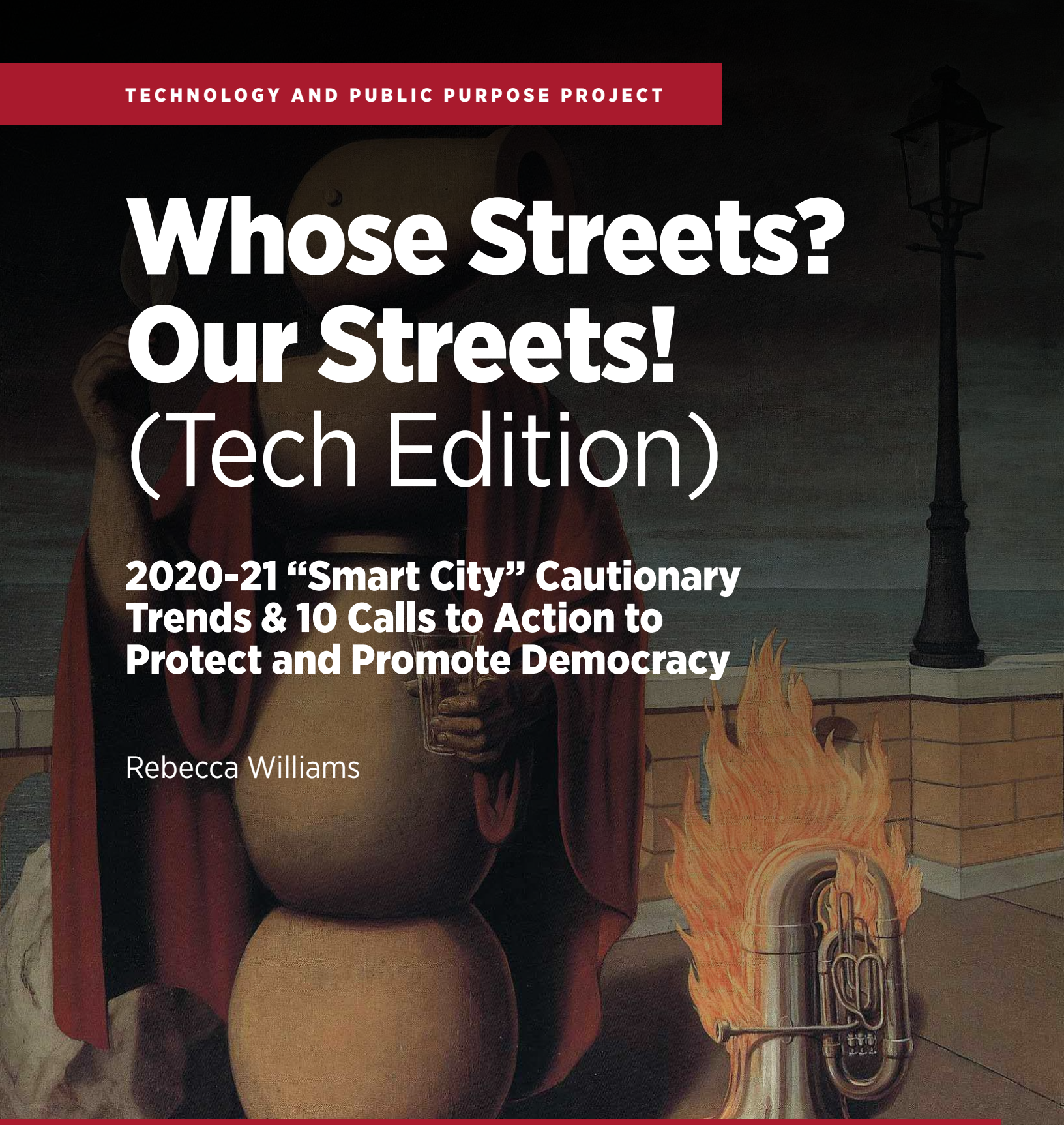
TECHNOLOGY AND PUBLIC PURPOSE PROJECT

Whose Streets? Our Streets! (Tech Edition)

2020-21 "Smart City" Cautionary Trends & 10 Calls to Action to Protect and Promote Democracy

Rebecca Williams



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
AUGUST 2021

Technology and Public Purpose Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/TAPP

Cover image: Les Droits de l'Homme, Rene Magritte 1947

Design and layout by Andrew Facini

Printed in the United States of America

TECHNOLOGY AND PUBLIC PURPOSE PROJECT

Whose Streets? Our Streets! (Tech Edition)

2020-21 "Smart City" Cautionary Trends & 10 Calls to Action to Protect and Promote Democracy

Rebecca Williams

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
AUGUST 2021

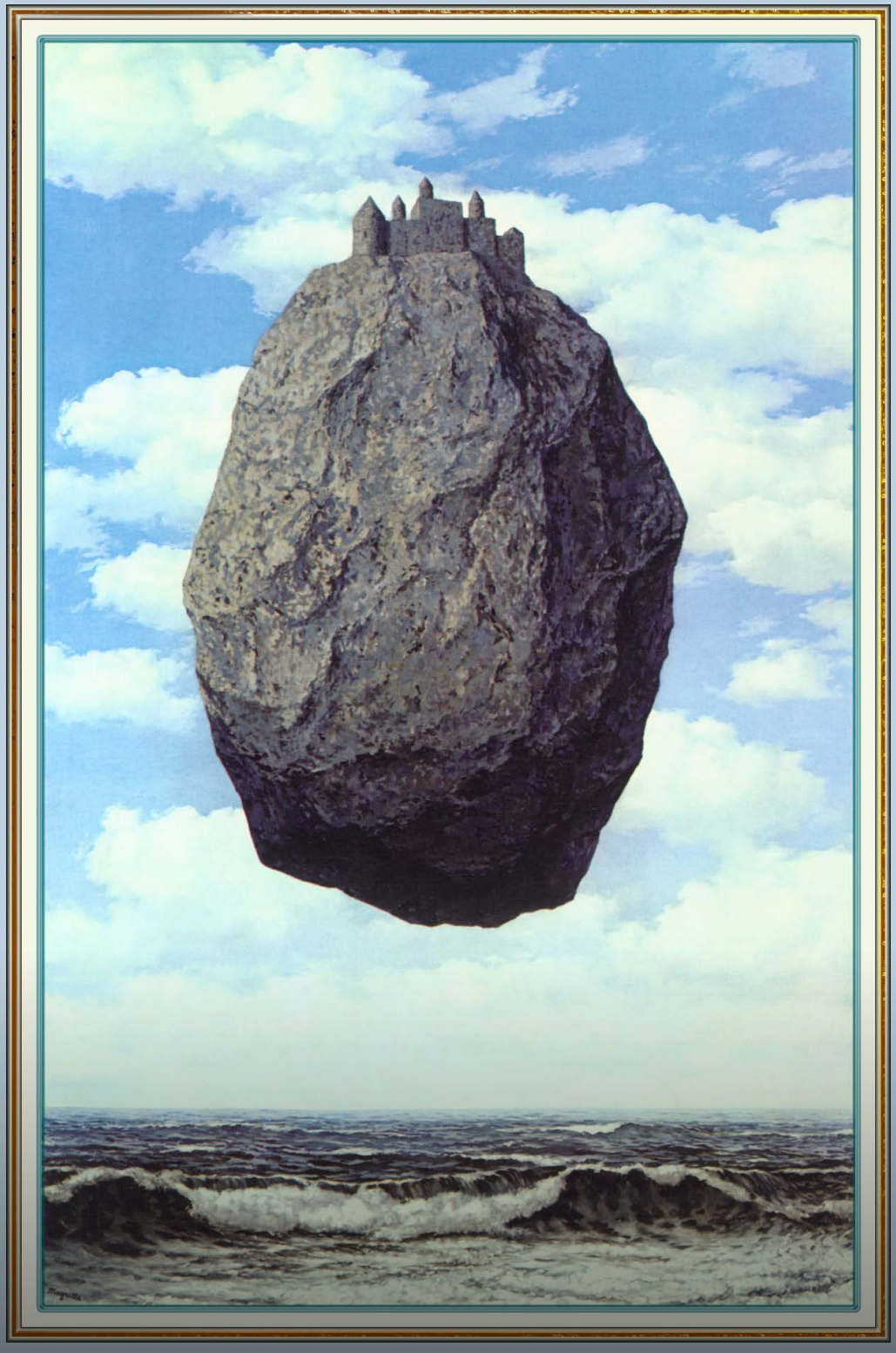
Acknowledgments

This report culminates my research on "smart city" technology risks to civil liberties as part of Harvard Kennedy School's Belfer Center for Science and International Affairs' Technology and Public Purpose (TAPP) Project. The TAPP Project works to ensure that emerging technologies are developed and managed in ways that serve the overall public good.

I am grateful to the following individuals for their inspiration, guidance, and support: Liz Barry, Ash Carter, Kade Crockford, Susan Crawford, Karen Ejiofor, Niva Elkin-Koren, Clare Garvie and *The Perpetual Line-Up* team for inspiring this research, Kelsey Finch, Ben Green, Gretchen Greene, Leah Horgan, Amritha Jayanti, Stephen Larrick, Greg Lindsay, Beryl Lipton, Jeff Maki, Laura Manley, Dave Maass, Dominic Mauro, Hunter Owens, Kathy Pettit, Bruce Schneier, Madeline Smith who helped so much wrangling all of these examples, Audrey Tang, James Waldo, Sarah Williams, Kevin Webb, Bianca Wylie, Jonathan Zittrain, my fellow TAPP fellows, and many others. Lastly, I am especially grateful to all of the journalists and scholars cited throughout this report; without your incredible dedication and insights, this report would not be possible.

All images included in this report are paintings by Rene Magritte, who once said, "If one looks at a thing with the intention of trying to discover what it means, one ends up no longer seeing the thing itself, but of thinking of the question that is raised." To which I say, *Whose Streets?*

Table of Contents



Le Chateau de Pyrenees

Rene Magritte 1959

Why Public Spaces Are Important for Democracy

The extent to which "smart city" technology is altering our sense of freedom in public spaces deserves more attention if we want a democratic future. Democracy–the rule of the people–constitutes our collective self-determination and protects us against domination and abuse. Democracy requires safe spaces, or commons, for people to organically and spontaneously convene regardless of their background or position to campaign for their causes, discuss politics, and protest. In these commons, where anyone can take a stand and be noticed is where a notion of collective good can be developed and communicated. Public spaces, like our streets, parks, and squares, have historically played a significant role in the development of democracy. We should fight to preserve the freedoms intrinsic to our public spaces because they make democracy possible.

Last summer, approximately 15 to 26 million people participated in Black Lives Matter protests after the murder of George Floyd making it the largest mass movement in U.S. history.[1] In June, the San Diego Police Department obtained footage[2] of Black Lives Matter protesters from "smart streetlight" cameras, sparking shock and outrage from San Diego community members. These "smart streetlights" were promoted as part of citywide efforts to become a "smart city" to help with traffic control and air quality monitoring. Despite discoverable documentation about the streetlight's capabilities and data policies on their website, including a data-sharing agreement about how they would share data with the police, the community had no expectation that the streetlights would be surveilling protestors. After media coverage and ongoing advocacy from the Transparent and Responsible Use of Surveillance Technology San Diego (TRUSTSD) coalition,[3] the City Council, set aside the funding for

1 Larry Buchanan, Quoctrung Bui & Jugal K. Patel, *Black Lives Matter May Be the Largest Movement in U.S. History*, The New York Times, July 3, 2020, https://perma.cc/N9MK-8A9A.

2 Jesse Marx, *Police Used Smart Streetlight Footage to Investigate Protesters*, Voice of San Diego, June 29, 2020, https://perma.cc/9Q5F-RTPN.

3 Sarah Holder, *In San Diego, 'Smart' Streetlights Spark Surveillance Reform*, Bloomberg CityLab, Aug. 6, 2020, https://perma.cc/H26Z-5NVS.

the streetlights[4] until a surveillance technology ordinance was considered and the Mayor ordered the 3,000+ streetlight cameras off. Due to the way power was supplied to the cameras, they remained on,[5] but the city reported it no longer had access to the data it collected. In November, the City Council voted unanimously in favor of a surveillance ordinance and to establish a Privacy Advisory Board.[6] In May, it was revealed that the San Diego Police Department had previously (in 2017) held back materials to Congress' House Committee on Oversight and Reform about their use facial recognition technology.[7] This story, with its mission creep and mishaps, is representative of a broader set of "smart city" cautionary trends that took place in the last year. These cautionary trends call us to question if our public spaces become places where one fears punishment, how will that affect collective action and political movements?

This report is an urgent warning of where we are headed if we maintain our current trajectory of augmenting our public space with trackers of all kinds. In this report, I outline how current "smart city" technologies can watch you. I argue that all "smart city" technology trends toward corporate and state surveillance and that if we don't stop and blunt these trends now that totalitarianism, panopticonism, discrimination, privatization, and solutionism will challenge our democratic possibilities. This report examines these harms through cautionary trends supported by examples from this last year and provides 10 calls to action for advocates, legislatures, and technology companies to prevent these harms. If we act now, we can ensure the technology in our public spaces protect and promote democracy and that we do not continue down this path of an elite few tracking the many.

4 Voice of San Diego, *Morning Report: 3 Body Cameras, No Footage*, Voice of San Diego, July 22, 2020, https://perma.cc/V3U8-8YYA.

5 Kate Cox, *San Diego's spying streetlights stuck switched "on," despite directive*, Ars Technica, Nov. 6, 2020, https://perma.cc/WAS7-SEHU.

6 Sarah Wray, *San Diego City Council backs surveillance technology ordinances*, Cities Today, Nov. 11, 2020, https://perma.cc/SJ5G-LVS6.

7 Jesse Marx, San Diego Held Back Materials Sought by Congress on Facial Recognition, Voice of San Diego, May 3, 2021, https://perma.cc/AG4Z-YSHQ.

How A "Smart City" Watches You

"Smart city" technology surfaced as a concept more than 20 years ago[8] and serves as an umbrella term for a wide range of technologies collecting and transmitting data in the city environment. For simplicity, this report will focus on "smart city" technology that is capable of collecting data that can identify individuals because that data can be used to target individuals, which in turn can erode the sense of safety and inclusivity requisite for public spaces to serve as commons for democratic functions.

Technology

Many types of technology may fall under the umbrella term of "smart city" technology. This report will focus primarily on the hardware and software associated with cameras, location trackers, and sensors. These technologies are common components in broader "smart city" technologies and projects, and they have the high-risk ability to collect data that can directly, or in combination with other data, identify individuals. Technologies all have inherent affordances, that is qualities or properties that define their possible uses or clarify how they can or should be used. These technology components all have the inherent capabilities to track individuals. Simply put, these are devices that may be watching you.

Cameras

Security cameras in public spaces first became a common practice in the 1970s and 1980s. The proliferation of these cameras, their capacity to identify individuals, and their uses by law enforcement are steadily increasing. Public Closed-Circuit Television (CCTV) cameras come in various shapes and sizes and may be attached to various government-owned fixtures such as buildings, telephone poles, and traffic lights. In addition, cameras may be inconspicuously attached to unmanned aerial vehicles (UAVs) like drones or spy planes or built into other devices like kiosks, mirrors,

8 GlobalData Thematic Research, *History of smart cities: Timeline*, Verdict, Updated July 6, 2020, https://perma.cc/Q86L-7LRS.

parking meters, poles, scooters, street lights, and traffic lights. Lastly, law enforcement may be wearing body-worn cameras. In addition to government-owned cameras, privately-owned cameras, including cameras built into cell phones, may be filming you. These cameras may have real-time biometric recognition software built into the device itself, such as facial recognition, fingerprint recognition, iris recognition, gait recognition, and tattoo recognition. These sets of software are often also referred to as "technologies."

Location Trackers

Cell phones and various transportation-related technologies collect location data. If governments or corporations collect this data at an individual level, it can be used to identify individuals and track their every move. Cell phones can disclose your location in many ways, including mobile signal tracking from towers, mobile signal tracking from cell-site simulators, Wi-Fi, Bluetooth, and location information from applications and web browsing.[9] Bikeshare, rideshare (including taxis), and scooters can collect individual trip data via GPS or their associated cell phone application and privately owned vehicles can provide telematics data or "vehicle forensics kits" to third parties. Public transit can collect individual trip data and link it to your transit card or personal financial information. Mobility data can be collected by third-party devices such as Automated License Plate Readers (ALPRs), Intelligent Transportation Systems, or cell phone location data brokers. ALPRs are commonly mounted on tow trucks, law enforcement cars, and surveillance cameras. In addition to cameras and sensors, Intelligent Transportation Systems can include induction loops, infrared, radar, sound or video imaging, or Bluetooth that collect mobility data.

Sensors

Sensors convert stimuli such as heat, light, sound, and motion into electrical signals and can be used to identify individuals' presence or identifying

9 Alexis Hancock, *Surveillance Self-Defense Playlist: Getting to Know Your Phone*, Electronic Frontier Foundation, May 6, 2021, https://perma.cc/XN3R-ZNNE.

qualities. Some common applications of using these sensors to watch people in cities have been the use of audio sensors (like ShotSpotter[10]) to detect and analyze audio signals, infrared sensors, Light Detection and Ranging (LiDAR) sensors, motion sensors (that use microwave, reflective, ultrasonic, or vibration sensing) to detect moving people and vehicles, and thermal sensors which are commonly used to detect the heat of suspects or victims by law enforcement.

