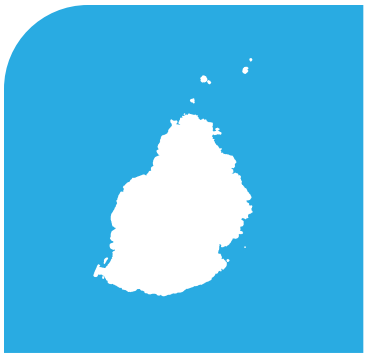
IS DIGITALIZATION ENDANGERING DEMOCRACY IN MAURITIUS?

// **ROUKAYA KASENALLY,** ASSOCIATE PROFESSOR, UNIVERSITY OF MAURITIUS

Digitalization has long been a prestige project for the government of Mauritius. In this regard, **the 2019 launch of a Safe City—a security-focused digitalization initiative using Huawei equipment and funding from the PRC—on this small island state fit within a well-oiled public rhetoric promising economic growth, global connectivity, and innovation**. Yet it is one of several recent projects in the digital sphere that could hasten the erosion of Mauritian democracy.

Reflecting a vision pursued by successive governments over the last thirty years, Mauritius boasts a well-developed ICT infrastructure. In the past decade, authorities have implemented **connectivity and e-governance initiatives** including the National Smart ID Card (2013), Open Data Mauritius (2015), the provision of 350 free Wi-Fi hotspots across the island (2017), the launch of a Citizen Support Portal (2017), the Mauritius Safe City Project, or MSCP (2019), and the rollout of 5G across the island (since 2021). The current focus is on achieving the goals set out in **"Digital Mauritius 2030,"** a policy blueprint that emphasizes digital government, ICT infrastructure, innovation, talent management, and cybersecurity.[26] Recently, however, this impressive technological trajectory has proceeded in tandem with a worrying political downturn.

Over the last five years, Mauritius has experienced significant democratic backsliding. It was classified by the V-Dem institute last year as among the "ten most rapidly autocratizing countries in the world,"[27] and only 32 percent of respondents in the most recent Afrobarometer public opinion survey expressed satisfaction with "the way democracy works in Mauritius."[28] Worrying trends include arbitrary arrests of journalists and other citizens, amendments to broadcasting and digital legislation, closures of certain private radio stations, the political weaponization of the police, and the weakening of key oversight institutions. This state of affairs can be attributed to a leader-centric political culture in which decision-making power is increasingly concentrated in the hands of one person. Over the last decade, these trends have intensified, giving rise to entrenched impunity, sycophantic behavior toward the country's leadership, and money-driven politics.



Mauritius is one of the "ten most rapidly autocratizing countries in the world"

At the very least, Mauritius's trajectory challenges any lingering assumptions that going digital automatically translates into greater transparency, accountability, and inclusion. But two recent initiatives suggest that the challenge runs deeper. **Together with a recent proposal by the country's Information and Communication Technologies Authority (ICTA) for regulating social media, the MSCP illustrates how the country's burgeoning digital ecosystem is offering both domestic and foreign actors alarming new powers through control over data.** These projects underscore the dangers of digital development in the absence of firm democratic guardrails; the difficulty of determining when projects launched in the name of enhancing public safety are actually tools for political surveillance; and the threats that opaque cross-border digital entanglements, particularly with authoritarian powers, can pose to democracy.

THE PUSHBACK AGAINST ONLINE SURVEILLANCE

In Mauritius's online sphere, an **attempted "authoritarian power grab"[29] involving new digital capabilities** was rebuffed last year amid massive local and international pushback. Although the proposal was put on hold, the debate around it illustrated how digital advances can enable or hasten democratic backsliding—in this case, one toward closing civic space online.

In April 2021, the ICTA released a consultation paper on "regulating the use and addressing the abuse and misuse of social media."[30] Its stated purpose was setting out a strategy to address "harmful and illegal online content" that would not depend on international social media companies. To this end, the paper proposed introducing a new decision-making body on online content, a technical enforcement unit, and a technical toolset.

The toolset, the provision that sparked the greatest outrage, would have served to separate social media data out from the broader flow of internet traffic in and out of Mauritius. After this division, **social media data would be routed through a government proxy server and "decrypted, re-encrypted and archived for inspection purposes as and when required."** ICTA justified the proposals as in sync with measures proposed or adopted to regulate online content in other democracies, such as Germany, the U.K., France, and India.

