AT A CROSSROADS

The PRC's dystopian practices underscore that smart cities are one of the many arenas in which **democratic societies are colliding with a digitally powered vision that threatens to corrode their basic normative fabric**. That vision involves not only bolstering state capacities for surveillance and control, but also cutting out the messy (albeit necessary) feedback mechanisms of open societies.

As digital systems with authoritarian affordances come to be more widely available, this model is becoming a dangerous temptation for democracies and "swing states" as well. Although appearing in the guise of hyper-efficient "solutions" to optimize good governance for a modern state, digital projects that follow this vision can also be a means for illiberal actors to install **new levers of social manipulation** at the public's expense. Ultimately, they may intensify such potent challenges to democracy as popular alienation from governance systems and the erosion of institutional accountability.

Writing in *Foreign Affairs*, Henry Farrell, Abraham Newman, and Jeremy Wallace argued that authoritarians will **see AI tools as an alternative to popular political participation**—a system that can tip authorities off to potential problems and "tell rulers whether their subjects like what they are doing without the hassle of surveys or the political risks of open debates and elections."[21] PRC smart city projects that use a web of sensors and "city brains" to handle local governance challenges fit neatly within this rubric. Down to the most local level, authorities "use data integration platforms to decide whether local challenges are best resolved via service provision or via more coercive forms of demobilization."[22]

But the aspiration for automated tools that can obviate the need for democratic feedback is by no means limited to autocratic settings. It is, rather, the logical endpoint of a technocratic impulse present in all too many democratic polities. In *The Smart Enough City*, Ben Green has described how smart city projects can reflect and encourage a prioritization of technical means over social ends. In other words, municipal authorities presume that their main responsibility is identifying the best technological tool for achieving what they presume to be an uncontroversial goal—often described in terms of "efficiency"—rather than engaging the pluralistic societies they govern to achieve a better understanding of what their goals should be. In such instances, **putative technological fixes can serve as a distraction from addressing underlying social issues**.[23] As our colleagues at the National Democratic Institute have argued, "Obsession with innovative technologies can overshadow better, less technical solutions."[24]

In today's unstable, ever-shifting social and economic landscape, governments may take comfort in a digital vision that elides unpredictable, fraught, and contentious processes of popular consultation. The preceding reflections and the essays that follow nonetheless underscore the **crucial importance of both formal and informal democratic institutions** to sound decision making about smart cities. They are vital not only to protecting civil liberties, but also to ensuring basic good governance. Farrell, Newman, and Wallace argue that authoritarians' aspiration to make data a substitute for dialogue is likely to backfire:

> *Although ubiquitous state surveillance could prove effective in the short term, the danger is that authoritarian states will be undermined by the forms of self-reinforcing bias that machine learning facilitates. As a state employs machine learning widely, the leader's ideology will shape how machine learning is used, the objectives around which it is optimized, and how it interprets results. The data that emerge through this process will likely reflect the leader's prejudices right back at him. . . . Instead of good policy, this will lead to increasing pathologies, social dysfunction, resentment, and, eventually, unrest and instability.*[25]

In this context, repressive digital systems aimed at maintaining "social stability" while denying the public a voice may instead end up exacerbating the governance challenges facing societies worldwide, as citizens grow increasingly alienated from distant, opaque, and unresponsive institutions.

Repressive digital systems aimed at maintaining "social stability" may instead exacerbate the governance challenges facing societies worldwide.

LOOKING FORWARD

Because the complex issues surrounding personal data collection and relationships with smart city vendors are challenging for even the most established democracies to manage, identifying promising, participatory models in this space is perhaps more difficult than naming the risks. It is, however, worth noting that inspiration on this front may come from the ranks of younger democracies and other "swing states." Simão and Santos note that **Brazil**, for all its recent political struggles, has issued **national-level policies that propose important democratic norms for municipal digitalization**, including a Charter for Smart Cities that was itself developed through wide consultation with civil society. These guidelines address issues such as respect for rights, stakeholder engagement, and mindfulness of how new digital projects intersect with socioeconomic inequalities. Building on joint research from Internet Lab, Article 19, and LAPIN, Simão and Santos also propose that cities consider alternate pathways for smart city development, such as **collaborations with social collectives or universities** rather than traditional vendors.