Other Watching Technology

Other "smart city" technology items that are not covered in the broad three categories above that may be collecting data that can identify individuals include Information and Communications Technology (ICT) infrastructure (cell phone towers powering up to 5G[11] and public Wi-Fi), Internet of Things (IoT) or GPS-system connectivity to various things such as electronic monitoring, "smart tags" and RFID Chips, online activity (of government websites, financial transactions, social media analysis), police robots (like Boston Dynamics' digidogs[12] or Knightscope's rolling pickles[13]), and "smart kiosks" and USB ports.

Data

What data cameras, location trackers, and sensors collect, whether or not it is being analyzed in real-time, and how it is managed throughout its life all affect its likelihood of creating risks for individuals. Identifying data exists on a spectrum.[14] For example, data with "direct identifiers" such as your name, biometric, or address can readily identify you. This data type has historically been categorized as personally identifiable information (PII)

10 Freddy Martinez & Lucy Parsons Labs, *Op-Ed: End the City's ShotSpotter Contract*, South Side Weekly, Apr. 28, 2021, https://perma.cc/BP69-SL24.

11 Robert Muggah & Greg Walton, *'Smart' Cities Are Surveilled Cities,* Foreign Policy, Apr. 17, 2021, https://perma.cc/TB7G-42JQ.

12 Boston Dynamics, *Spot*, Boston Dynamics, https://perma.cc/2Q2B-SFWV.

13 Frank Hansen, *Little Girl Meets Knightscope Security Robot Patrolling Mall*. YouTube, https://perma.cc/T3L6-KQXU.

14 Boris Lubarsky, *Re-Identification of "Anonymized" Data*, Georgetown Law Technology Review (2017), https://perma.cc/GBR8-X5L3.

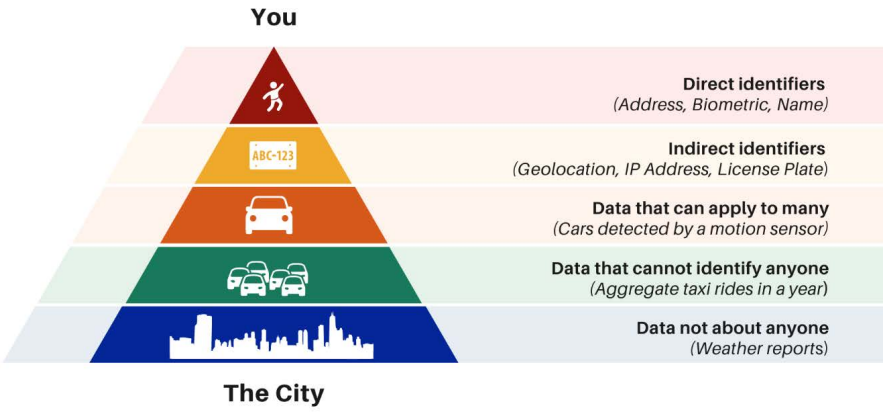
and is the riskiest data for the technologies above to collect. Further along the spectrum, and the next riskiest are "indirect identifiers" that combine with other data to identify you—for example, your IP address, geolocation, or license plate number. Further still along the spectrum are data that can be ambiguously linked to multiple people—for example, cars detected by a motion detector.

This data by itself may not be able to identify you, but in certain contexts it may be able to. As more data is collected and data joining techniques become more sophisticated, so does the ability to re-identify someone within a seemingly ambiguous dataset. This ability is commonly referred to as the "mosaic effect" derived from the mosaic theory of intelligence gathering, in which "disparate pieces of information—although individually of limited utility—become significant when combined with other types of information."[15] As re-identifying risks increase, data practitioners are challenged with the trade-offs of collecting granular data, which can be of high research utility and protecting against re-identification harms.

Throughout this report, I will refer to data that can directly or indirectly or through re-identification techniques identify an individual as "identifying data." I will argue that in the "smart city" context, identifying data collection can lead to harms that threaten democracy, so the question for communities will be, what utility is worth that trade-off? Further down the identifying data spectrum is data that cannot be linked to a specific person, such as aggregated taxi rides in a year. And lastly, on the spectrum is data that is not linked to individuals, like weather reports.

15 John Czajka, et al., *Minimizing Disclosure Risk in HHS Open Data Initiatives*, ASPE (2015), https://perma.cc/E4R8-U6L7.

How a "Smart City" Watches You: *Identifying Data Spectrum*

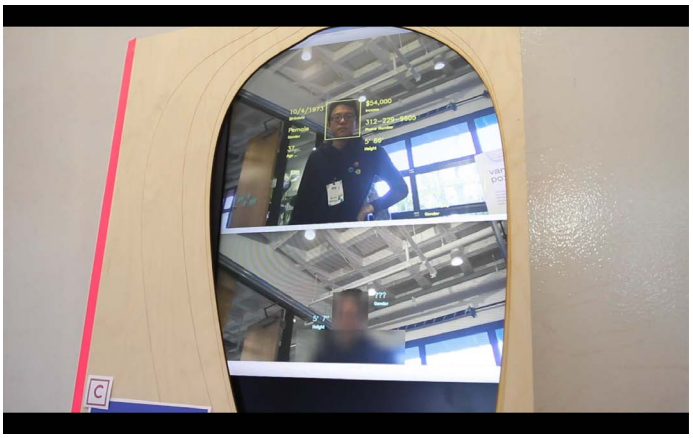


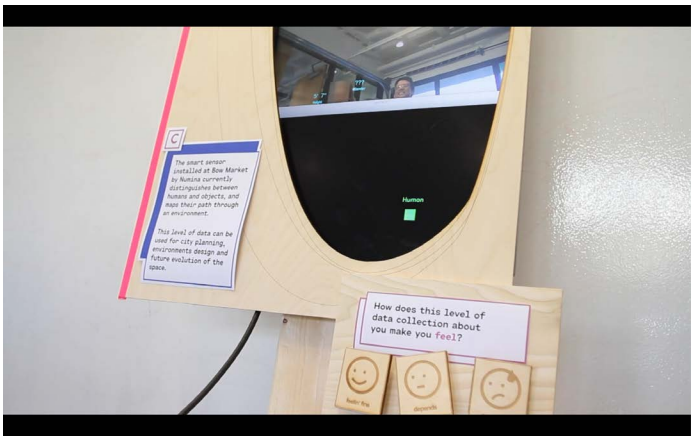
Source: Rebecca Williams, Whose Streets? Our Streets! (Tech Edition)

Whether or not identifying data is analyzed in real-time, as opposed to historical snapshots, affects its riskiness because it allows for real-time targeting. Lastly, beyond the collection of identifying data, how these data-sets are managed throughout the entire data lifecycle (stored, accessed, analyzed, joined, etc.) can expand the ability to identify, and thus target, individuals.

While the above technologies can collect data that can be used to identify you, it does not necessarily mean that they are or have to. For example, cameras can be replaced with motion detectors or configured with "video anonymization software" to collect blurred images. Images can also be altered after collection to better protect against re-identification with image-altering tools that blur or pixelate and strip identifying metadata or use generative adversarial network (GAN) escape detection techniques to create fake derivative images that look similar to the naked eye. (These post-collection techniques may not successfully protect against the risks of re-identification by highly skilled technologists now or in the future as traces of the original image may be detectable.) On the other hand, cameras can be augmented with facial recognition technology which can use algorithms to match a crisp image of your passing face with a known image of you. Relatively new, facial recognition technology got twenty times better at recognizing a person out of a collection of millions of photos between 2014 and 2018. In addition, the technology has become much more affordable. Until recently, it would be a safe assumption to remain anonymous in public spaces unless you ran into someone you knew. If

facial recognition technology is scanning public spaces at all times, that is no longer a safe assumption[16] and changes the nature of public spaces and how we will operate in them. At the farthest end of the spectrum, cameras can be augmented with real-time biometric recognition capabilities to quickly identify you and lookup related datasets about you to form a composite of who you are. These big data systems are already being used, such as in Kashgar, where a state-run defense manufacturer, China Electronics Technology Corporation, runs a high-tech surveillance system to monitor and subdue millions of Uyghurs and members of other Muslim ethnic groups.[17] Examples of these developing big data systems in the U.S. include advanced analytics promising "digital twins," predictive policing, fusion centers or real-time crime centers, and video analytics. IDEO CoLab illustrated this range of data possibilities for cameras in an interactive art exhibit. See *screengrabs below.*





16 Tom Simonite, *How Face Recognition Can Destroy Anonymity*, Wired, Apr. 20, 2021, https://perma.cc/C25R-CTV8.

17 Chris Buckley & Paul Mozur, *How China Uses High-Tech Surveillance to Subdue Minorities*, The New York Times, May 22, 2019, https://perma.cc/7MJ4-HZM3.

Screengrabs from Vanishing Points: An IDEO CoLab Prototype, a Collaborative Cities concept from the April 2019 IDEO CoLab design sprints depicting how cameras can be collecting different types of data

Location trackers can range in granularity of data between individual trips and aggregate yearly trips. Personal trip data can easily be used to connect you to specific sensitive trips. For example, when a trip begins at a sensitive location such as a political protest, all the government would need to know is who lives at the house at the end of the trip to identify them and note their involvement in the demonstration. Location trackers can range in how location data is joined with other datasets. For example, cell phone applications sometimes include subcomponent software, like X-Mode,[18] that can track your location across applications to create a complete dataset of your location at all times.

Sensors range in how they sense people, sometimes collecting identifying data such as biometrics, re-identifying data such as drug use in water,[19] or aggregate foot traffic data while generating energy.[20] While many sensors are not directly aimed at tracking individuals, it does not mean that information collected from them could not be paired with other data streams like facial recognition and artificial intelligence (AI) against an individual. Steve Bellovin, a computer science professor at Columbia University, offered the *Wall Street Journal*[21] the following hypothetical: "might a pollution sensor detect cigarette smoke or vaping, while a Bluetooth receiver picks up the identities of nearby phones? Insurance companies might be interested." Still, other sensors may be collecting data about the environment, such as precipitation sensors, that cannot be used to identify anyone.

18 Byron Tau, *Apple and Google to Stop X-Mode From Collecting Location Data From Users' Phones*, Wall Street Journal, Dec. 9, 2020. https://perma.cc/87RK-KVFA.

19 Troy Farah, *The Plan to Test Cities' Sewage for Drugs Is a New Form of Mass Surveillance*, Motherboard Tech by VICE, Jan. 23, 2017, https://perma.cc/X6RG-T79C.

20 OVO Energy, *Kinetic Pavements Are Giving a Whole New Meaning to 'Power Walking',* OVO Energy, Feb. 28, 2018, https://perma.cc/3AFA-NAM4.

21 Matthew Kassel, *As 5G Technology Expands, So Do Concerns Over Privacy*, Wall Street Journal, Feb. 27, 2019, https://perma.cc/MH8E-HX7H.

Uses

While certain technologies create dangerous affordances and identifying data creates inherent risks to individuals, how this data is legally permitted to be accessed and used is of great significance to societal power structures and effects on democracy. Today, "smart city" technology, often sold under a banner of "collective goods," is knowingly or unknowingly being repurposed by law enforcement for widespread surveillance and punitive purposes. Specific examples of this mission creep will be detailed further in the report.

To minimize the harms of this technology, some jurisdictions have begun to regulate facial recognition technology[22] and surveillance technology.[23] To reduce the harms that can arise from collecting identifying data, some jurisdictions have started to regulate the collection of biometrics,[24] consumer data,[25] and general data protection, like the European Union's (EU) General Data Protection Regulation (GDPR), and specific other datasets. Finally, to minimize the harms of these uses, some jurisdictions have begun regulating how this data can be used after it is collected, such as banning the use of facial recognition databases like ClearviewAI in Canada[26] or the sharing of personal transit data by transit agencies without a warrant in Massachusetts.[27] Many of these laws regulate all three aspects of technology, data, and use to some extent. Still, I have found it helpful to think about these items distinctly because they each have different ways of creating harm and different regulatory challenges, which will become evident as we explore these harms and interventions further.

22 Jameson Spivack & Clare Garvie, *A Taxonomy of Legislative Approaches to Face Recognition in the United States*, AI Now Institute, https://perma.cc/7W97-AABU.

23 Rebecca Williams, *Everything Local Surveillance Laws Are Missing In One Post,* Belfer Center for Science and International Affairs, Apr. 26, 2021, https://perma.cc/RN59-KUZ3.

24 Epiq, *State Biometric Laws are Trending and Class Actions Could be on the Rise*, JD Supra, Mar. 24, 2021, https://perma.cc/4XJ4-933P.

25 Sarah Rippy, *US State Privacy Legislation Tracker*, IAPP, Updated June 21, 2021, https://perma.cc/V83P-6B2U.

26 Office of the Privacy Commissioner of Canada, *PIPEDA Report of Findings #2021-001: Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*, Feb. 2, 2021, https://perma.cc/2VFR-5FDC.

27 An Act Authorizing and Accelerating Transportation Investment. 2020 Mass. Acts Chapter 383.

"Smart City"
2020-21
Cautionary Trends

Totalitarianism

- *Deploying Without the Will of the People*
- *Replacing Participation with Technocraticism*
- *Collecting Data That Serves Totalitarianism*

Panopticonism

- *Eroding Privacy, Autonomy, & Freedom*
- *Allowing Unwarranted Searches & Seizures & Permission-less Experimentation*
- *Risking Security*

Discrimination

- *Targetting Discriminated Against Populations*
- *Deepening Historic Discrimination & (In)visibility*
- *Providing Unequal (Digital Services*

Privatization

- *Replacing Democracy With Corporate Decision-making*
- *Bypassing Constitutional Protections & Accountability Laws*
- *Expanding Surveillance Monopolies*

Solutionism

- *Deploying Without Proven Efficacy Or Risk Analyses*
- *Taking Resources Away From Providing For People's Material Needs*
- *Technology Begets More Technology*

Source: Rebecca Williams, Whose Streets? Our Streets! (Tech Edition)

La Trahison des images (Ceci n'est pas une pipe)
Rene Magritte 1929

2020-21 "Smart City" Cautionary Trends

Below I have briefly outlined cautionary trends of where "smart city" technology may be headed. No section is intended to provide a comprehensive description of these concepts, nor are the examples an exhaustive account of these phenomena. Instead, this framework is intended to be a provocation and a 2020-21 highlight reel of "smart city" technology cautionary tales, with all of the cited examples taking place in the last year. While this report is primarily intended for a U.S. audience, these problems are global, and these cautionary tales come from around the world to highlight that these harms are not hypothetical but happening today. My hope for readers is to consider these possibilities, their likely ends and to build on these ideas.

Totalitarianism

Totalitarianism is a form of government that controls all aspects of its people's public and private lives and is often described by scholars as the opposite of democracy. In *The Human Condition*, Hannah Arendt articulates how the public realm is requisite to pluralism and democracy itself:

> This attempt to replace acting with making is manifest in the whole body of argument against "democracy," which, the more consistently and better reasoned it is, will turn into an argument against the essentials of politics. The calamities of action all arise from the human condition of plurality, which is the condition sine qua non for that space of appearance which is the public realm. Hence the attempt to do away with this plurality is always tantamount to the abolition of the public realm itself. The most obvious salvation from the dangers of plurality is monarchy, or one-man-rule, in its many varieties, from outright tyranny of one against all to benevolent despotism and to those forms of democracy in which the many

> form a collective body so that the people is "many in one" and constitute themselves as a "monarch."[28]

In *The Origins of Totalitarianism*, she goes on to describe how the destruction of the public realm fuels totalitarian rule stating, "totalitarian government, like all tyrannies, certainly could not exist without destroying the public realm of life, that is, without destroying, by isolating men, their political capacities."[29] "Smart city" technology disrupts and destroys the public realm in our cities in three ways:

- It is deployed without the will of the people;
- It replaces a participatory dialogue, "*What would we like in our neighborhood?*" with technocratic analysis by the state, *"They will design data collection that will inform them to what they will do with our neighborhood;"* and
- It is designed with identifying data collection that empowers mono-ideology, a police state, and the chilling of freedom of expression and dissent.

Deploying Without the Will of the People

A first-order question is whether the local community wants the "smart city" technology? To know the answer to this question, government representatives must facilitate ongoing engagement with community members to learn what they desire in their community and if participatory data collection is a part of their collective goals. For governments to deploy technology that can identify individuals and their activity without their will–such as affirmative consent or informed vote, or protections like warrant authorizations–should be viewed as a totalitarian act. The government should not be tracking you without a democratic discussion and decision about that.

28 Hannah Arendt, The Human Condition (1958)

29 Hannah Arendt, The Origins Of Totalitarianism (1951)

2020-21 "Smart City" Examples:

- In Toronto, community members protested the city's deal with Sidewalk Labs citing issues with the privatization of public space, privacy of a corporation collection data in public spaces, and accountability risks if the corporation was allowed to analyze, and display the activities, choices, and interpersonal interactions in the fine detail of the individuals who use the space. This protest exemplified that the community was not consulted before the city sought out procurement with Sidewalk Labs.[30]
- In Detroit, the public spoke against a $2.5 million plan to install hundreds of traffic light-mounted cameras at city intersections in a public meeting.[31]
- In the U.S., after technology company Apple provided the capability to opt-out of app tracking in their iPhone iOS 14.5 update, 96% of users used it,[32] strongly suggesting that when given that option, people do not want to be tracked by applications on their phone.