Although these countries have introduced requirements for social media platforms to take down certain categories of content, none of them have deployed a "technical toolset" allowing government officials to directly intercept and remove such content. The proposed measures also contravened rights enshrined in the Mauritian Constitution, which guarantees "freedom to . . . receive and impart ideas and information without interference."[31]

These intrusive proposals present particular concerns given a recent **trend toward suppression of civic activity online**, which has intensified since the most recent general election, held in 2019. Acts of repression have included the arrests of citizens who posted "anti-government comments," "routine" blocks on opposition politicians' social media accounts, and removal of these politicians' posts criticizing the government.[32] **Such incidents add force to concerns that the ICTA proposal was, in fact, aimed at suppressing dissent** on social media platforms, which have become extremely popular civic fora for politicians, CSOs, and ordinary citizens.

In this context, channelling social media traffic through government-controlled servers could fundamentally change the conditions for civic expression. Moreover, international precedents exist—most notably in the PRC—for the integration of social media data with data collected via offline surveillance in order to track individuals and intensify social control.[33]

The ICTA recommendations acted as a wake-up call for Mauritian citizens. ICTA received **more than 1,500 citizen submissions** concerning the document, civil society groups forcefully condemned the proposals, and sectors of the media decried the tactics used to advance them. This outcry ultimately caught the attention of international advocacy groups, which released a "joint civil society statement" asking the Mauritian Government and ICTA to "retract the consultation paper which proposes radically disproportionate measures to counter offensive speech on social media and presents a threat to human rights."[34] Observers believe that this **concerted approach by both local and international civil society** was a determining factor in shelving the proposal.

Channeling Mauritius's social media traffic through government-controlled servers could fundamentally change the conditions for civic expression.

Huawei advertising in Accra, Ghana.

THE QUIET SPREAD OF OFFLINE SURVEILLANCE

As with the ICTA proposals, Mauritius's democratic backsliding provides important context for the launch of the **Mauritius Safe City Project (MSCP)**. The Safe City Project emerged through an opaque, irregular process that evinces further erosion of the country's democratic guardrails. At the same time, broader political trends in Mauritius lend extra credence to concerns about the ends to which the MSCP's data collection capacities will ultimately be put. Yet in contrast to the outcry that followed ICTA's social media proposals, the installation of surveillance systems in Mauritius's physical public square has proceeded with remarkably little debate. Citizens have little to no understanding of the project. The only resistance to this initiative came from opposition parliamentarians who regularly questioned the MSCP, raising concerns about its financing, the absence of a legal or regulatory framework, and other accountability gaps. Subsequently, some media outlets started covering the MSCP. Amid this scrutiny, **the government hid behind the confidentiality clauses signed between the different parties involved in the project: the Mauritian police, the Mauritius Telecom, and Huawei**.

First announced in 2016, the MSCP is **one of more than twenty Huawei-backed smart or "Safe" city projects across the African continent**.[35] "Safe Cities" technologies are a relatively new feature of the African digital ecosystem. For this reason, there has not been much in-depth research into their impact on local political, economic, and social dynamics. The case of Mauritius, however, suggests cause for concern.

One of the MSCP's core justifications has been safety and security, and this focus is reflected in the project's technical makeup. As of its official launch in December 2019, the project entailed the installation of **four-thousand cameras with facial recognition and license plate recognition capabilities**, of which 2,760 are now fully operational, in addition to "a command and control centre and seven subcommand centres . . . cloud computing services, data centres, intelligent road surveillance and emerging communications equipment and services."[36] Tellingly, however, various interlocutors (including parliamentarians) have informed this author that they have on different occasions gone to the police to ask for the retrieval of images from the Safe City cameras pertaining to crimes committed in their constituencies but were told the cameras were not working or that they did not have access to the images. Moreover, the country's Safe City cameras allegedly failed to capture any information pertaining to the suspicious death (suspected murder) of a ruling party political agent in 2020.

The real intent behind the MSCP, which runs a total cost of US$455 million—financed by a loan from the Export-Import Bank of China—remains unclear. The project was casually announced in the Mauritian National Assembly during the national budget discussion and has "succeeded" in evading all forms of oversight ever since. **Confidentiality clauses** obscure the contracts among the key stakeholders involved. Furthermore, officials decided to **waive a competitive bidding requirement** for public procurements in order to select Mauritius Telecom to operate and maintain the MSCP. Some question whether this company's status as a para-statal body **outside the financial scrutiny of parliament and the government's own auditors** leaves the public largely in the dark about the project's actual cost.