Digital advances are further facilitating technocratic visions of absolute control. In this context, understanding the limits of data-driven technologies and opening up space for input from civil society, accountability institutions, and the broader public is crucial to guarding against both human rights risks and cross-border authoritarian influence. At the same time, **embedding digitalization within the robust give-and-take of democratic politics** may be the only path toward re-establishing an even more fundamental form of control: the power to ensure that digital data and the imperfect maps it creates serve the interests of the human societies they depict, rather than holding these societies hostage.

Drones being used to get surveillance inside a Polling booth in New Delhi, India.

ENDNOTES

Smart Cities and Democratic Vulnerabilities

1 Marcus Michaelsen and Marlies Glasius, "Authoritarian Practices in the Digital Age," *International Journal of Communication* 12, (2018), 3788-3794.

2 David Belcher, "A New City, Built upon Data, Takes Shape in South Korea," *New York Times,* 28 March 2022, www.nytimes.com/2022/03/28/technology/eco-delta-smart-village-busan-south-korea.html.

3 Menna A. Farouk, "Saudi 'surveillance city': Would you sell your data to The Line?," Reuters, 23 August 2022, www.reuters.com/article/saudi-city-surveillance-idAFL8N2ZL0CM. This project, however, has been slow to materialize in practice—for more information, please see: Nicolas Pelham, "MBS: Despot in the Desert," *the Economist*, 28 July 2022, www.economist.com/1843/2022/07/28/mbs-despot-in-the-desert.

4 Katherine Atha et al., "China's Smart Cities Development," U.S.-China Economic and Security Review Commission, January 2020, www.uscc.gov/sites/default/files/China_Smart_Cities_Development.pdf.

5 For more information, please consult: Sidney Fussell, "The City of the Future Is a Data-Collection Machine," *the Atlantic*, 21 November 2018, www.theatlantic.com/technology/archive/2018/11/google-sidewalk-labs/575551/; Alissa Walker, "Sidewalk Labs' 'smart' city was destined to fail," Curbed, 7 May 2020, https://archive.curbed.com/2020/5/7/21250678/sidewalk-labs-toronto-smart-city-fail; and Moira Warburton, "Alphabet's Sidewalk Labs cancels Toronto 'smart city' project," Reuters, 7 May 2020, www.reuters.com/article/us-canada-sidewalk/alphabets-sidewalk-labs-cancels-toronto-smart-city-project-idUSKBN22J2FN.

6 Steven Feldstein et al., *The Global Struggle over AI Surveillance: Emerging Trends and Democratic Responses*, National Endowment for Democracy, June 2022, www.ned.org/wp-content/uploads/2022/06/Global-Struggle-Over-AI-Surveillance-Emerging-Trends-Democratic-Responses.pdf.

7 Katherine Atha et al., "China's Smart Cities Development."

8 Huirong Chen and Sheena Chestnut Greitens, "Information capacity and social order: The local politics of information integration in China," *Governance,* (2021), 1-27, www.sheenagreitens.com/uploads/1/2/1/1/121115641/chen___greitens_-_info_capacity___social_order__governance_2021_.pdf.

9 Samantha Hoffman, "China's Tech-Enhanced Authoritarianism," *Journal of Democracy* 33, 2 (2022), 76-89, https://muse.jhu.edu/article/852746.

10 Jonathan E. Hillman and Maesea McCalpin, *Watching Huawei's "Safe Cities,"* Center for Strategic and International Studies, 4 November 2019, www.csis.org/analysis/watching-huaweis-safe-cities; and for details on the spread of PRC Safe City projects, please see: https://chinatechmap.aspi.org.au/#/map/f5-Smart%20City-Public%20Security%20project,f6-Smart%20cities.

11 Chen and Greitens, "Information capacity and social order."

12 Dan Strumpf and Waqar Gillani, "Huawei Accused in Suit of Installing Data 'Back Door' in Pakistan Project," *Wall Street Journal*, 14 August 2021, www.wsj.com/articles/huawei-accused-in-suit-of-installing-data-back-door-in-pakistan-project-11628947988.