Replacing Participation With Technocraticism

The next question is, does "smart city" technology help democratic input and governance by the people? "Smart city" technology, data, and uses currently skew top-down, with government officials and their vendors deciding what is collected and how it is used, rather than a more bottom-up approach, where people willingly participate in defining collective goals and the design of any related data collection. Further, the rhetoric of data-driven government, "Moneyball for government," behavioral nudges, and evidence-based policy popular in U.S. government management circles rest on the premise that if the government collects enough data, they can derive operational efficiencies and save money managing government programs and services. With enough data, you can "manage" the people

30 Privacy International, *City of Toronto Deal with Sidewalk Labs Sparks Public Protests*, Privacy International, https://perma.cc/R8GR-ECK7.

31 Christine Ferretti, *Traffic light-mounted camera expansion in Detroit spurs privacy concerns*, Detroit News, Nov. 16, 2020, https://perma.cc/4BPN-Y2PW.

32 Samuel Axon, *96% of US users opt out of app tracking in iOS 14.5, analytics find*, Ars Technica, May 7, 2021, https://perma.cc/6DRQ-SZSV.

themselves. Technocratic analysis by governments is not new, but the vast expansion of surveilling individuals, rather than engaging in dialogue with them directly through participatory means is unprecedented. This move away from participatory dialogue needs to be corrected if we want democracy to serve community needs.

2020-21 "Smart City" Examples:

- In Birmingham, their Mayor Randall Woodfin declared, "If we don't have witnesses to come forward, then our only other option is more [police] technology."[33]
- In Lucknow, India, the police deployed facial recognition technology aimed at women's faces claiming to use artificial intelligence (AI) to read whether or not a woman was in distress while walking about the city to alert law enforcement.[34]
- Globally, governments are using services like Media Sonar, Social Sentinel, and Geofeedia to analyze online conversations to try to gauge public sentiment. Even "privacy-protecting" companies like Zencity, which only offers aggregate data and forbids targeted surveillance of protestors, have been used for potentially alarming uses such as police monitoring of speech that is critical of police. When Pittsburgh City Councilor Deb Gross learned of the use of this tool (which was not disclosed to the city council before its use due to a free trial), she said, "Surveilling the public isn't engaging the public, it's the opposite."[35]

Collecting Data That Serves Totalitarianism

Lastly, we must ask, does this "smart city" data collection support totalitarian qualities, such as mono-ideology, chilling of dissent, or a police state? An essential function of democracy is for the people to be able to debate different

33 Sam Prickett, *Birmingham Police Need The Public's Help In Solving Homicides, Woodfin Says*, WBHM 90.3 BIRMINGHAMWATCH, Dec. 30, 2020, https://perma.cc/85VL-WGPH.

34 Pramit Chatterjee, *Lucknow Police's Decision To Use AI Cameras To Keep Track Of Women In Distress Raises Concerns*, Mashable India, Jan. 22, 2021, https://perma.cc/FU62-NBQF.

35 Sidney Fussell, *This AI Helps Police Monitor Social Media. Does It Go Too Far?*, Wired, https://perma.cc/6WT6-Y3J5.

ideologies. In an increasingly watched world, the data collectors and managers set the narrative by what they choose to collect and what they do not. This narrative-setting quality can result in mono-culture or promote mono-ideologies. Because of this threat, the community should critically examine who collects the data and how they use it in story-telling. In the U.S., the First Amendment protects the five freedoms of speech, religion, press, assembly, and the right to petition (protest) the government. The surveillance imposed by "smart city" technology could have a chilling effect on community members feeling comfortable participating in these protected activities for fear of harassment or retaliation by law enforcement. Beyond the chilling of dissent, how does "smart city" technology fuel a police state? "Smart city" data supposedly collected for planning or efficiency purposes can be repurposed for enforcement purposes and currently without the requirement of review like a warrant. At what point does "safe city" rhetoric create an environment where you can effectively be tracked by law enforcement at all times?

2020-21 "Smart City" Examples:

- Globally surveillance of protesters has harmed people's right to privacy and right to free assembly and association. In the United States, the unprecedented participation in Black Lives Matters protests during the summer of 2020[36] were met with surveillance by streetlights in San Diego, business district cameras in San Francisco,[37] Ring cameras in Los Angeles,[38] helicopters in Philadelphia, Minneapolis, Atlanta, and Washington,[39] spy planes in Baltimore[40] and Florida,[41] and facial recognition technology in New York,[42] Miami,[43] and

36 Larry Buchanan, Quoctrung Bui & Jugal K. Patel, *supra* note 1.

37 Dave Maass and Matthew Guariglia, *San Francisco Police Accessed Business District Camera Network to Spy on Protestors*, Electronic Frontier Foundation, July 27, 2020, https://perma.cc/RL62-25QP.

38 Sam Biddle, *LAPD Sought Ring Home Security Video Related to Black Lives Matter Protests*, The Intercept, Feb. 16 2021, https://perma.cc/X6DP-3J8W.

39 April Glaser, *Experts weigh in on National Guard monitoring protests*, NBC News, Jan. 10, 2021, https://perma.cc/WE5A-MS8Q.

40 Kim Lyons, *Baltimore spy plane program was invasion of citizens' privacy, court rules*, The Verge, June 24, 2021, https://perma.cc/E9WV-5RGM.

41 Joseph Cox, *Florida Cops Flew Spy Plane Above Press Conference for Black Teens Killed by Police*, Motherboard Tech by VICE, Apr. 26, 2021, https://perma.cc/9T32-TDK2.

42 George Joseph & Jeff Offenhartz, *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment*, Gothamist, Aug. 14, 2020, https://perma.cc/JDN2-KT9N.

43 Kate Cox, *Cops in Miami, NYC arrest protesters from facial recognition matches*, Ars Technica, Aug. 19, 2020, https://perma.cc/232S-JHDB.

Pittsburgh.[44] At least 270 hours of aerial footage from 15 cities was gathered on behalf of the Department of Homeland Security (DHS)[45]. Abroad, protestors were monitored by facial recognition technology in China,[46] England,[47] Hong Kong,[48] India,[49] Israel,[50] Myanmar,[51] Russia,[52] Slovenia,[53] South Africa,[54] Uganda,[55] and the United Arab Emirates.[56] In addition, facial recognition technology was used by laypeople to identify the rioters who stormed the U.S. Capitol on January 6th, highlighting that these identifying tools are available to anyone and that policymakers take care to in defining provisions to protect protestors.

- Globally, law enforcement has expanded their surveillance capabilities, such as Chula Vista's experimentation with drones powered with artificial intelligence,[57] U.S. Customs and Border Protection's plans to collect the faceprint of virtually every non-U.S. citizen and store them in a government database for 75 years,[58]

---

44 Mike Holden, *Pittsburgh police used facial recognition technology during Black Lives Matter protests*, WPXI-TV, May 21, 2021, https://perma.cc/R7L9-6V66.

45 Zolan Kanno-Youngs, *U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance*, The New York Times, June 19, 2020, https://perma.cc/5JZY-HK4P.

46 Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, The New York Times, Apr.14, 2019, https://perma.cc/95YT-56SV.

47 Isobel Asher Hamilton, *British police scanned 8,600 people's faces in London without their consent, resulting in just 1 arrest and 7 false positives*, Business Insider, Mar. 4, 2020, https://perma.cc/B3VV-Z87M.

48 Paul Mozur, *In Hong Kong Protests, Faces Become Weapons,* The New York Times, July 26, 2019, https://perma.cc/3RLG-V9XJ.

49 Benjamin Parkin, *Indian police use facial recognition in search for farmer protesters*, Financial Times, Jan. 28, 2021, https://perma.cc/5XKF-TCJV.

50 Amitai Ziv, *This Israeli face-recognition startup is secretly tracking Palestinians*, Haaretz, Jul. 15, 2019, https://perma.cc/GU5M-AJGZ.

51 Nyan Hlaing Lin & Min Min, *Hundreds of Huawei CCTV cameras with facial recognition go live in Naypyitaw*, Myanmar NOW, Dec. 15, 2020, https://perma.cc/236F-QRWW.

52 Robyn Dixon, *Russia's surveillance state still doesn't match China. But Putin is racing to catch up.*, Washington Post, Apr. 17, 2021, https://perma.cc/5J34-XSXA.

53 Lenart J. Kučić, *Slovenian police acquires automated tools first, legalizes them later,* AlgorithmWatch, July 7, 2020, https://perma.cc/QJ3X-96T2.

54 Carien du Plessis, *Why Johannesburg's anti-crime cameras are similar to apartheid-era pass laws - expert*, News24, Apr. 13, 2021, https://perma.cc/PG85-E75S.

55 Stephen Kafeero, *Uganda is using Huawei's facial recognition tech to crack down on dissent after protests*, Quartz, Nov. 27, 2020, https://perma.cc/MJM8-UT9H).

56 Ali Al Shouk, *How Dubai's AI cameras helped arrest 319 suspects last year*, Gulf News, Mar. 18, 2019, https://perma.cc/K6FB-WNCM.

57 Cade Metz, *Police Drones Are Starting to Think for Themselves*, The New York Times, Dec. 5, 2020, https://perma.cc/FHK9-E8ST.

58 Homeland Security Department, *Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States*, Federal Register, Nov. 19, 2020, https://perma.cc/RT67-X8LN.

and the expansion of "real-time crime centers" throughout the United States.[59] In Greece, police have been given devices that let them carry out facial recognition and fingerprint identification in real-time.[60] As will be detailed further in this report, the scope of data law enforcement has access to without a warrant extends far beyond their tools to seemingly benign infrastructure like streetlights and scooters and to private entities.

- Throughout the U.S., governments have not disclosed this expansion to the public. Washington D.C.'s failed to publicly disclose their use of a facial recognition system until it arose in protest court documents[61] and San Diego failed to disclose their use of facial recognition to Congress.[62] Use of these technologies has been repeatedly lied about, such as with Baltimore's false statements about how their mass surveillance data was used in their surveillance plane,[63] Long Beach's broken promise to not send license plate data to ICE,[64] and New Orleans' police use of facial recognition software to investigate crime despite years of assurances that they were not.[65] Further, many police technology programs erected in the name of transparency have under police management failed to deliver that promise, such as Omaha and Tallahassee's police department's failures to disclose police bodycam footage[66] and New York City's police department's failure to meaningfully disclose their use of surveillance technologies as required by the *Public Oversight of Surveillance Technology Act*.[67]

---

59 Rowan Moore Gerety, *Inside the rise of police department real-time crime centers*, MIT Technology Review, Apr. 19, 2021, https://perma.cc/HQ26-N4UV.

60 OODA Analyst, *Greek Police to Introduce Live Facial Recognition*, OODA Loop, Feb. 2, 2021, https://perma.cc/3T5B-HHYD.

61 Electronic Privacy Information Center, *EPIC Seeks Documents on Facial Recognition System Used to Identify D.C. Protester*, Electronic Privacy Information Center, Nov. 13, 2020, https://perma.cc/NZ4W-GH4L.

62 Jesse Marx, *supra* note 7.

63 Todd Feathers, *Baltimore Police Lied About Almost Every Aspect of Its Spy Plane Program*, Dec. 10, 2020, Motherboard Tech by VICE, https://perma.cc/B4B7-VWRN.

64 Suhauna Hussain & Johana Bhuiyan, *Police in Pasadena, Long Beach pledged not to send license plate data to ICE. They shared it anyway*, Los Angeles Times, Dec. 21, 2020, https://perma.cc/A38R-MYQT.

65 Michael Isaac Stein, *New Orleans PD Using Facial Recognition Despite Earlier Denials*, GovTech, Nov. 17, 2020, https://perma.cc/E6WJ-N9Z7.

66 Chad Marlow, *A Tale of Two Body Camera Videos*, American Civil Liberties Union, Dec. 23, 2020, https://perma.cc/6THC-6S6H.

67 The Surveillance Technology Oversight Project, *POST Act - Resources*, S.T.O.P. - The Surveillance Technology Oversight Project, Updated June 18th, 2020, https://perma.cc/W22J-TB5N.

Le fils de l'homme
Rene Magritte 1964

Panopticonism

Panopticonism, first proposed by English philosopher Jeremy Bentham in the 18th century and then criticized by French philosopher Michel Foucault in the 21st century, describes a system of control where prisoners don't know when they are being watched, and thus act as though they are being watched at all times. As "smart city" technology increases the ability to watch people, it enables panopticonism in three ways:

- It erodes privacy, autonomy, and freedom by increasing how often you are watched;
- It allows for unwarranted searches and seizures and permission-less experimentation; and
- It risks our security, not just from surveillance by the state or the state's corporate partners but via data breaches and foreign adversaries.

Eroding Privacy, Autonomy, & Freedom

As discussed, there are many ways "smart city" technology can create a genuine panopticon by being able to track you (via your identity) and your activity (via your movement and other data) at all times. Governments are currently expanding their cameras and identifying capabilities on the ground and in the air and obtaining mobility data without a warrant. This collection of identifying data is often done in the name of public safety. Still, there have not been many high-profile cases of this new collection bringing to bear the security promised. For example, U.S. Customs and Border Protection scanned more than 23 million people in public places with facial recognition technology in 2020 and caught zero imposters. Further, while these tools have not yet fulfilled their promise, much of the rhetoric about implementing "smart city" technology, such as creating "digital twins" of community members movement around the city for government analysis or "real-time crime centers," implies that a panopticon is the goal of these technologies. These goals should be categorically rejected.

This invasion of privacy effectively creates a loss of liberty, social detriment, and chills First Amendment rights.

2020-21 "Smart City" Examples:

- Globally, cities expanded their use of CCTV and aerial surveillance beyond unprecedented levels, such as China's 'Sharp Eyes' program, which aims to surveil 100% of public space,[68] Scotland's major Edinburgh upgrade,[69] and throughout India in Chhattisgarh,[70] Ludhiana,[71] Shimla,[72] Visakhapatnam,[73] and including Uttar Pradesh's expansive automated facial recognition cameras (AFRS),[74] and in Bhubaneswar where local news reported that police were "groping in dark" when a crime took place in a location with little CCTV installed.[75]
- Throughout the U.S., cities have expanded aerial camera surveillance, such as Baltimore's Aerial Investigative Research (AIR) program[76] and Chula Vista's drones with artificial intelligence.[77]
- Globally, cities are augmenting this camera footage with identifying tools such as advanced video analytics by more than 35 law

68 Dave Gershgorn, *China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space*, OneZero, https://perma.cc/33N8-NQ6D.

69 Global MSC Security, *The City Of Edinburgh Council Appoints Global MSC Security To Carry Out Major Upgrade Of Their Public Space Video Surveillance System*, Security Informed, 21 Jan. 21, 2021, https://perma.cc/68HZ-2LC8.

70 Avdhesh Mallick, *Chhattisgarh: Raipur traffic police collected Rs 1 cr through e-challans in 2020*, Free Press Journal, Jan. 20. 2021, https://perma.cc/KA7A-8Q5H.

71 Nikhil Bhardwaj, *Pvt CCTVs linked to police stations in Ludhiana*, Tribuneindia News Service, Dec. 16, 2020, https://perma.cc/4W8C-WSJ6.

72 Anu P. Lohumi, *60 CCTV cameras to check traffic violations in Shimla*, Tribune India News Service, Apr. 6, 2021, https://perma.cc/2QFH-VSZ4.

73 Nalla Babu, *Visakhapatnam cops warn of action against firms without CCTV cameras*, The Times of India, Jan. 25, 2021, https://perma.cc/2297-UDLG.

74 Varsha Rani, *Varanasi Is Using Crime Control as an Excuse for Facial Recognition Surveillance*, VICE, Nov. 27, 2020, https://perma.cc/7JV9-PAZQ.

75 Asish Mehta, *Inadequate CCTVs in Capital, cops grope in dark*, The New Indian Express, Jan. 24, 2021, https://perma.cc/CHE7-E2EU.

76 The Policing Project, *The Policing Project's audit of Baltimore's Aerial Investigation Research Progra*m, The Policing Project, Dec. 12, 2020, https://perma.cc/G4M4-HSLE.

77 Cade Metz, *Police Drones Are Starting to Think for Themselves*, The New York Times, Dec. 5, 2020, https://perma.cc/WN8L-Y76Y.

enforcement agencies in the US,[78] digital profiles in Russia,[79] and facial recognition technology in Buenos Aires,[80] Brasilia,[81] Como,[82] Gurugram,[83] South Orange, CA,[84] and Uruguay.[85] This high-risk technology has been used for civil case identification in Malaysia,[86] and toilet paper enforcement in Dongguan, China.[87] In addition, commercial facial recognition database tools like ClearviewAI (for law enforcement) and PimEyes (for the general public) make it possible to identify people based on images of their face without a warrant or their consent which opens up endless possibilities for abuse.

- Throughout the U.S., cities are collecting private-sector real-time mobility data via bike and scooter trip data Mobility Data Specification.[88]

- Throughout the U.S., many jurisdictions have begun codifying these intrusive searches, such as North Carolina's propose *Kelsey Smith Act* which allows law enforcement to obtain cell phone data without a warrant in an emergency,[89] and Florida's *Use of Drones by Government Agencies law*,[90] thereby reinforcing such activities.

78 Dave Maass & Matthew Guariglia, *Video Analytics User Manuals Are a Guide to Dystopia*, Electronic Frontier Foundation, Nov. 19, 2020, https://perma.cc/4NKK-K2DL.