Critical questions about how the MSCP will affect Mauritian politics against the backdrop of the country's recent democratic backsliding are also unanswered. Specifically, will data collected by MSCP cameras that are pumping images on a 24/7 basis serve to advantage or undermine particular political actors? Also, what safeguards are in place to ensure that these images will be secure from manipulation or misuse? It is believed that Mauritius has one of the best data protection laws in Africa; however, there is a **clause that authorizes the prime minister to override data protection safeguards in the interest of "national security, defence or public security**."[37]

Particularly in light of the island's recent shift toward authoritarianism, observers have voiced concerns that this concentration of personal power could enable political interference in data handling, including the abuse of Mauritius's new surveillance tools to control, manipulate, or intimidate opponents. These concerns are exacerbated by **opacity regarding the division of responsibilities among the different players involved—the Mauritian Police, Mauritius Telecom,[38] and Huawei**[39]—which makes it difficult to say who "owns" the data from the MSCP.

A final "red flag" concerns the role of Huawei within the MSCP. **Huawei is the main promoter of the "Safe Cities" across Africa and beyond.** Scant information has been disclosed about the exact nature of the controversial PRC company's role in conceiving and managing the MSCP. What can be ascertained so far is that Huawei approached the Government of Mauritius in early 2015 with an **unsolicited bid for setting up the MSCP**. Why was that so? Why did the Government of Mauritius respond positively? And whose model of safety or surveillance is being realized—one bounded by democratic norms and safeguards, or one premised on the pervasive government monitoring that underpins PRC digital authoritarianism?

A final "red flag" concerns the role of Huawei within the MSCP.

BETWEEN DEMOCRATIC BACKSLIDING AND FOREIGN DIGITAL ENTANGLEMENT

Like many backsliding democracies, Mauritius is now the site of a high-budget urban digitalization project that is transforming where and how authorities can surveil citizens. This project has been shrouded in secrecy, unfurling in a way that has **subverted democratic norms around government transparency, competitive procurement, and institutional accountability**—and potential malfeasance by local authorities is not the only cause for concern.

Huawei's role in the MSCP illustrates the particular risks that **engagement with foreign tech vendors** can present in the context of democratic backsliding. These kinds of projects present opportunities for politically influenced deals that subvert good governance norms, the import of undemocratic digital models from actors like the PRC, and the collection of sensitive data that could enable Beijing to further hone its tools of political influence.[40]

In its quest for greater digital connectivity and security, Mauritius has relied heavily on two foreign countries: the PRC and India. Both powers have aggressively expanded their footprint on the island over the last decade. In addition to its role in the MSCP, **Huawei has been instrumental in developing Mauritius's internet infrastructure**, including 3G (2004), 4G (2012), and 5G networks (2021), as well as the Mauritius Rodrigues Submarine fiberoptic cable (MARS). The current Chinese Ambassador to Mauritius has touted Huawei's role in enabling Mauritius to take its place "among the key contenders in the region."[41]

A Mauritian government minister recently took a dimmer view of the matter, publicly declaring that "the ex-CEO of Mauritius Telecom has surrendered our country completely to Huawei."[42] In addition to these concerns, it was recently disclosed that India—with Mauritian government permission—had used special equipment to "sniff" (intercept and retain) traffic on one of the submarine cables carrying internet data into and out of Mauritius, an action prompted by concerns about PRC digital espionage using Huawei infrastructure. These disclosures have triggered political scandal and a diplomatic mess for the island state.[43]

So, it is fitting to ask: Who is digitalization really benefitting? Will Mauritius's democratic institutions have control over the country's digital trajectory, or will that trajectory instead be shaped by opaque deals, growing concentrations of power, and unaccountable foreign actors? Mauritius sits amid a geopolitical battleground, the Indian Ocean, where key contenders—the U.S., the U.K., France, and India—have already secured a strategic foothold and where Beijing is desperately trying to mark its presence. It seems that data could be the most sought after resource. **In the MSCP, foreign digital influence and next-generation surveillance powers have converged with remarkably little public debate, let alone oversight.** If these key accountability mechanisms are not re-engaged, the flow of digital data could deal a further blow to Mauritian democracy.

If key accountability mechanisms are not re-engaged, the flow of digital data could deal a further blow to Mauritian democracy.

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