13 Samantha Hoffman, *Engineering global consent: The Chinese Communist Party's data-driven power expansion*, Australian Strategic Policy Institute, 14 October 2019, www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

14 Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, 15 August 2019, www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

15 For more information on the risks of dependence, please consult: Stefan Vladisavljev, *China's 'Digital Silk Road' Enters the Western Balkans*, China Observers in Central and Eastern Europe (CHOICE), June 2021, https://chinaobservers.eu/wp-content/uploads/2021/06/CHOICE_policy-paper_digital-silk-road_A4_web_04.pdf; and Stefan Vladisavljev, "Surveying China's Digital Silk Road in the Western Balkans," War on the Rocks, 3 August 2021, https://warontherocks.com/2021/08/surveying-chinas-digital-silk-road-in-the-western-balkans/.

16 For more information about Serbia's case, please see: Danilo Krivokapić, "Starting the Debate on Facial Recognition: A Case Study from Belgrade," part of Feldstein et al., *The Global Struggle over AI Surveillance: Emerging Trends and Democratic Responses*, June 2022, www.ned.org/wp-content/uploads/2022/06/Starting-Debate-on-Facial-Recognition-Case-Study-from-Belgrade-Krivokapic.pdf.

17 Bianca Wylie, "In Toronto, Google's Attempt to Privatize Government Fails—For Now," *Boston Review*, 13 May 2020, www.bostonreview.net/articles/bianca-wylie-sidewalk-labs-toronto/.

18 Dahlia Peterson, *How China harnesses data fusion to make sense of surveillance data*, Brookings Institution, 23 September 2021, www.brookings.edu/techstream/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/.

19 I am grateful to Samantha Hoffman for calling my attention to this issue. For more information, please see: "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," Human Rights Watch, 1 May 2019, www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

20 Feldstein et al., *The Global Struggle over AI Surveillance: Emerging Trends and Democratic Responses*.

21 Henry Farrell, Abraham Newman, and Jeremy Wallace, "Spirals of Delusion: How AI Distorts Decision-Making and Makes Dictators More Dangerous," *Foreign Affairs*, September/October 2022, www.foreignaffairs.com/world/spirals-delusion-artificial-intelligence-decision-making.

22 Chen and Greitens, "Information capacity and social order." In addition, and as a possible variant on this theme, which Gulnaz Sharafutdinova describes in the case of Russia, is the introduction of digital platforms that selectively allow popular input on "non-political" aspects of urban governance in order to shore up support for the government.

23 Ben Green, *The Smart Enough City: Putting Technology in its Place to Reclaim Our Urban Future* (Cambridge, MA: MIT Press, 2020).

24 Priyal Bhatt, Chris Doten, and Jillian Gilburne, *Municipal Digital Transformation Guidebook: A guide for municipal leaders with the drive to embark on digital transformation programs*, National Democratic Institute, 2021, www.ndi.org/sites/default/files/Municipal%20Digital%20Transformation%20Guidebook_final%20%281%29.pdf.

25 Farrell et al., "Spirals of Delusion."

Is Digitalization Endangering Democracy in Mauritius?

26 "Digital Mautirius 2030," Ministry of Technology, Communication & Innovation, Government of the Republic of Mauritius, 17 December 2018, https://govmu.org/EN/communique/Documents/DM%202030%2017%20December%202018%20at%2012.30hrs.pdf.

27 "Autocratization Turns Viral: Democracy Report 2021," Varieties of Democracy Institute (V-Dem), March 2021, www.v-dem.net/static/website/files/dr/dr_2021.pdf.

28 "Mauritians' satisfaction with democracy reaches new low, Afrobarometer study shows," Afrobarometer, 9 June 2022, www.afrobarometer.org/wp-content/uploads/2022/06/mau_r9.news_release-mauritians_satisfaction_with_democracy_reaches_new_low_9jun22.pdf.

29 Jessica Fjeld et al., "Mauritius Is Considering an Unprecedented Attack on Online Freedom," *Slate*, 20 May 2021, https://slate.com/technology/2021/05/mauritius-online-speech-government-proxy-servers.html.

30 "Consultation Paper on proposed amendments to the ICT Act for regulating the use and addressing the abuse and misuse of Social Media in Mauritius," Information & Communication Technologies Authority (ICTA), 14 April 2021, www.icta.mu/documents/2021/10/Social_Media_Public_Consultation.pdf.