79 Open Media, *Moscow City Hall seeks to expand 'digital profiles' of local residents through new monitoring system*, Meduza, Nov. 24, 2020, https://perma.cc/2VFE-Q56Q.

80 Verónica Arroyo, *Facial recognition in Latin America: Why civil society must fight back*, Access Now, Dec. 16, 2020, https://perma.cc/T6H7-AELD.

81 *Id.*

82 Laura Carrer, Riccardo Coluccini, & Philip Di Salvo, *Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale*, Wired.it, June 9, 2020, https://perma.cc/3QWD-ZKK5.

83 Ashok Kumar, *Gurugram's Millennium City gets smart eyes in the sky*, The Hindu, Jan. 3, 2021, https://perma.cc/TR2X-C7AK.

84 Daniel O'Connor, *SOPD to expand surveillance network, adding dozens of facial recognition cameras*, The Setonian, May 6, 2021, https://perma.cc/XH6H-ZEC3.

85 Verónica Arroyo, *supra* note 80.

86 Yuen Meikeng, *Facing off wrong-doers with more accuracy*, The Star, Jan 10, 2021, https://perma.cc/2EQL-RJY7.

87 Tracy Qu, *Facial recognition paused in public toilet amid mounting privacy concerns*, South China Morning Post, Dec. 6, 2020, https://perma.cc/D49Z-55B8.

88 Press Release, *EFF, ACLU File Lawsuit to Stop Los Angeles From Collecting Real-Time Tracking Data on Citizens' Rental Scooters*, Electronic Frontier Foundation, June 8, 2020, https://perma.cc/DZT8-RLYD.

89 Will Doran & Danielle Battaglia, *NC lawmakers want to give police even more power to track your phone without a warrant*, The News & Observer, Apr. 21, 2021, https://perma.cc/5H97-77NL.

90 Ch. 2021-165, Laws of Fla. (2021).

Allowing Unwarranted Searches & Seizures & Permission-less Experimentation

As "smart city" technology collects more and more identifying data, the ability to learn sensitive information by searching across these databases and joining these datasets also increases. The U.S. Constitution's Fourth Amendment provides a "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" by the government. New cases asserting Fourth Amendment search violations in the digital age have slowly been changing Fourth Amendment doctrine. In *Carpenter v. the United States*, the Supreme Court ruled that obtaining historical cell-site location information (CSLI) containing the physical locations of cell phones without a search warrant violated the Fourth Amendment. Before *Carpenter*, the government could obtain cell phone location records without a warrant. Since then, a series of Fourth Amendment cases have been brought to challenge the bounds of that ruling.[91] Without strict limits via the Fourth Amendment or other privacy regulations, cities are experimenting with new technologies to track individuals such as police robots.

2020-21 "Smart City" Examples:

- In *Leaders of Beautiful Struggle v. Baltimore Police Department,* the US Court of Appeals for the 4th Circuit held[92] that because the aerial surveillance program "enables police to deduce from the whole of individuals' movements … accessing its data is a search, and its warrantless operation violates the Fourth Amendment."[93] It was only after an amicus brief revealed the AIR program was not being truthful in its surveillance capabilities[94] this case was reheard.
- In *Sanchez v. Los Angeles,*[95] relying heavily on *Carpenter*, the American Civil Liberties Union (ACLU) and Electronic Frontier

91 United States of America v. Hammond, 3:18-cr-00005, No. 45 (N.D.Ind. Oct. 24, 2018))

92 Leaders of a Beautiful Struggle v. Baltimore Police Department, No. 20-1495 (4th Cir. 2021)

93 Tim Prudente, *Federal appeals court rebukes Baltimore spy plane program, likely blocks access to cache of remaining footage*, Baltimore Sun, June 25, 2021, https://perma.cc/BSE9-EZHR

94 Brief of The Policing Project as Amici Curiae In Support of Neither Party And In Support of Rehearing En Banc, Leaders of a Beautiful Struggle v. Baltimore Police Department, No. 20-1495 (4th Cir. 2021)

95 Justin Sanchez et al v. Los Angeles Department of Transportation et al, 2:20-cv-05044, No. 1 (C.D.Cal. Jun. 8, 2020)

Foundation (EFF) argued that the Los Angeles Department of Transportation's collection of bulk granular e-scooter data surmounted to an unreasonable search. The District Court dismissed the case for failure to state a claim not seeing the *Carpenter* connection. Since, ACLU and EFF have urged the U.S. Circuit Court of Appeals for the 9th Circuit to revive the challenge.

- In *Structural Sensor Surveillance,*[96] Andrew Ferguson examines the privacy risks of a future in which sensors are integrated and connected enough to track an individuals' movement across a city and argues that such a world would violate our Fourth Amendment protections and suggests preventative design interventions, such as less data, and less connectivity.
- Police robots like Boston Dynamics' "digidogs" and Knightscope's "rolling pickles" are being tested and deployed in cities to navigate and traverse the terrain, read license plates with infrared cameras, and identify cell phones within its range down to the MAC and IP addresses.[97]

Risking Security

As "smart city" technology collects more identifying data, the risk of individual and collective exploits of that data increases. A data breach could lead to identity theft, causing threats to one's safety and well-being or economic loss. Further, breachers can make collective utility grids vulnerable or governments vulnerable to hackers who may hold data hostage for ransom (also known as ransomware attacks), forcing governments to pay large sums of money to protect individual and national security.

96 Andrew Guthrie Ferguson, *Structural Sensor Surveillance*, Iowa Law Review, 106 Iowa L. Rev. 47, (2020).

97 Matthew Guariglia, *Police Robots Are Not a Selfie Opportunity, They're a Privacy Disaster Waiting to Happen*, Electronic Frontier Foundation, Jan. 7, 2021, https://perma.cc/6KSS-6JXR.

2020-21 "Smart City" Examples:

- In 20 U.S. cities, surveyed transit agency officials found that cybersecurity concerns and protocols were inadequate across organizations of all sizes.[98] Researchers at the University of California at Berkeley found that the "smart city" technologies most vulnerable to a cyberattack were emergency alert systems, street video surveillance, and some types of traffic signals. They recommended that leaders consider the significant disruption and negative consequences that would occur if these systems were hacked by bad actors and how that would affect community members.[99]

- Throughout the U.S., cameras, location trackers, and sensors attached to utilities have been breached during this last year. Cameras and associated biometric data have been breached by hackers inside of jails and hospitals, like Verkada's breach of more than 150,000 surveillance cameras,[100] by security bugs in and outside of people's homes, like Eufy's server glitch,[101] and held for ransom, like when the U.S. Customs and Border Protection's contractor Perceptics' had their pilot biometrics of travelers' faces held hostage on the dark web.[102] Location trackers have been breached with the hacking of social media applications like Parler disclosing location data.[103] Utility sensors have been breached, like the Colonial pipeline's ransomware attack,[104] the Tampa-area water utility hack,[105] and the potential hacking of "smart intersections."[106]

---

98 Skip Descant, *Transit Agencies Aren't Taking Cybersecurity Seriously Enough*, GovTech, Dec. 8, 2020, https://perma.cc/Z6TX-LE5J.

99 Karen Trapenberg Frick, et al., *The Cybersecurity Risks of Smart City Technologies: What Do The Experts Think?*, UC Berkley Center for Long-term Cybersecurity, Feb. 2021, https://perma.cc/D846-4CRN.

100 Dan Goodin, *Hackers access security cameras inside Cloudflare, jails, and hospitals*, Ars Technica, Mar. 3, 2021, https://perma.cc/EC6Z-M9XP.

101 Russell Brandom, *Server glitch allowed Eufy owners to see through other homes' cameras*, The Verge, May 17, 2021, https://perma.cc/98XX-PPG7.

102 Andrea Guzman, *The government wants to scan your face when you enter the US. It hasn't gone well so far.*, Mother Jones, Jan. 6, 2021, https://perma.cc/BRV6-H8UT.

103 Andy Greenberg, *An Absurdly Basic Bug Let Anyone Grab All of Parler's Dat*a, Wired, Jan. 12, 2021, https://perma.cc/TU2P-R9ZP.

104 Sean Hollister, *Colonial Pipeline reportedly paid the hackers nearly $5 million, despite suggestions to contrary*, The Verge, May 13, 2021, https://perma.cc/AV4Y-RU4P.

105 Samantha Schwartz, *Security flaws enabled Tampa-area water utility hack*, Smart Cities Dive, Feb. 12, 2021, https://perma.cc/S7CA-35T7.

106 Chris Teale, *Smart intersections may be prone to "congestion attacks,"* Smart Cities Dive, Mar. 8, 2018, https://perma.cc/JW46-EEF7.

Identifying data has been hacked and held for ransom including that of 22 police officers in D.C.[107] and an undisclosed amount of individuals' data in multiple cities during the pandemic.[108]

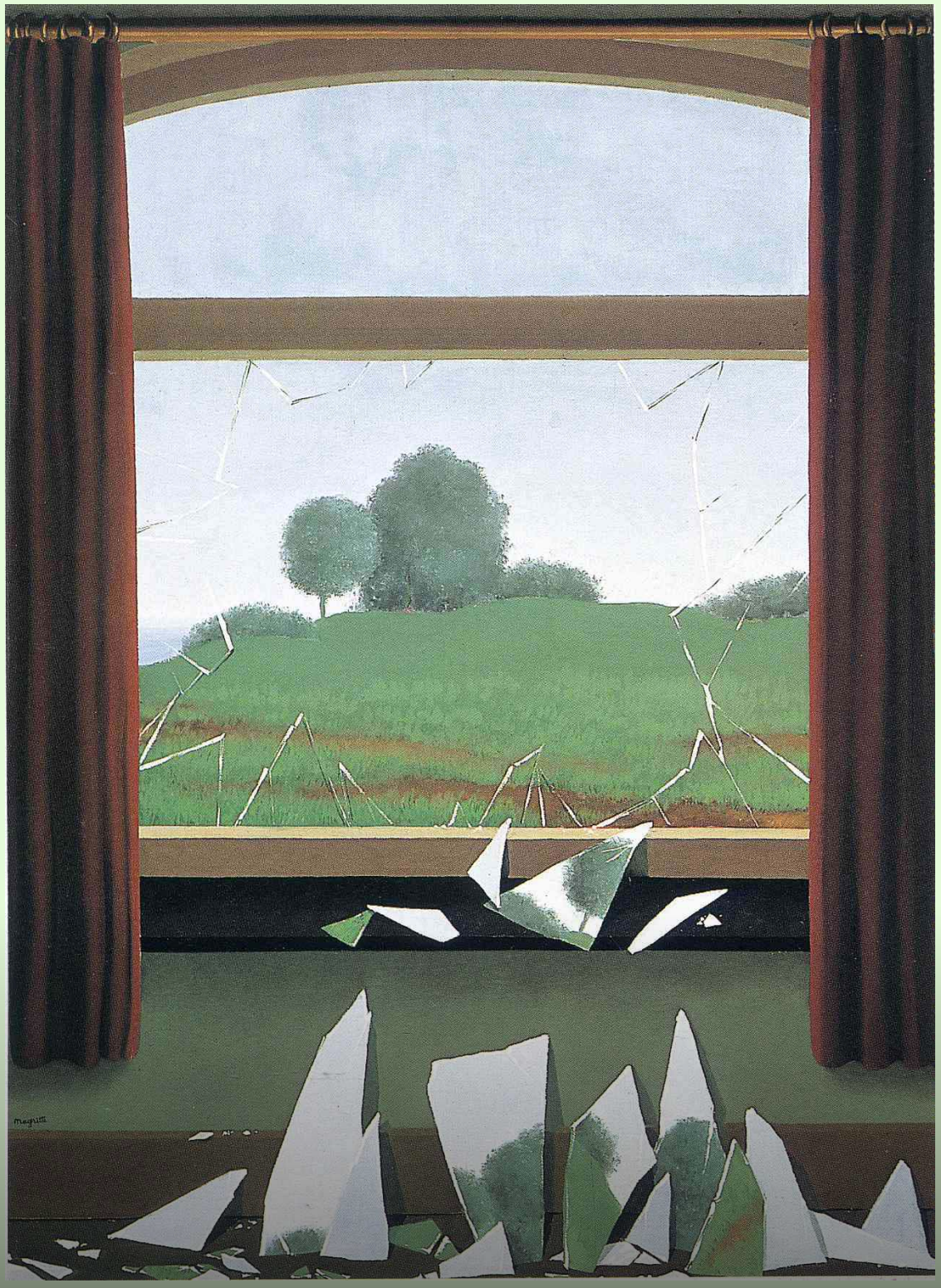
- Globally, i addition to cyberattacks by independent hackers, cybersecurity breaches of "smart city" technology have been linked to foreign adversaries. The *lawful use* of "smart city" technology provided by foreign companies has come under scrutiny for its ties to foreign espionage, such as several China-based technology companies with Chinese military ties[109] such as New York City's subway cameras.[110]

107 Kevin Collier, *Hackers release personal info of 22 D.C. police officers*, NBC News, May 11, 2021, https://perma.cc/J56J-KR62.

108 Chris Teale, *Cybersecurity risks spike as COVID-19 forces city staff to go remote*, Smart Cities Dive, Apr. 6, 2020, https://perma.cc/WY6X-TXJL.

109 Press Release, *List of Chinese Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021*, U.S. DEPARTMENT OF DEFENSE, June 3, 2021, https://perma.cc/2XS7-M3HM.

110 Adam Ismail, *NYC Ends Subway Camera Test After Learning Of Supplier's Link To Chinese Government, Facial Recognition Work*, Jalopnik, Apr. 26, 2021, https://perma.cc/6P4V-XXLA.



The Key to the Fields
Rene Magritte 1936

Discrimination

Discrimination is when a person is unable to enjoy their human rights on an equal basis with others because of an unjustified distinction made in policy, law, or treatment based on their race, ethnicity, nationality, class, caste, religion, belief, sex, gender, language, sexual orientation, gender identity, sex characteristics, age, health or another status.[111] In *Dark Matters: On the Surveillance of Blackness,* Simone Browne, traces back the over surveillance and "hypervisibility" of Black people to the "lantern laws" of the 17th and 18th century which required slaves to carry a lantern or candle if they were walking at night without a white owner to make them more visible and trackable. "Smart city" technology continues this trend of discriminatory surveillancein three ways:

- It targets historically discriminated against populations; and
- It deepens historical discriminatory practices already present in public administration and it makes certain groups more or less visible than others; and
- It provides (digital) services to some groups of people and not to others.

Targeting Discriminated Against Populations

As "smart city" technology continues to collect identifying data, including data related to gender, race, and religious affiliation, stewards of this data can target ethnic and religious minorities and other marginalized and oppressed communities for monitoring, analyzing, enforcement, imprisonment, torture, and in worst-case scenarios, genocide.

2020-21 "Smart City" Examples:

- In Xinjiang, China, the government has reportedly been forcing more than 1 million ethnic minority Uyghur people into labor

111 Amnesty International, *What drives discrimination and how do we stop it*?, Amnesty International (2021), https://perma.cc/F4J5-ZKHT.

camps. To support these efforts, China law enforcement are surveilling the Uyghur population with facial recognition technology that is designed to identify Uyghur individuals,[112] attempting to detect their emotions,[113] and surveilling their movements with the Integrated Joint Operations Platform which tracks their movement by monitoring the "trajectory" and location data of their phones, ID cards, and vehicles.[114] Technology companies such as Alibaba,[115] Dahua,[116] Huawei, Intel, Megvii, and Nvidia[117] were all scrutinized for their part in aiding this detection and surveillance.

- In the U.S., location and timestamp data from Muslim Prayer cell phone applications (Salaat First and Muslim Pro) via their embedded Software Development Kits (Telescope and X-Mode) managed by data brokers like Predico were procured by federal immigration law enforcement.[118]

- In Russia, the technology companies AxxonSoft, NtechLab, Tevian, and VisionLabs offer ethnicity analytics as part of the facial recognitional technology offerings to the Russian government, raising concerns by researchers that the country's law enforcement can track minorities.[119]

- In Lesbos, Greece, a range of experimental, rudimentary, and low-cost "smart city" technologies (drones, facial recognition, and LiDAR) were tested on refugees in camps first.[120]

---

112 Drew Harwell & Eva Dou, *Huawei tested AI software that could recognize Uighur minorities and alert police, report says*, Washington Post, Dec. 8, 2020, https://perma.cc/6PTM-4ZTK.

113 Jane Wakefield, *AI emotion-detection software tested on Uyghurs*, BBC News, May 26, 2021, https://perma.cc/FDZ3-AXNP.

114 Yael Grauer, *Millions of Leaked Police Files Detail Suffocating Surveillance of China's Uyghur Minority*, The Intercept, Jan. 29, 2021, https://perma.cc/636R-XUSV.

115 Raymond Zhong, *As China Tracked Muslims, Alibaba Showed Customers How They Could, Too*, The New York Times, Dec. 16, 2020, https://perma.cc/9RRW-M2WU.

116 Johana Bhuiyan, *Major camera company can sort people by race, alert police when it spots Uighurs*, Los Angeles Times, Feb. 9, 2021, https://perma.cc/A5UC-R7PT.

117 Drew Harwell & Eva Dou, *supra* note 112.

118 Joseph Cox, *Leaked Location Data Shows Another Muslim Prayer App Tracking Users*, Motherboard Tech by VICE, Jan. 11, 2021, https://perma.cc/7ECW-44PX.

119 Donald Maye, *Russian Face Rec Suppliers Offer Ethnicity Analytics, Raising Alarm*, IPVM , July 5, 2021, https://perma.cc/P4T7-AZDB.

120 Raphael Tsavkko Garcia, *How the Pandemic Turned Refugees Into 'Guinea Pigs' for Surveillance Tech*, OneZero, Jan. 21, 2021, https://perma.cc/8HNR-XZPY.

- In Lucknow, India, the decision to surveil women (rather than perpetrators) for signs of street harassment via facial recognition technology perpetuates patriarchal controls that limit the choices of women, and results in an intrusion of privacy and autonomy of women in public spaces, which is essential for women to exercise their freedom and political action fully. Further, emotion recognition has continually been proven ineffective across genders.[121]

Deepening Historic Discrimination & (In)visibility

In addition to aiding the targeting of particular groups of people, "smart city" technology can exacerbate current discriminatory practices by reinforcing the spatial inequities rife in urban planning, racial inequity in police technology[122], and extending those inequities to digital worlds, which is often referred to as "digital redlining."[123] These technologies can replicate inequity, exacerbate inequitable harms, mask inequity, transfer inequity, and compromise inequity oversight.[124] The result of facial recognition technology (which reads dark-skin and women's faces less accurately) being placed in predominantly Black and Latino neighborhoods results in compounded bias. Potential harms that flow from disproportionate use or disparate impact include loss of opportunities, economic loss, and social determinants.[125]

121 Anushka Jain, *How Facial Recognition Technology By the Police Perpetuates Patriarchal Norms*, Feminism In India, Apr. 16, 2021, https://perma.cc/WZ4C-RTMV.

122 Nick Cumming-Bruce, *U.N. Panel: Technology in Policing Can Reinforce Racial Bias*, The New York Times, Nov. 27, 2020, https://perma.cc/J5K2-SQ8V.

123 *Digital Redlining*, Wikipedia, Dec. 23 2020, https://perma.cc/3GWZ-U3R4.

124 Laura Moy, *A Taxonomy of Police Technology's Racial Inequity Problems*, Illinois Law Review, 2021 U. Ill. L. Rev. 139, (2021).

125 Grace Huckins, *For Marginalized Groups, Being Studied Can Be a Burden*, Wired, Jan. 6, 2021, https://perma.cc/U6RX-CXGP.

2020-21 "Smart City" Examples:

- In Argentina,[126] Brazil,[127] Detroit,[128] and Woodbridge,[129] facial recognition technology misidentifications have led to the wrongful arrests of innocent individuals resulting in distress, lost wages, the undermining of people's rights to due process and freedom of movement. The National Institute of Standards and Technology have found high rates of false positives in matching photos of Asians, African Americans, and Native groups,[130] and researchers Joy Buolamwini and Timnit Gebru found an error rate of less than 1 percent for light-skinned men but at least 20 percent for dark-skinned women.[131] Facial recognition technology's accuracy is continually improving[132] with new training data, including the ability to identify people with masks on,[133] which could help solve this harm, but in turn, only strengthen the discriminatory targeting examples above.
- In Chicago, 13-year-old Adam Toledo, was shot by the police after being alerted to the scene by a ShotSpotter, a gunfire detection system. Here, the system created an unacceptable risk of officers responding to perceived threats in Black and Latino neighborhoods with deadly force, which would have not otherwise occurred.[134]

126 Alejandra Hayon, *Seis días arrestado por un error del sistema de reconocimiento facial | La pesadilla de Guillermo Ibarrola, víctima del Gran Hermano porteño*, Pagina 12, Aug. 3, 2019, https://perma.cc/E3PD-52PB.

127 Bruna Fantti, *Reconhecimento facial falha e mulher é detida por engano,* O DIA, Oct. 7, 2019, https://perma.cc/4KUU-FP7G.

128 Drew Harwell, *Wrongfully arrested man sues Detroit police over false facial recognition match*, Washington Post, Apr.13, 2021, https://perma.cc/6FWK-KEVK.

129 Matt Bruce, *'Was It Malicious or Was It Lazy?': 3rd Black Man Arrested Based on 'Faulty Facial Recognition' Technology Files Federal Lawsuit Alleging Excessive Force, False Imprisonment,* Atlanta Black Star, May 11, 2021, https://perma.cc/C7EC-S6EW.

130 Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face recognition vendor test part 3:: demographic effects* NIST IR 8280 (2019), https://doi.org/10.6028/NIST.IR.8280.

131 Larry Hardesty, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, MIT News | Massachusetts Institute of Technology, Feb. 11, 2018, https://perma.cc/H8CP-PR4T.

132 Natasha Dailey, *New Facial-Recognition Technology Can Accurately Identify Travelers Wearing Masks 96% of the Time, According to a Test Run by the Department of Homeland Security*, Business Insider, Jan. 6, 2021, https://perma.cc/XHU9-56DN.

133 Sebastian Klovig Skelton, *Major Facial-Recognition Supplier Builds System to Identify Masked Faces*, Computer Weekly, Jan. 8, 2021, https://perma.cc/SWC2-AR9B.

134 Jamie Kalven, *Chicago Awaits Video of Police Killing of 13-Year-Old Boy*, The Intercept, Apr. 13, 2021, https://perma.cc/4CNW-ED9U.

Throughout the U.S., ShotSpotter is disproportionately deployed in Black neighborhoods.[135]

- Throughout the U.S., cities such as Baltimore and D.C.[136] have installed over two-and-a-half times more CCTV cameras in majority Black neighborhoods than in majority nonwhite areas. Cities with an above U.S.-average Black population are twice as likely to have a Police-Ring partnership surveilling your community.[137]
- Throughout the U.S., various cities have used "smart city" technology to surveil and enforce the poor. In Tampa, the city has installed CCTV outside of public housing units and Detroit has come under scrutiny by local activists for using facial recognition technology in public housing,[138] spurring the introduction of Federal legislation[139] to prohibit "the use of biometric recognition technology in certain federally assisted dwelling units." In parts of Florida, Louisiana, and Nevada, and throughout Oklahoma, roadway surveillance systems featuring ALPRs have been installed to bill uninsured drivers.[140]
- In Los Angeles, the act of looking up your information in predictive policing systems via ALPRs may increase your criminal risk score.[141]

135 Todd Feathers, *Gunshot-Detecting Tech Is Summoning Armed Police to Black Neighborhoods*, Motherboard Tech by VICE, July 19, 2021, https://perma.cc/P4NG-GNQ9.

136 Gracie Todd, *Police Cameras Disproportionately Surveil Nonwhite Areas of DC and Baltimore, CNS Finds*, CNS Maryland, Nov. 19 2020, https://perma.cc/WJ9J-AQAZ.

137 Jeremy Ney, *Surveillance and Inequality*, American Inequality, Mar. 31, 2021, https://perma.cc/GX6P-QGEH.

138 Lola Fadulu, *Facial Recognition Technology in Public Housing Prompts Backlash*, The New York Times, Sept. 24, 2019, https://perma.cc/36E3-LK39.

139 H.R.4008 - 116th Congress (2019-2020): No Biometric Barriers to Housing Act of 2019, H.R.4008, 116th Cong. (2019), https://perma.cc/GK6M-GG4S.

140 Ella Fassler, *Oklahoma Quietly Launched a Mass Surveillance Program to Track Uninsured Drivers*, OneZero, Apr. 7, 2021, https://perma.cc/6DFM-S4AF.

141 Sarah Brayne, Predict and Surveil: Data, Discretion, and the Future of Policing (2020).

Providing Unequal (Digital) Services

By contrast, there are instances where access to digital goods, including internet access,[142] have not been equally provided to historically marginalized communities.

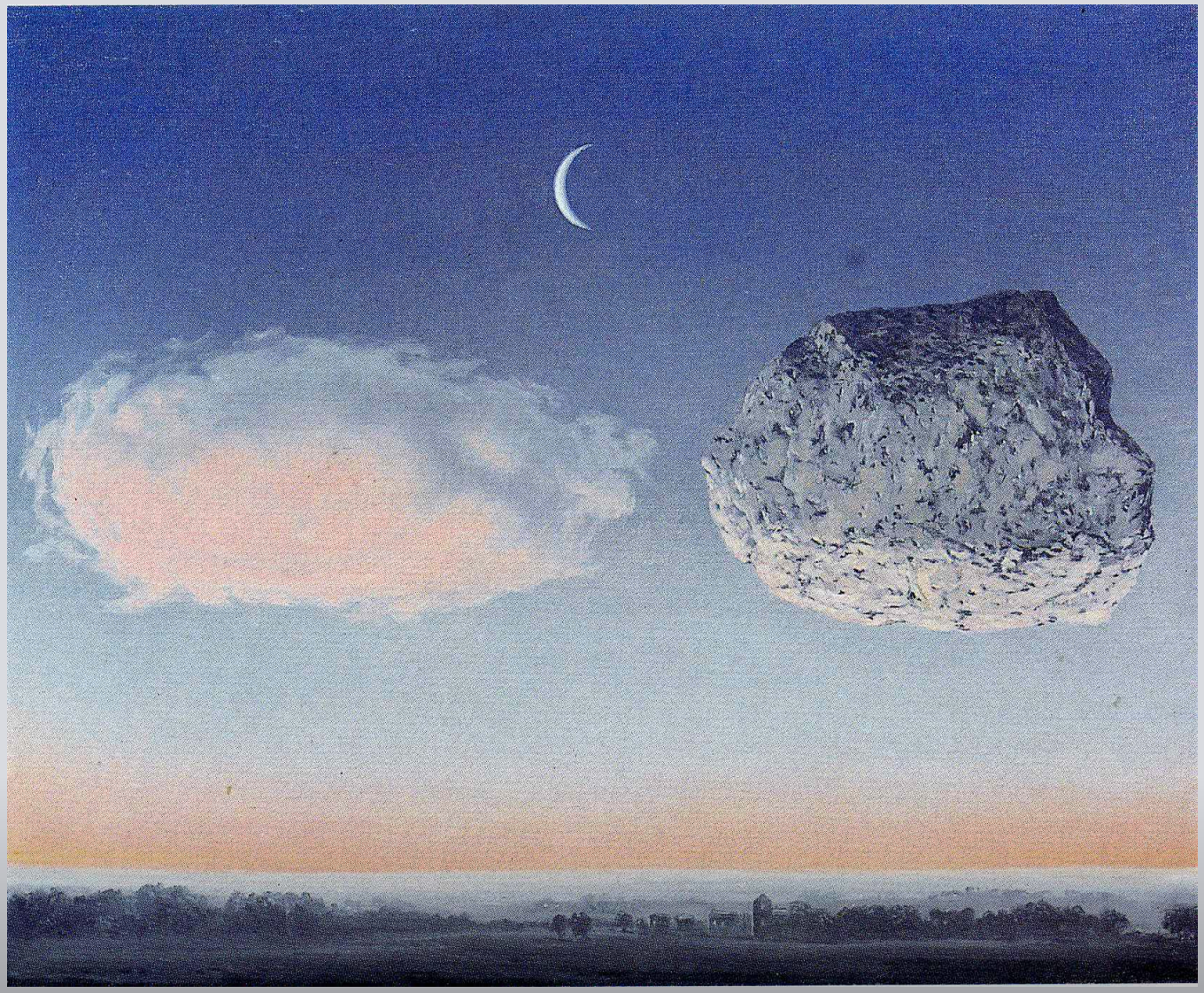
2020-21 "Smart City" Examples:

- In New York City, digital Wi-Fi kiosks were promoted as "a critical step toward a more equal, open, and connected city," by Mayor Bill de Blasio, but unevenly clustered in Manhattan and in its bordering neighborhoods where people did not need these services, but where the company behind LinkNYC, CityBridge, which relies on advertising revenue, to sell ads, with more impoverished areas having few or no kiosks.[143]
- In Thailand, residents in the deep south, primarily home to the Malay Muslim population, began reporting targeted mobile network shutdowns after residents were required to re-register their SIM cards through a new facial recognition system.[144]

142 Ernesto Falcon, *The FCC and States Must Ban Digital Redlining*, Electronic Frontier Foundation, Jan. 11, 2021, https://perma.cc/47FP-4KKB.

143 Annie Correal, *Just a Quarter of New York's Wi-Fi Kiosks Are Up. Guess Where.*, The New York Times, Dec. 6, 2019, https://perma.cc/QBS2-YKSB.

144 Civil Rights Defenders News, *Thailand's Facial Recognition Policy in the Deep South Raises Serious Human Rights Concerns,* Civil Rights Defenders, June 18, 2020, https://perma.cc/UZ6A-8L8K.



La bataille de l'Argonne

Rene Magritte 1959

Privatization

Privatization is the transfer of a public commodity or service to private ownership and control. For example, many companies offering "smart city" technology effectively privatize government infrastructure or services–either through government procurement or public-private partnership agreements–and often the land the infrastructure occupies. In addition to *replacing* public services, technology companies are also *displacing* public services, such as how the heavily venture-backed and unregulated Uber and Lyft rideshare services have shifted public transit use to rideshare services. These examples also collect proprietary data, which is often exclusively controlled by the technology companies, creating another, and perhaps the most powerful layer of privatization, the privatization of knowledge. "Smart city" technology ushers toward privatization in three ways:

- It replaces democracy with corporate decision-making; and
- It bypasses constitutional protections and accountability laws; and
- It expands surveillance monopolies.

Replacing Democracy With Corporate Decision-making

The privatization of city services by corporations replaces democratic decision-making with corporate profit-driven decision-making. By owning "the digital layer," companies can decide what information is collected and how it is used. When this data informs service delivery, it effectively controls how public services are delivered rather than voting, representation, or other democratic means. This phenomenon is particularly insidious for "smart city" technologies that offer "black box" AI as part of their toolset, where not only do they control the decision-making process, but it is not visible to community members. Lastly, these proprietary data systems can create lock-in and dependency on technology companies making it harder for governments to move away from this ownership and control.[145]

145 Eliska Drapalova & Kai Wegrich, *Who governs 4.0? Varieties of smart cities*, 22 Public Management Review 668–686 (2020), https://doi.org/10.1080/14719037.2020.1718191.

2020-21 "Smart City" Examples:

- In Nevada, Governor Steve Sisolak has proposed the legislature consider "Innovation Zones" that would create autonomous districts for private developers that own more than 50,000 acres of land (such as Blockchain, LLC) to take over responsibilities for tax collection, K-12 education, and other services. The proposal would allow companies to test out "revolutionary projects" and, in exchange, promise to invest up to $1 billion in the Zone and agree to an "innovative technology" tax.[146]
- In Toronto, Sidewalk Labs proposed[147] to collect data on energy, parking, telecommunication, transportation, and waste management with the intent of establishing markets for how these assets are accessed, priced,[148] and used until walking away from the project citing a weakened real estate market.
- Throughout the U.S., technology companies are affecting democratic decision-making directly by lobbying representatives, such as ClearviewAI lobbying against biometrics regulations,[149] various technology companies lobbying against state privacy laws,[150] and various data brokers[151] lobbying against data regulation bills like the *Artificial Intelligence in Government Act*,[152] *Artificial Intelligence Initiative Act*,[153] *Data Accountability and Trust Act*,[154] *Data Broker*

146 Riley Snyder & Michelle Rindels, *'Innovation Zones' promoted by Sisolak would create semi-autonomous county at behest of Blockchains LLC*, The Nevada Independent, Feb.3, 2021, https://perma.cc/NF84-TPM7.

147 Sidewalk Toronto, *Project update: Submitting the Digital Innovation Appendix*, Sidewalk Toronto, Nov. 5, 2019, https://perma.cc/8XVV-K8QS.

148 Bianca Wylie, *In Toronto, Google's Attempt to Privatize Government Fails—For Now*, Boston Review, May 13, 2021, https://perma.cc/LSJ9-5G86.

149 Chris Burt, *Clearview hires DC lobbyists to educate on face biometrics technology,* Biometric Update, May 11, 2021, https://perma.cc/8JVA-NSPN.

150 Todd Feathers, *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*, The Markup, Apr. 15, 2021, https://perma.cc/NK7F-DS4F.

151 Alfred Ng & Maddy Varner, *The Little-Known Data Broker Industry Is Spending Big Bucks Lobbying Congress*, The Markup, Apr. 1, 2021, https://perma.cc/EGN7-U6WS.

152 H.R.2575 - 116th Congress (2019-2020): AI in Government Act of 2020, H.R.2575, 116th Cong. (2020), https://perma.cc/7WRK-T7EH.

153 S.1558 - 116th Congress (2019-2020): AI–IA, S.1558, 116th Cong. (2019), https://perma.cc/Q7AM-QR4R.

154 H.R.1282 - 116th Congress (2019-2020): Data Accountability and Trust Act, H.R.1282, 116th Cong. (2019), https://perma.cc/RHX2-MVPZ

Accountability and Transparency Act,[155] and the *Information Transparency & Personal Data Control Act*.[156]

Bypassing Constitutional Protections & Accountability Laws

Many of our rights and accountability mechanisms disappear when "smart city" technology projects privatize public infrastructure and services. For example, the Fourth Amendment privacy protections of the US Constitution discussed earlier often do not apply to private-sector data collection due to the third-party doctrine. In many cases, this private sector data collection (usually attached to a transaction) is much more granular than would be allowable under privacy regulations like *Health Insurance Portability and Accountability Act (HIPAA)* or by an Institutional Review Board (IRB), which protects the rights and welfare of human research subjects. Also, where these companies are also purchasing land (Sidewalk Toronto, Amazon HQ, Under Armor's Port Covington project), these lands are converted to private ownership and are no longer protected by the First Amendment, which can prevent protest. Despite taking on quasi-government functions,[157] technology companies are not currently required to comply with the accountability measures built into government functions such as public records access, public audits, or consequences for elected officials if services do not meet community members' expectations.