31 "Constitution of the Republic of Mauritius," Attorney General's Office of the Government of the Republic of Mauritius, 12 March 1968, https://attorneygeneral.govmu.org/Documents/Laws%20of%20Mauritius/A-Z%20Acts/C/Co/Constitution,%20GN%2054%20of%201968.pdf.

32 "Mauritius 2020 Human Rights Report," U.S. Department of State, 2021, www.state.gov/wp-content/uploads/2021/10/MAURITIUS-2020-HUMAN-RIGHTS-REPORT.pdf.

33 "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," Human Rights Watch, 1 May 2019, www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

34 "Mauritius ICT Act Submission," Access Now, 12 May 2021, www.accessnow.org/cms/assets/uploads/2021/05/Mauritius-ICT-Act-Submission.pdf.

35 For more information, please see the Australian Strategic Policy Institute's "Mapping China's Tech Giants" interactive map here: https://chinatechmap.aspi.org.au/#/map/f2-Huawei.

[36] For more information, please see: https://chinatechmap.aspi.org.au/#/map/f5-Smart%20City-Public%20Security%20project.

[37] "The Data Protection Act 2017," Government of the Republic of Mauritius, 15 January 2018, https://dataprotection.govmu.org/Documents/DPA_2017_updated.pdf?csf=1&e=0rlrff.

[38] Mauritius Telecom was selected to provide security equipment, related hardware and software and licenses to the Government of Mauritius for a contractual period of 20 years.

[39] Huawei is the principal supplier of MSCP equipment.

[40] Samantha Hoffman, "China's Tech-Enhanced Authoritarianism," *Journal of Democracy* 33, 2 (2022), 76-89, https://muse.jhu.edu/article/852746.

[41] "Polémiques : Liying Zhu, ambassadeur de Chine « Je laisse le soin aux autorités d'enquêter »," *Le Mauricien*, 8 August 2022, www.lemauricien.com/actualites/societe/polemiques-autour-de-huawei-liying-zhu-ambassadeur-de-chine-je-laisse-le-soin-aux-autorites-denqueter/507262/.

[42] Axcel Chenney and Florian Lepoigneur, "«Sniffing» allégué: pourquoi l'excuse Huawei avancée par Hurreeram est complètement bidon," *L'Express*, 31 July 2022, https://lexpress.mu/article/411747/sniffing-allegue-pourquoi-lexcuse-huawei-avancee-hurreeram-est-completement-bidon.

[43] Praveen Swami, "How fears of Chinese digital espionage 'got RAW involved in Mauritius, led to snooping scandal'," *the Print*, 28 July 2022, https://theprint.in/world/how-fears-of-chinese-digital-espionage-got-raw-involved-in-mauritius-led-to-snooping-scandal/1055705/; and Axcel Chenney and Florian Lepoigneur, "«Sniffing» allégué: pourquoi l'excuse Huawei avancée par Hurreeram est complètement bidon."

Brazilian Smart Cities: From Principles to Practice

[44] Blenda Santos, "Smart cities and data protection," InternetLab, 26 July 2022, https://internetlab.org.br/en/news/smart-cities-and-data-protection-possible-routes/. (Full article only available in Portuguese).

[45] José Roberto Amaral, "São José é certificada a primeira Cidade Inteligente do Brasil," Prefeitura São José dos Campos, 16 March 2022, www.sjc.sp.gov.br/noticias/2022/marco/16/sao-jose-e-certificada-a-primeira-cidade-inteligente-do-brasil/.

[46] Minister Rogério Simonetti Marinho et al., "The Brazilian Charter for Smart Cities: Short Version," eds. Almir Mariano de Sousa Júnior et al., Brazilian Ministry of Regional Development, 2021, www.gov.br/mdr/pt-br/assuntos/desenvolvimento-urbano/carta-brasileira-para-cidades-inteligentes/The_Brazilian_Charter_for_SmartCities_Short_VersionFinal.pdf.

[47] "Câmara aprova lei que regula proteção de dados do município," Câmara Municipal de Vinhedo (Estado de São Paolo), 12 June 2018, www.camaravinhedo.sp.gov.br/portal/noticias/0/3/22289/camara-aprova-lei-que-regula-protecao-de-dados-do-municipio/.