2020-21 "Smart City" Examples:

- Throughout the U.S., governments have acquired private security camera footage (through programs like Amazon's Ring program[158]) and facial recognition services (through services like ClearviewAI) without a warrant. Further, government employees may be using these services without the knowledge of government leadership

155 H.R.6675 - 116th Congress (2019-2020): Data Broker Accountability and Transparency Act of 2020, H.R.6675, 116th Cong. (2020), https://perma.cc/T6KG-HFGY.

156 H.R.2013 - 116th Congress (2019-2020): Information Transparency & Personal Data Control Act, H.R.2013, 116th Cong. (2019), https://perma.cc/8TUX-6D8C.

157 Bianca Wylie, *The Critical Design Process of Democracy in Smart Cities*, ReSITE (2019), https://perma.cc/HC5H-LZXX.

158 Kim Lyons, *Amazon's Ring now reportedly partners with more than 2,000 US police and fire departments*, The Verge, Jan. 31, 2021, https://perma.cc/5RP4-F853.

or legislative approval. BuzzFeed News showcased this with audits of police department use of ClearviewAI,[159] and again with five federal law enforcement agencies use of ClearviewAI that was not discovered by the Government Accountability Office's audit.[160]

- Throughout the U.S., governments have acquired location data via cell phones (through application software X-Mode and Telescope[161] and data brokers like Acxiom, CoreLogic, and Epsilon that provide a wide range of consumer data[162]), vehicles (through services like Flock's TALON ALPR program[163] and iVe,[164] Otonomo,[165] The Ulysses Group's[166] vehicle data programs), and scooters (through data sharing agreements like the Mobility Data Specification[167]) without a warrant.

- Throughout the U.S., governments have acquired utility records (through services like Thomas Reuters CLEAR[168]) from private-sector data brokers without a warrant.

Expanding Surveillance Monopolies

As technology companies expand their "smart city" offerings, this creates risks that users will be tracked across multiple systems. As large technology companies with ample stores of personal data and their affiliates become more engaged with "smart city" projects, this becomes more worrisome.

159 Ryan Mac, et al. *How A Facial Recognition Tool Found Its Way Into Hundreds Of US Police Departments, Schools, And Taxpayer-Funded Organizations*, BuzzFeed News, Updated Apr. 9, 2021, https://perma.cc/KV4N-KP27.

160 Caroline Haskins & Ryan Mac, *A Government Watchdog May Have Missed Clearview AI Use By Five Federal Agencies In A New Report*, BuzzFeed News, June 30, 2021, https://perma.cc/TW7K-7K4U.

161 Joseph Cox, *supra* note 118.

162 Justin Sherman, *Data Brokers Are a Threat to Democracy*, Wired, Apr. 13, 2021, https://perma.cc/ZZD8-PX32.

163 Joseph Cox, *Inside 'TALON,' the Nationwide Network of AI-Enabled Surveillance Cameras*, Motherboard Tech by VICE, Mar. 3, 2021, https://perma.cc/T98M-RUZ4.

164 Sam Biddle, *Your Car Is Spying on You, and a CBP Contract Shows the Risks*, The Intercept, May 3, 2021, https://perma.cc/3MFX-SW23.

165 Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go*", Motherboard Tech by VICE, June 10, 2021, https://perma.cc/4Y7R-R72M.

166 Joseph Cox, *Cars Have Your Location. This Spy Firm Wants to Sell It to the U.S. Military*, Motherboard Tech by VICE, Mar. 17, 2021, https://perma.cc/J5MV-XXH9.

167 Open Mobility Foundation, *About MDS,* Open Mobility Foundation (2021), https://perma.cc/PJ5A-HEDQ/.

168 Drew Harwell, *ICE investigators used a private utility database covering millions to pursue immigration violations,* Washington Post, Feb. 26, 2021, https://perma.cc/WG7J-9N2V.

At what point does a single corporation have "vertical integration" (in terms of identifying data) of a whole neighborhood? If a single technology company captures government technology markets, it will also effectively control the design, access, and availability of many different kinds of surveillance technologies. For example, a company that achieves platform dominance in policing would not only reap economic benefits, but would also gain enormous power over functions essential to issues of democratic policing."[169]

2020-21 "Smart City" Examples:

- In Chongqing, BIG and Terminus discussed plans for the "smart city" project named Cloud Valley aimed to collect data via sensors and devices to "help people live more comfortably by monitoring their habits and anticipating their needs" and explicitly striving to achieve enough personal data so that when customers walked into a bar, the bartender would know their favorite drink.[170]
- Throughout the U.S., large technology companies are becoming more engaged with "smart city" projects, including Google's affiliates involvement with CityBridge in New York City, Sidewalk Labs in Toronto, and Replica in Oregon and Amazon's Ring partnership with law enforcement, and their recent launch of Amazon Sidewalk, a mesh network for Amazon products expanding IoT connectivity.

169 Elizabeth E. Joh & Thomas Wuil Joo, *The Harms of Police Surveillance Technology Monopolies*, Denver Law Review Forum, Forthcoming, Apr. 26, 2021, https://papers.ssrn.com/abstract=3834777.

170 Postmedia News, '*I know your favourite drink': Chinese smart city plans to put AI in charge*, Toronto Sun, Dec. 4, 2020, https://perma.cc/H8NZ-REMR.

Hegel's Holiday

Rene Magritte 1958

Solutionism

Technological "solutionism," coined by Evgeny Morozov in 2014, refers to the phenomenon of trying to reframe political, moral, and irresolvable problems as solvable by quantifying, tracking, or gamifying behavior with technology. In, *The Smart Enough City*, Ben Green builds on this concept describing the "tech goggles" perspective as:

> At their core, tech goggles are grounded in two beliefs: first, that technology provides neutral and optimal solutions to social problems, and second, that technology is the primary mechanism of social change. Obscuring all barriers stemming from social and political dynamics, they cause whoever wears them to perceive every ailment of urban life as a technology problem and to selectively diagnose only issues that technology can solve. People wearing tech goggles thus perceive urban challenges related to topics such as civic engagement, urban design, and criminal justice as being the result of inefficiencies that technology can ameliorate, and they believe that the solution to every issue is to become "smart"—internet-connected, data-driven, and informed by algorithms—all in the name of efficiency and convenience. Seeing technology as the primary variable that can or should be altered, technophiles overlook other goals, such as reforming policy and shifting political power. The fundamental problem with tech goggles is that neat solutions to complex social issues are rarely, if ever, possible. The urban designers Horst Rittel and Melvin Webber describe urban social issues as "wicked problems," so complex and devoid of value-free, true-false answers that "it makes no sense to talk about optimal solutions.[171]

"Smart city" technology is and reinforces solutionism in three ways:

- It is deployed with little or no evidence that it is effective at solving the problem at hand and no examination of what risk it creates; and

171 Ben Green, The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future (2019), https://doi.org/10.7551/mitpress/11555.001.0001.

- It takes budgets away from providing material goods and services to community members to collect more data instead; and
- It creates the need for more technology and thus more solutionism.

Deploying Without Proven Efficacy Or Risk Analyses

"Smart city" technology is steeped in solutionism, and its rhetoric and promotional materials are often couched in the promise of what it could solve rather than what it has demonstrably solved in similar instances. "Smart city" sales pitches argue that with more data collection, processes can inherently be made more efficient and thus solved. These claims don't take into consideration failures in models or theories of change or the many externalities that impact a city.

2020-21 "Smart City" Examples:

- In Mexico City, their extensive C5 CCTV video surveillance system has failed to meet the promise of crime prevention in several ways, including corrupt police using the footage as leverage rather than encroachment, it does not deter violent crimes, and while it may have an effect on larceny, it disproportionately affects the poor while not capturing white-collar crimes.[172]
- Technology companies themselves have struggled to hone in a business model with Cisco–one of the first companies to use the "smart city" term–announcing in 2020 that it would stop providing its Kinetic for Cities software platform because "cash-strapped" cities were opting for solutions for "specific use cases."[173]

172 Madeleine Wattenbarger, *Where surveillance cameras work, but the justice system doesn't*, Rest of World, Jan. 19, 2021, https://perma.cc/87QK-3HZG.

173 Kristin Musulin, *Cisco explains its smart city software exit*, Smart Cities Dive, Jan. 15, 2021, https://perma.cc/6XUZ-KKRJ.

Taking Resources Away From Providing for People's Material Needs

Procuring technology and data collection systems is expensive and costly to obtain, manage, secure, and upgrade. While data can help you identify problems you were unaware of or hone in on efficiencies, these efficiencies can be dwarfed by the costs to collect more data. For example, with better traffic data collection, cities would still need policy interventions like congestion pricing or infrastructure interventions like new thruways or medians to reduce congestion or accidents; the data only helps to outline the problem, which the community is likely already aware of.

2020-21 "Smart City" Examples:

- In Utah, the state spent $20.7 million dollars on a five-year contract with Banjo, an AI surveillance company that promised to analyze traffic cameras, CCTV cameras, social media, 911 emergency systems, and location data in real-time and to create a "solution for homelessness" and to detect "opioid events" using its Live Time software that review by a state auditor was found not to have any AI capabilities.[174]
- Globally, during the COVID-19 pandemic, many cities invested in surveillance technologies such as heat mapping, face-mask detection, and artificial intelligence to monitor the capacity of its light rail system in New Jersey,[175] AI cameras in Peachtree Corners,[176] CCTV to detect crowds in the UK,[177] contact-tracing applications in many countries.[178] Thorough out the U.S., law enforcement agencies used *Federal Coronavirus Aid, Relief, and Economic Security Act (CARES) Act* grants to purchase encrypted

174 Jason Koebler & Joseph Cox, *Utah Gave $20 Million Contract to AI Surveillance Firm That Didn't Have AI*, Motherboard Tech by VICE, Mar. 30, 2021, https://perma.cc/TA8T-Q74R.

175 Ryan Johnston, *NJ Transit will test AI-powered face-mask detection*, StateScoop, Jan. 25, 2021, https://perma.cc/G3LJ-JF2C.

176 Peachtree Corners, *Smart City Peachtree Corners Deploys Cawamo's Industry-First AI Camera Tech For COVID-19 Safety and Security*, PRNewswire, Jan. 15, 2021, https://perma.cc/EAM6-JY29.

177 Brandon Vigliarolo, *New AI software can turn regular security cameras into COVID-19 policy enforcement points*, TechRepublic, Jan. 19, 2021, https://perma.cc/8YLE-WDLW.

178 Bobbie Johnson, *Some prominent exposure apps are slowly rolling back freedoms*, MIT Technology Review, Nov. 23, 2020, https://perma.cc/96M5-93XC.

radios, body cameras, and communications upgrades.[179] These surveillance technologies were prioritized while non-surveillance technology solutions such as testing, masks, and financial assistance were under-resourced in these same communities.

Technology Begets More Technology

Finally, the use of "smart city" technology encourages and in fact requires the use of more technology. For example, many cities are investing in the infrastructure needed for 5G upgrades currently and being sold technologies to run off such a network. Similarly, cities procure one piece of technology and end up being offered add-ons, plug-ins, or enterprise services that can seem like a deal, but lock in cities to specific vendors via proprietary data and software investment and create an environment where the city must stay with that vendor because transferring vendors would result in high-costs of data transformation.

2020-21 "Smart City" Examples:

- In Oklahoma, companies like Rekor One are converting regular cameras into ALPRs.[180]
- In San Diego, their smart streetlights program (which came under scrutiny for filming protestors) had issues with over a million dollars in overrun costs due to a lack of oversight and separate fees for LED lighting and for the sensors to collect data and shoot video. [181]

179 Charlie McGee, *Blue Bailout: Covid-19 Cash Is Militarizing Cops Across the Country*, Rolling Stone, May 5, 2021, https://perma.cc/5FRJ-HANX.

180 Ella Fassler, *supra* note 140.

181 Dorian Hargrove, et al, Memo Reveals Huge Cost Overruns For San Diego's 'Smart Streetlights', NBC 7 San Diego, Feb. 15, 2020, https://perma.cc/R2NQ-Y7PV.

The discovery of fire

Rene Magritte 1935

10 Calls to Action to Protect & Promote Democracy

While the last year has provided many cautionary trends, it has also begun to outline paths forward to prevent these harms, and more importantly, ways to think differently about how technology influences and affects our broader political goals. To protect and promote democracy, I believe we must issue regulations that immediately blunt the ability to execute these cautionary trend harms but also build capacity for evaluating how technology affects society, and fortify our democratic spaces with technology in mind.

To do so, we will need digital advocates to integrate into more substantive political advocacy movements that relate to the material needs of communities, legislatures to move beyond oversight and restore eroding rights and create new rights, and technology companies to rely on business models that do not create these harmful data markets and risks.

Below I outline 10 calls to action to protect and promote democracy based on current intervention strategies being deployed and leading theory in this space. While the cautionary trends included global examples, these calls to action are outlined with the current U.S. legal framework and regulations in mind. In addition to current intervention examples to build from, I have included resources and communities to build with. My hope is like the cautionary trends section of this report, is that these calls to action serve as a time capsule of the current policy options in 2020-21, but that these options expand and change through these communities and further global examples.

Stop Harmful "Smart City" Technology, Data, and Uses

1. Strictly Limit Law Enforcement Access to Identifying Data

To stop harmful "smart city" technology, data, and uses, we must prohibit the current mission creep of "smart city" technologies being available for dragnet searches by police without strict limits. To do this, we must examine how our current legal frameworks can be reinforced to consider these new risks, and where those frameworks are insufficient how we can fill those gaps with policies and practices that properly address these new risks.

Current interventions that should be expanded to limit law enforcement access to identifying data include Fourth Amendment litigation and scholarship, regulation, whistle-blowing, audits by third parties, and corporate transparency reports. To meaningfully preserve the privacy protections formerly available under the Fourth Amendment, advocates and legal scholars must continue to articulate how tracking technologies create the ability to conduct dragnet searches akin to cell-phones in *Carpenter* and, with the degree of government and private-sector entanglement currently present in society, narrow the third-party doctrine exception to meet that reality. Outcomes like the recent Leaders of Beautiful Struggle v. Baltimore Police Department holding[182] are encouraging examples of how new data collection technology capabilities have changed what is acceptable under past tactics. Advocates should bring all cases in violation of unreasonable searches with a warrant, but be especially mindful of opportunities to litigate the unwarranted tracking of individuals via cameras, location trackers (from phones to vehicles), and sensors because of their widespread application. Beyond Fourth Amendment litigation, legislatures must begin regulating the use of the privacy invasive tools by law enforcement, such as surveillance technology oversight laws and data sharing regulations Massachusetts' recent law[183] that prevents transit authorities from disclosing personal information related to individuals' transit system use for

182 Leaders of a Beautiful Struggle v. Baltimore Police Department, No. 20-1495 (4th Cir. 2021)

183 An Act Authorizing and Accelerating Transportation Investment. 2020 Mass. Acts Chapter 383.

non-transit purposes. The recent introduction of the *Fourth Amendment is Not for Sale Act*, which requires the government to get a court order to compel data brokers to disclose data,[184] and the *Cell-Site Simulator Warrant Act*, which establishes a probable cause warrant requirement for federal, state, and local law enforcement agencies to use a cell-site simulator[185] are also encouraging. Digital advocates and investigative journalists must continue to investigate how law enforcement is obtaining identifying data from companies and using surveillance technology unbeknownst to the public and legislative representatives. Projects like BuzzFeed News' *Surveillance Nation* that showcase which law enforcement agencies have used ClearviewAI and The Policing Project's evaluation of the Baltimore spy plane are critical facts needed to effectively develop policy that will prevent these harms. Similarly, technology companies should produce transparency reports of when law enforcement have requested identifying data from them as Amazon Ring has begun to do.

To support interventions like these in your community, discuss the examples listed above with your local community groups and local representatives. To consider more deeply about how surveillance technology and capitalism enable wholesale criminalization, check out Action Center on Race and the Economy's *21st Century Policing: The RISE and REACH of Surveillance Technology*[186] and STOP LAPD Spying Coalition's *The Algorithmic Ecology: An Abolitionist Tool for Organizing Against Algorithms.*[187]

2. End High-tech Profiling

To stop harmful "smart city" technology, data, and uses, we must also ensure that identifying data is not used to track, sort, or otherwise endanger certain groups of people. This includes explicit tracking of individuals

184 S.1265 - 117th Congress (2021-2022): Fourth Amendment Is Not For Sale Act, S.1265, 117th Cong. (2021), https://perma.cc/6MPE-9UM3.

185 S.2122 - 117th Congress (2021-2022): Cell-Site Simulator Warrant Act of 2021, S.2122, 117th Cong. (2021), https://perma.cc/3DR6-3GY5.

186 Action Center on Race and the Economy and The Community Resource Hub for Safety and Accountability, *21st Century Policing: The RISE and REACH of Surveillance Technology*, Action Center on Race and the Economy, Apr. 19, 2021, https://perma.cc/32KK-2SGE.

187 STOP LAPD Spying Coalition and the Free Radicals, *The Algorithmic Ecology: An Abolitionist Tool for Organizing Against Algorithms*, STOP LAPD Spying, Mar. 2, 2020, https://perma.cc/DLJ2-S53G.

of certain groups, such as being done with the Uyghur population in Xinjiang for their "correction" or with women in Lucknow for their "protection" and the implicit tracking of certain types of individuals by tracking Muslim regions or self-reinforcing predictive-policing searches. To be clear, there are many scenarios where the collection of demographic information can be in service to justice, such as when it proves unequal treatment, but unconsented continual tracking in our public streets without people's consent is not one of them given the documented risks. Further, governments should be obligated to continually evaluate whether these technologies have a discriminatory effect.

Current interventions that should be expanded to end high-tech profiling include indictments and sanctions for human rights violations, regulation, equity impact assessments, responsible data practices, audits, and corporate refusal to sell to governments for these purposes. Amnesty International has articulated facial recognition technology's human rights violations and called for it to be banned.[188] The Paris Judicial Court's Crimes Against Humanity and War Crimes unit has indicted senior executives at Nexa Technology for the company's sale of surveillance software over the last decade led to authoritarian regimes in Libya and Egypt that resulted in the torture and disappearance of dissidents and other human rights abuses[189] and the U.S. Department of Commerce sanctioned 14 Chinese technology companies over links to human rights abuses against Uyghur Muslims in Xinjiang, including DeepGlin who is backed by a top Silicon Valley investment firm.[190] Legislatures like Washington's have included anti-discriminatory measures in their proposed *People's Privacy Act* protecting those who fail to opt-in[191] and Seattle's surveillance technology law requires Equity Impact Assessments be conducted for all surveillance technologies as part of their oversight requirements.[192] The calls for the EU to ban the use of AI in facial recognition technology that detects gender or sexuality

188 Amnesty International and partners, *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance*, Amnesty International, June 7, 2021, https://perma.cc/NK5H-4UH2.

189 Patrick Howell O'Neill, *French spyware bosses indicted for their role in the torture of dissidents*, MIT Technology Review, June 22, 2021, https://perma.cc/MJ9V-D8YK.

190 Dave Gershgorn, *US sanctions a Chinese facial recognition company with Silicon Valley funding*, The Verge, July 9, 2021, https://perma.cc/97MX-SVPT.

191 David Stauss, *People's Privacy Act Introduced In Washington State House Of Representatives*, JD Supra, Feb. 1, 2021, https://perma.cc/3MGN-72XD.

192 Rebecca Williams, *supra* note 23.

or credit scores have also been encouraging. Public scrutiny and campaigns by civil rights organizations[193] have successfully influenced companies like Amazon, IBM, and Microsoft[194] to put a moratorium on facial recognition technology to governments, Huawei to backtrack a patent application they filed for a facial recognition system meant to identify Uyghur people[195] and technology companies like Alibaba[196] to disavow the use of their technology for targeting of ethnic groups.

To support interventions like these in your community, discuss the examples listed above with your local community groups and local representatives. To consider more deeply how these tools can be expanded, check out the *Civil Rights, Privacy and Technology Table*, led by a coalition of civil and digital rights advocacy groups,[197] Laura Moy's *A Taxonomy of Police Technology's Racial Inequity Problems* article that features equity impact assessment application strategies,[198] Data 4 Black Lives' call for *#NoMoreDataWeapons*[199] and the Urban Institute's *Five Ethical Risks to Consider before Filling Missing Race and Ethnicity Data*[200] and *Creating Equitable Technology Programs A Guide for Cities.*[201]

3. Minimize the Collection & Use of Identifying Data Everywhere

To stop harmful "smart city" technology, data, and uses, we must specifically protect people from being monitored and targeted, which means we

193 Karen Hao, *Amazon is the invisible backbone of ICE's immigration crackdown*, MIT Technology Review, Oct. 22, 2018, https://perma.cc/33YJ-NGA7.

194 Karen Hao, *The two-year fight to stop Amazon from selling face recognition to the police*, MIT Technology Review, June 12, 2020, https://perma.cc/Z5NX-U2DR.

195 ANI, *China's Huawei backtracks after filing for patent to identify Uyghurs*, Business Standard India, January 15, 2021, https://perma.cc/HU3T-QTN3.

196 Benzinga, *Alibaba 'Dismayed' Over Ethnic Profiling in Facial Recognition Technology*, CFO, Dec. 18, 2020, https://perma.cc/N8PM-7TRC.

197 American Civil Liberties Union, et al., *Principles*, Civil Rights Privacy and Technology Table (2020), https://perma.cc/4RDM-LUJH.

198 Laura Moy, *supra* note 124,

199 Jamelle Watson-Daniels, Introducing #NoMoreDataWeapons, Data for Black Lives Blog, Feb. 26, 2021, https://perma.cc/46VT-T3JV.

200 Megan Randall, Alena Stern, & Yipeng Su, *Five Ethical Risks to Consider before Filling Missing Race and Ethnicity Data*, Urban Institute, Mar. 2021, https://perma.cc/9KPU-9ZQ6.

201 Alena Stern, Graham MacDonald, & Khuloud Odeh. Creating Equitable Technology Programs: A Guide for Cities, Urban Institute, Sept. 2020, https://perma.cc/YF9S-WX48.

must collectively think more carefully about how to minimize the creation of identifying data that can be abused. In addition to strictly limiting access to identifying data by law enforcement and ending high-tech profiling, we must also reduce the attack surface of potential abuses by law enforcement, corporations, and nefarious actors, by minimizing the collection of identifying data everywhere, full stop. To address this, we must explore policies that consider minimizing the creation, storage, and standardization of identifying data and regulate its use. Given the entanglement of private-sector and government surveillance, including governments growing dependence on data brokers,[202] to be successful, these policies must consider both the public and private sectors' roles in creating, managing, and using identifying data.

Current interventions that should be expanded to minimize the collection and use of identifying data everywhere include data privacy regulations, audits of misuses, demonstrations of security and other risks, and the use of methods that collect less harmful identifying data. In terms of data regulation, legislatures have begun regulating identifying technology, identifying data, and specific uses of the data, including:

- **Technology:** Legislatures have begun to regulate the government's use of facial recognition technology in 20 cities and counties, including Boston, Cambridge, Easthampton, Jackson, King County, WA, Madison, Minneapolis, New Orleans, Portland, ME, and Portland OR, Santa Cruz, and Teaneck, during this past year.[203] The calls for the banning of government use of facial recognition technology have steadily increased with a more significant push by 70 grassroots groups in June 2021 for Congress to pass a nationwide prohibition on biometric surveillance.[204] Congress has recently introduced the *Facial Recognition and Biometric Technology Moratorium Act of 2021,*[205] and the House Judicial Committee recently held a hearing on *Facial Recognition*

202 Justin Sherman, *supra* note 162.

203 Jameson Spivack & Clare Garvie, *supra* note 22.

204 Nicole Ozer, Kate Ruane, & Matt Cagle, *Grassroots Activists are Leading the Fight to Stop Face Recognition. It's Time for Congress to Step Up, Too.*, American Civil Liberties Union , June 17, 2021, https://perma.cc/V5FB-KFYB.

205 S.2052 - 117th Congress (2021-2022): Facial Recognition and Biometric Technology Moratorium Act of 2021, S.2052, 117th Cong. (2021), https://perma.cc/F5G9-6PZE.

Technology: Examining Its Use by Law Enforcement. Further, New York City and Oregon have regulated the use of facial recognition technology by private entities. Local legislatures have also begun to regulate ALPRs,[206] and surveillance technology broadly.[207] Congress has introduced legislation to require a warrant with the *Cell Site Simulator Warrant Act*.[208]

- **Data:** In terms of regulating the collection of certain types of identifying data, legislatures have begun regulating the collection of biometrics data,[209] such as Portland, OR[210]and New York City,[211] and consumer data privacy,[212] such as Virginia, and Colorado[213] this year. Congress has proposed regulation of data brokers with *The Fourth Amendment is Not For Sale Act,*[214] data privacy broadly with the *Data Protection Act*[215] and passed legislation that calls for the development of security standards for all IoT devices with the *IoT Cybersecurity Improvement Act*.[216]

- **Uses:** Lastly, legislatures have regulated *the use* of identifying data by prohibiting the use of facial recognition databases[217] or the secondary use of identifying data as with Massachusetts' transit data.[218]

Some highlights of these regulations that should be expanded include the requirement of third-party review in their surveillance technology

206 Dave Maass & Hayley Tsukayama, *EFF Joins Effort to Restrict Automated License Plate Readers in California*, Electronic Frontier Foundation, Mar. 19, 2021, https://perma.cc/MMN5-DGVA.

207 Rebecca Williams, *supra* note 23.

208 S.2122 - 117th Congress (2021-2022): Cell-Site Simulator Warrant Act of 2021, S.2122, 117th Cong. (2021), https://perma.cc/3DR6-3GY5.

209 Epiq, *supra* note 24.

210 Taylor Hatmaker, *Portland passes expansive city ban on facial recognition tech*, TechCrunch, Sept. 9, 2020, https://perma.cc/8LZ8-QSDL.

211 Zack Whittaker, *New York City's new biometrics privacy law takes effect,* TechCrunch, July 9, 2021, https://perma.cc/UZ8F-JMK6.

212 Pam Greenberg, *2020 Consumer Data Privacy Legislation*, National Conference of State Legislatures, Jan. 17, 2021, https://perma.cc/3MEM-AUAP.

213 Aaron Nicodemus, *Colorado third state to enact comprehensive privacy law*, Compliance Week, July 8, 202, https://perma.cc/N7YG-CB57.

214 S.1265 - 117th Congress (2021-2022): Fourth Amendment Is Not For Sale Act, S.1265, 117th Cong. (2021), https://perma.cc/6MPE-9UM3.

215 S.2134 - 117th Congress (2021-2022): Data Protection Act of 2021, S.2134, 117th Cong. (2021), https://perma.cc/UGF9-48PY.

216 Internet of Things Cybersecurity Improvement Act of 2020, 15 U.S. Code § sections 278g–3a to 278g–3e.

217 Office of the Privacy Commissioner of Canada, *supra* note 27.

218 An Act Authorizing and Accelerating Transportation Investment. 2020 Mass. Acts Chapter 383.

regulations,[219] and governments expanding their commitment to evaluate data rights issues with full-time staff and governance bodies dedicated to these issues such as Privacy Officials, Commissions, and Advisory Bodies.

Absent new regulation, there has been consumer protection litigation related to the use of facial recognition technology, such as when the Federal Trade Commission filed a complaint that Everalbum had deceived consumers about the use of facial recognition technology and their retention of images of users who had deactivated their accounts,[220] protective privacy policies[221] and standard contractual clauses related to data rights, such as those offered by Johns Hopkins' Center for Government Excellence to ensure data is retained by governments as open data[222] and those adopted by the EU to govern exchanges and international transfers of personal data.[223] There have also been calls for minimizing data-sharing agreements across government agencies, such as when the Electronic Privacy Information Center (EPIC) urged a comprehensive review of DHS's Information Sharing Access Agreements.[224]

In addition to refusing to sell identifying tools to police, technology companies are developing new methods and strategies to reduce the amount of identifying data that is created. Technology companies are creating tools to minimize the identifying capacity of images such as image altering tools (like Fawkes, which image cloaks by subtly changing pixels, or Everest Pipkin, which strips images of identifying metadata, or Anonymizer, CycleGAN, and Deep Privacy, which use GAN escape detection to create fake derivative images that look similar to the naked eye), camera applications (like Anonymous Camera, which blurs and pixelates images and strips images of identifying metadata), and video anonymization

219 Rebecca Williams, *supra* note 23.

220 Press Release, *California Company Settles FTC Allegations It Deceived Consumers about use of Facial Recognition in Photo Storage App*, Federal Trade Commission, Jan. 11, 2021, https://perma.cc/K2VJ-FRT8.

221 *Intersection,* LinkNYC, https://perma.cc/AJM8-FK52.

222 GovEx, *Data Ownership and Usage Terms for Government Contracts,* GovEx Labs, https://perma.cc/64KZ-BKG8.

223 Sheila A. Miller & Tracy P. Marshall, *EU Adopts New Standard Contractual Clauses For Transfers of Personal Data*, The National Law Review, July 7, 2021, https://perma.cc/29HB-2KBK.

224 Electronic Privacy Information Center, *EPIC Urges DHS Data Privacy Committee to Ensure Meaningful Oversight of Information Sharing Agreements*, Electronic Privacy Information Center, May 14, 2021, https://perma.cc/R3CL-KZ4R.

software (like Brighter.ai or FaceBlur).[225] Technology companies such as Apple are using the power of their App store approval to provide a new AppTrackingTransparency feature that allows users to opt-out of tracking by applications on their phone.[226] While technology tools can aid in data minimization, technology companies are still beholden to profit incentives, as exhibited by Apple's decision to abandon encryption technology, digital keys, and data maintenance to Chinese state employees.[227]

Advocates have also minimized data collection through obfuscation techniques such as computer vision dazzle makeup techniques that confound facial recognition technology, disabled phone tracking, concealed messages through stenography, disappearing messages, and encrypted messaging applications.[228] These obfuscation techniques should be used as demonstrative campaigns–not long-term policy solutions–and used with caution as they may be penetrable[229] and cause more suspicion and surveillance by police.

To support interventions like this in your community, you can join campaigns to regulate identifying technologies and data, like facial recognition technology, organized by your local ACLU chapter[230] or EFF's Electronic Frontier Alliance[231] or join global campaigns hosted by Amnesty International and Access Now. To track recent data privacy regulations can check out JD Supra's *U.S. Biometric Laws & Pending Legislation Tracke*r,[232] National Conference of State Legislature's *2020 Consumer Data Privacy Legislation* round up.[233] To protect your identifying data, you can check

225 Sejuti Das, *Is There A Case Of Regulating Facial Recognition Technology?*, Analytics India Magazine June 20, 2020, https://perma.cc/857M-D7GN.

226 Brian X. Chen, *To Be Tracked or Not? Apple Is Now Giving Us the Choice.*, The New York Times, Apr. 26, 2021, https://perma.cc/4MML-5WY4.

227 Jack Nicas, Raymond Zhong & Daisuke Wakabayashi, *Censorship, Surveillance and Profits: A Hard Bargain for Apple in China*, The New York Times, May 17, 2021, https://perma.cc/GE5Q-AX69.

228 Pavlina Pavlova, *Did they crack the code? The importance of encryption for protest movements,* Open Global Rights, Nov. 20, 2020, https://perma.cc/BQ97-EFUS.

229 Lily Hay Newman, *How law enforcement gets around your smartphone's encryption*, Ars Technica, Jan. 15, 2021, https://perma.cc/BQG2-DCGE.

230 *ACLU Affiliates,* American Civil Liberties Union (2021), https://perma.cc/W3Q3-WG8M.

231 *Electronic Frontier Alliance,* Electronic Frontier Foundation (2021), https://perma.cc/4EWL-BGQ5.

232 Lauren Caisman, Amy de La Lama, & Melissa Ruth Whigman, *U.S. Biometric Laws & Pending Legislation Tracker*, JD Supra, May 13, 2021, https://perma.cc/2HAJ-RL9H.

233 Pam Greenberg, *supr*a note 212.

out resources like EFF's *Surveillance Self-Defense Playlist: Getting to Know Your Phone.*[234]

4. Provide Meaningful Redress for Those Harmed

Finally, To stop harmful "smart city" technology, data, and uses, we must ensure there are consequences for using identifying data beyond our politically negotiated standards and that those consequences provide proportional redress for those harmed. It is not enough to pass data regulations if they are not enforced. Further, and especially important at this time, with many data regulation gaps, we must ensure that those who are harmed have swift and proportional channels of justice. The status quo of providing limited causes of action for those misidentified, no redress for those overly surveilled, and nominal damages to victims of data breaches is not enough.

Current interventions for data regulation enforcement that should be expanded include the human rights injunctions and sanctions mentioned above, fines for violations (like the GDPR[235]), and the cancelation of contracts with violating companies, public sector employee discipline and criminal penalties, private rights of action for those harmed, and suppression of evidence inappropriately obtained that are available under some regulations. These enforcement provisions are bolstered by whistleblower protections to encourage folks to come forward with knowledge of such misuses. Legislatures should be mindful of scoping what constitutes a misuse of identifying data and penalize it appropriately (for example, *Van Buren v. the United States,*[236] recently found that misuse of databases that one was otherwise authorized to use would not violate the *Computer Fraud and Abuse Act*, which comes with steep criminal penalties). In addition to penalties for misuse, individuals must have recourse when their identifying data has been misused against them. Private rights of action under surveillance technology laws are available in Berkeley, Cambridge, Davis, Grand Rapids, Lawrence, Oakland, San Francisco, Santa Clara, Seattle, and Somerville, and

234 Alexis Hancock, *supra* note 9.

235 Privacy Affairs, GDPR Fines List: Find all GDPR fines & detailed statistics, PRIVACY Affairs (2021), https://perma.cc/9M4G-BJMB.

236 United States v. Mayweather, No. 17-13547 (11th Cir. 2021)

suppression remedies are available in Lawrence and Somerville.[237] And the *IL Biometric Information Privacy Act*,[238] which has provoked a series of lawsuits, including a recent $650 million Facebook settlement, is an encouraging example of redress.