[48] "Quem Somos?," ANDUS (Apoio à Agenda Nacional de Desenvolvimento Urbano Sustentável no Brasil), 11 November 2020, www.andusbrasil.org.br/sobre-o-andus/quem-somos; and "Seleção do Projeto," ANDUS, (originally put forth August, 2015), 14 November 2020, www.andusbrasil.org.br/sobre-o-andus/linha-do-tempo.

[49] This finding was one of the key conclusions outlined in a 2022 InternetLab report on the emergency aid transfer implemented in Brazil during the COVID-19 pandemic. For more information, please see: Clarice Tavares et al., "Emergency Aid in Brazil: Challenges in the Implementation of a datafied social protection policy," Derechos Digitales América Latina, February 2022, www.derechosdigitales.org/wp-content/uploads/03_Informe-Brasil_Artificial-Intelligence-and-Inclusion_EN_22042022.pdf.

[50] "Children's Right to Privacy: Obstacles and agenda for privacy protection and the development of informational self-determination of children in Brazil," Alana Institute and InternetLab, February 2021, https://internetlab.org.br/wp-content/uploads/2021/03/ilab-alana_childrens-privacy_EN_20210214-1.pdf.

[51] For more information, please consult: Larry Hardesty, "Study finds gender and skin-type bias in commercial artificial-intelligence systems," MIT News, 11 February 2018, https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212; Jesse Damiani, "New Research Reveals Facial Recognition Software Misclassifies Transgender, Non-Binary People," *Forbes*, www.forbes.com/sites/jessedamiani/2019/10/29/new-research-reveals-facial-recognition-software-misclassifies-transgender-non-binary-people/?sh=49924d41606b; and Tom Simonite, "The Best Algorithms Struggle to Recognize Black Faces Equally," *Wired*, 22 July 2019, www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/.

[52] "[Metrô] TJSP mantém proibição do uso de reconhecimento facial no metrô paulista," InternetLab, 29 April 2022, https://internetlab.org.br/pt/semanario/29-04-2022/#19066.

53 For more information, please visit the "Tire meu rosto da sua mira" ("take my face out of your sight") campaign website: https://tiremeurostodasuamira.org.br/en/home-eng/.

54 One of the most famous of these rankings is the "Ranking Connected Smart Cities," launched in 2015 and led by companies that sell market intelligence solutions. For more information, please consult: https://ranking.connectedsmartcities.com.br/.

55 "Prefeitura fortalece parcerias com Organizações da Sociedade Civil," Prefeitura de Contagem, 29 April 2022, www.portal.contagem.mg.gov.br/portal/noticias/0/3/75181/prefeitura-fortalece-parcerias-com-organizacoes-da-sociedade-civil.

ACKNOWLEDGMENTS

The authors appreciate the contributions of the International Forum's staff and leadership, including Christopher Walker, John Glenn, Kevin Sheives, John Engelken, Rachelle Faust, Lily Sabol, and Joslyn Brodfuehrer, all of whom played important roles in the editing and publication of this report. Particular acknowledgment goes to Beth Kerley, whose support and vision for this project were vital to its completion.

In addition, Roukaya Kasenally would like to acknowledge the Hoover Institution and its ongoing China's Global Sharp Power Project for which she wrote a paper entitled, "The Trappings of the Mauritius Safe City." She has used some of the findings outlined in that paper in this report.

Finally, the Forum wishes to thank Factor3 Digital for their efforts and invaluable support in designing this report for publication.

PHOTO CREDITS

Cover image: Photo by Vasin Lee/Shutterstock

Page 3: Photo by Blue Planet Studio/Shutterstock

Page 5: Photo by Tanawat Chantradilokrat/Shutterstock

Page 8: Photo by metamorworks/Shutterstock

Page 10: Photo by Sanchit Khanna/*Hindustan Times*/Shutterstock

Page 11: Photo by agilard/Shutterstock

Page 14: Photo by Nataly Reinch/Shutterstock

Page 18: Photo by fredex/Shutterstock

Page 19: Photo by Arnika Ganten/Shutterstock

Page 21: Photo by Joa Souza/Shutterstock