To support interventions like these in your community, discuss the examples listed above with your local community groups and local representatives. To think more deeply about how regulation can provide those harmed with justice, check out analyses of local privacy laws like Berkeley Law's Samuelson Law, Technology, and Policy Clinic's *Local Surveillance Oversight Ordinances*[239] that analyze available remedies and their implementation track record.

237 Rebecca Williams, *supra* note 23.

238 Nicholas Iovino, *Judge Approves $650 Million Settlement in Facebook Biometric Case*, Courthouse News Service, Aug. 20, 2020, https://perma.cc/PNH8-2DQW.

239 Ari Chivukula & Tyler Takemoto, *Local Surveillance Oversight Ordinances*, Berkeley Samuelson Law, Technology & Public Policy Clinic, Feb. 2021, https://perma.cc/Y7KN-NL3S.

Build Our Collective Capacity to Evaluate How Technology Impacts Democracy

5. Mandating Transparency & Legibility for Public Technology & Data

To build our collective capacity to evaluate how technology impacts democracy, it is imperative we understand what our governments are doing in the first place. It is crucial to democracy to hold our government representatives accountable. This means to not only be aware of what "smart city" technologies are augmenting our neighborhoods but to firmly understand what data they are collecting and what the implications of that collection are.

Current interventions for mandating transparency and legibility for public technology and data that should be expanded include government transparency regulations and practices, campaigns to watch the watchers, third-party audits, and corporate transparency reports. Legislatures have called for transparency-related "smart city" technology with surveillance technology laws and practices such as providing discoverable documentation the procurement via the Open Contracting Partnership[240] and by documenting the call for such tools, such as Boston's New Urban Mechanics' *Beta Blocks* program, which posted a broad "Smart City" Request for Information (RFI)[241] in 2017 and publicly posted the 100+ responses online.[242] Beyond broadcasting proposal responses and procurement activity, governments should provide context and facilitate feedback loops related to novel technologies as Amsterdam,[243] and Helsinki[244] have done for AI; and Seattle[245] has done for "surveillance technologies."

240 *Open Contracting Data Standard,* Open Contracting Partnership (2021), https://perma.cc/8CGX-SSF6.

241 *Beta Blocks Request for Information (RFI),* City of Boston (2021), https://perma.cc/N9GG-JR8M.

242 *Beta Blocks Public RFI responses,* City of Boston, https://perma.cc/8T8K-XJX6.

243 *The Algorithm Register,* City of Amsterdam, https://perma.cc/6GJY-8TT3.

244 *The Algorithm Register,* City of Helsinki, https://perma.cc/JSP8-Q98G.

245 *Surveillance Technology Under Review,* City of Seattle, https://perma.cc/PKS5-BASN.

Advocates have issued campaigns to inventory surveillance technology, such as Amnesty International's *Decode Surveillance*,[246] which crowdsources the location of cameras in New York City, or EFF's *Atlas of Surveillance*,[247] which aggregates where many types of surveillance technology are located throughout the US through a variety of datasets. Beyond knowing what is being used, we must collectively understand the consequences of its use through third-party testing, evaluation, and hypotheticals. Examples of testing and evaluation include highlighting the unregulated use of facial recognition technology by Buzzfeed News' ClearviewAI audits (mentioned above) and privacy engineers demonstrating with publicly available datasets how easy it is to re-identify commuters, such as Morgan Herlocker's project that combined Mobility Data Specification data with other public datasets to identify sensitive scooter trips, including a midday trip from a high school in a conservative area of a city to a Planned Parenthood clinic.[248]

Lastly, technology companies like Amazon's Ring, have begun to disclose when governments request their data publicly for transparency purposes[249] and third-party commissions like Biometrics and Forensic Ethics have called for a publicly accessible record on the collaborative uses of live facial recognition (LFR) to reduce the secrecy around public-private partnerships.[250] Technology companies should go further in their transparency reports and include information about all data collection, storage, subcontractor data linkage, secondary uses, and provide city officials with safety options and options community residents can add into individually if they desire more insights.

To support interventions like these in your community, discuss the examples listed above with your local community groups and local representatives. To become an active auditor of the technology in your

246 *Join Decode Surveillance NYC*, Amnesty International, https://perma.cc/24C3-AZ79.

247 Electronic Frontier Foundation, Atlas of Surveillance, Electronic Frontier Foundation, https://perma.cc/3RS9-9DAL

248 Harry Campbell, *RSG113: Morgan Herlocker on Mobility Data and Privacy Concerns*, Ride Share Guy, Dec. 17, 2019, https://perma.cc/NLY9-KD3H.

249 Ring, *Ring Launches Request for Assistance Posts on the Neighbors App*, The Ring Blog, June 3, 2021, https://perma.cc/X9RL-P3TH.

250 Sebastian Klovig Skelton, *Biometrics ethics group addresses public-private use of facial recognition*, Computer Weekly, Jan. 29, 2021, https://perma.cc/3TVC-JUVT.

community, check out my *Your Guide to Watching the Watchers*[251] blog post, which also includes "smart city" contract documentation from 15 jurisdictions and a public records request template to get you started. You can also join or follow advocacy groups and investigative journalists such as Access Now, ACLU, Action Center on Race and the Economy, Amnesty International, Center for Democracy and Technology, Data 4 Black Lives, EFF, EPIC, Hiljade.Kamera.rs, Lucy Parson Labs, Reclaimyourface.eu, STOP LAPD Spying Coalition, STOP Spying NY, and journalists such as Ars Technica, Gizmodo, The Markup, MIT Tech Review, OneZero, ProPublica, The Intercept, Logic Magazine, Techdirt, The Verge, and VICE.

6. Question Technology's Role in Wicked Problems

To build our collective capacity to evaluate how technology impacts democracy, we must also all take a step back and consider how power is redistributed by technology companies beyond data rights. Evgeny Morozov penned an op-ed this May, suggesting that by focusing on privacy advocacy that we may have missed some of the more extensive ways technology companies are reconstructing power. In it, he writes:

> I suspect we've been looking in the wrong places for potent critiques of this industry. We have assumed that surveillance and fake news are what economists would call 'externalities' attached to what are otherwise good, progressive, and innovative business practices.
>
> But does that assumption hold? It's time that we see through the tech industry's lip service to innovation and ask, instead, just who is allowed to innovate – and under what conditions – in the current system. For all the creative disruption that its leaders promise us, the tech industry delivers an extremely unappetizing dish that invariably features the same set of ingredients: users, platforms, advertisers, and app developers.

251 Rebecca Williams, *Your Guide to Watching the Watchers*, Belfer Center for Science and International Affairs, May 25, 2021, https://perma.cc/P56R-KYEB.

> The institutional imagination of the tech industry simply does not admit other actors who can play a role in shaping the socially beneficial uses of digital infrastructures…
>
> The tech giants' recent respect for privacy should not mislead us. After all, it's their monopolistic hold on our imagination – making us unable to see technology not as applied science but as a potent political institution for transforming other institutions – that constitutes the greatest problem for democracy. And it's only by reclaiming that imagination – rather than by overdosing on feelgood solutionism – that we can aspire to tame them.[252]

We must change our thinking beyond technology efficiency solutions and reframe social challenges around the material needs of community members. To the extent data plays a role in these goals, it should be secondary and thoroughly tested, understood, and desired by community members before deploying.

Current interventions for questioning technology's role in wicked problems that should be expanded include government-led efforts to incrementally test how technology can support broader programming, advocates calls to stop the use of certain technologies, and third-party audits of technology's efficacy. Governments have demanded more rigor from technical support to broader solutions with practices such as Boston's New Urban Mechanics *Smart City Playbook,*[253] which includes plays such as, "Solve real problems for real people, "Don't worship efficiency," "Better decisions, not (just) better data," and "Platforms make us go ¯_(ツ)_/¯."[254] As mentioned, advocates like Action Center on Race & the Economy have included explicit calls to end surveillance data collection and end all funding of surveillance technology in their recommendations for *21st Century Policing* coupled with broader calls to defund the police and invest in community

252 Evgeny Morozov, *Privacy activists are winning fights with tech giants. Why does victory feel hollow?,* the Guardian, May 15, 2021, https://perma.cc/S8XE-S752.

253 Mayor's Office of New Urban Mechanics, *Boston Smart City Playbook,* Boston.gov, https://perma.cc/7X-PW-TU73.

254 *Id.*

safety.[255] Technology companies have provided vetted "smart city" technology case studies on platforms such as Marketplace.city that demonstrate where and how they have been used.

To support interventions like these in your community, discuss the examples listed above with your local community groups and local representatives. To think more deeply about technology ideology check out Morozov's work, as well as technology critiques by scholars and thinkers featured on the *Tech Won't Save Us* podcast and newsletter.

7. Challenge Data Narratives

Finally, to build our collective capacity to evaluate how technology impacts democracy we must ensure that community members can test and vet government data collection and the narratives they reinforce. This includes challenging what data is collected, identifying what data is not collected, whom it serves, and creating missing data.

Current interventions to challenge data narratives that should be expanded include governments providing bottom-up tools for communities to collect their own data and community members challenging top-down data collection through obfuscation, art, and the creation of alternative datasets. Governments have explored more ways to facilitate data collection by the community rather than dictate it, such as St. Louis' *Movement Lab*,[256] where community members mapped monuments in their community to tell a bottom-up history, or Barcelona's committment "to solve city challenges by fostering innovation through open government, towards pluralist social transformation" as part of their *Digital Plan*.[257] Advocates have altered the way dominant datasets are created about them by generating "data noise" by wearing adversarial fashion[258] that features images such as

255 Action Center on Race and the Economy and The Community Resource Hub for Safety and Accountability, *supra* note 186.

256 Lyndsay Knecht, *St. Louisans Mapped Monuments of Their City, and Uncovered Surprising Connections*, NEXT CITY, Jan. 27, 2021, https://perma.cc/Q74C-C8TL.

257 Corey Recvlohe, *How Smart Cities Succeed or Fail*, Dialogue & Discourse, Dec. 8, 2020, https://perma.cc/GD4R-79MA.

258 Adversarial Fashion, Adversarial Fashion, https://perma.cc/76EJ-5BHJ.

fake license plates, and other techniques.[259] Much like the limits of obfuscation techniques to minimize identifying data collection, these techniques are best used as demonstrations, with the long-term goals being formal processes to challenge and change data collection processes. Beyond demonstrating capabilities of technology, applying these tools to the powerful can be an effective advocacy tool as when Italian artist Paolo Cirio created a database with 4000 faces of French police officers to crowdsource their identification[260] amongst protests and provoking changes in the law.[261] Advocates have also called to record the police[262] to create evidence and counter data narratives against those who evade accountability.

To support interventions like these in your community, discuss the examples listed above with your local community groups and local representatives. To think more deeply about challenging data narratives, check out *Obfuscation: A User's Guide for Privacy and Protest* by Finn Burton and Helen Nissenbaum, community participation organizations like Public Lab, research organizations such as Data & Society, and leading investigative data journalism work feature at the Investigative Reporter's and Editor's annual *National Institute for Computer-Assisted Reporting* conference.

259 DJ Pangburn, *How to Disappear in a Fog of Data (and Why)*, Motherboard Tech by VICE, Nov. 16, 2016, https://perma.cc/QRH8-N734.

260 Censored work showing faces of 4,000 French police officers goes on show in Berlin, https://perma.cc/3M89-CKRX.

261 The Associated Press, *France to rewrite controversial bill restricting publication of police images in wake of nationwide protests,* CBC News*,* Nov. 30, 2020, https://perma.cc/BQ59-PMFK.

262 Andrew Couts, *Record the Police*, Gizmodo, Apr. 21, 2021, https://perma.cc/HH5Z-SJCU.

Fortify Old and Build New Democratic Spaces

8. Build Up Spaces for Community Decision-making

To fortify old and new democratic spaces we must create spaces for discussions about our community goals and how technology or data collection may serve those goals. We must reinforce these spaces for discussion through community organizing, legal protections, and tools that make it easier to do so. Further, to be able to meaningfully discuss community issues and applicable technology, communities need the support of trusted intermediaries, bodies of knowledge and resources to develop technology and data literacy.

Current interventions to build spaces for community decision-making that should be expanded include mandated community advisory bodies, advocacy resources and organizing, and tools that facilitate discussion of social problems rather than dictate their solution. Legislatures must have an ongoing dialogue with their community members, and advisory bodies are one tool to help facilitate this. Local governments have created hyperlocal community-led advisory bodies such as New York City's community boards or Washington D.C.'s advisory neighborhood commissions for broad policy advice. Berkeley, Oakland, San Francisco, and Seattle require independent review as part of their surveillance technology oversight. Digital advocacy organizations like the ACLU, EFF, and the Future for Privacy Forum have provided digital literacy guides related to surveillance and "smart city" issues, as well as communities for advocates and practitioners to join and discuss recent technology issues. In Toronto, community members gathered to host *Some Thoughts*[263] an impromptu call to discuss issues central to the Sidewalk Toronto proposal. Public-private member associations, like the Minnesota Connected and Automated Vehicle Alliance, are working to collectively create a privacy and security framework to guide local "smart" transportation infrastructure and vehicle projects.[264]

263 *The Tables*, Some Thoughts (2021), https://perma.cc/5H9D-EHQA.

264 Jule Pattison-Gordon, *Minnesota Crafts Privacy Principles for Emerging Transit Tech*, GovTech, Apr. 13, 2021, https://perma.cc/XHV4-R6MD.

To support interventions like these in your community, discuss the examples listed above with your local community groups and local representatives. To think more deeply about the process behind designing community solutions, check out the *Design Justice Network Principles.*[265]

9. Explore How Technology and Data Can Serve Democratic Goals

To fortify old and new democratic spaces we must also work together to consider how technology can bolster new ways to be in democratic dialogue with our fellow community members and build consensus toward our collective goals.

Current interventions to explore how technology and data can serve democratic goals that should be expanded include calls for data practices and policies that consider collective rights and decision-making and the building of technology tools that facilitate consensus-building. Advocates and scholars have begun to articulate how new approaches to data governance can serve collective decision-making, such as Jonathan van Geuns and Ana Brandusescu's *Shifting Power Through Data Governance,* which explores a taxonomy of data governance approaches,[266] Salome Viljoen's *Democratic Data: A Relational Theory For Data Governance,* which considers data's collective purposes,[267] and Bennett Cyphers and Cory Doctorow's *Privacy Without Monopoly: Data Protection and Interoperability,* which calls for open standards to minimize the corporate concentration of data control.[268] Government's such as Taiwan have provided tools such as Pol.is to facilitate consensus building among community members to inform policy. Technology companies, like Remix, which creates editable streets, facilitate community collaboration on imagining changes to their neighborhood.

265 *Principles*, Design Justice Network, https://perma.cc/P83X-WJCU.

266 Mozilla Insights, Jonathan van Geuns, & Ana Brandusescu, *Shifting Power Through Data Governance*, Mozilla, Sept. 2020, https://perma.cc/9YB6-ZP3U.

267 Salome Viljoen, *Democratic Data: A Relational Theory For Data Governance*, Yale Law Journal, Forthcoming, Nov. 11, 2020, http://dx.doi.org/10.2139/ssrn.3727562.

268 Bennett Cyphers & Cory Doctorow, *Privacy Without Monopoly: Data Protection and Interoperability*, Electronic Frontier Foundation, Jan. 2021, https://perma.cc/WN3D-VNSD.

To support interventions like these in your community, discuss the examples listed above with your local community groups and local representatives. To think more deeply about how we might reconceptualize data to serve collective goals, check out *On Property* by Rinaldo Walcott, *Indigenous Data Sovereignty and Policy* by Maggie Walter and Tahu Kukutai, and *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* by Julie E. Cohen.

10. Imagine New Democratic Rights in the Wake of New Technologies

Finally, to fortify old and new democratic spaces, we must imagine new ways of governing by the will of the people and develop new rights that serve those ends. To do this, we may need to rethink long-held frameworks (such as, but not limited to Fourth Amendment doctrine, anti-trust law, conceptions of personally identifiable information, property, and individual rights, and capitalism itself) that do not translate to the modern world. This will require robust and continuous dialogue and creative thinking about how technology relates to supporting the many and not the few.

Current interventions to develop new democratic rights in the wake of technological capabilities that should be expanded include interdisciplinary evaluations, articulating new risks, challenging old paradigms, and science fiction. In *Suspect Development Systems: Databasing Marginality and Enforcing Discipline*, Rashida Richardson and Amba Kak create a definitional and analytical framework for understanding an ever-evolving ecosystem of technologies that consider the technical, legal, political economy, organizational, and social outcomes based on examples from around the world.[269] In *The Age of Surveillance Capitalism,* Shoshana Zuboff articulates the potential behavioral futures economy being created by an unprecedented amount of personal behavior data collection by the private sector aimed at increasing sales that she argues will not be addressed by

269 Rashida Richardson & Amba Kak, *Suspect Development Systems: Databasing Marginality and Enforcing Discipline*, University of Michigan Journal of Law Reform, Vol. 55, Forthcoming, June 1, 2021, http://dx.doi.org/10.2139/ssrn.3868392.

current privacy or antitrust legal frameworks.[270] In *Roles for Computing in Social Change*, the authors identify ways technology can serve to "rethink" social issues by acting as a diagnostic, a formalizer, a rebuttal, or a synecdoche.[271] Finally, as we think about potential outcomes of current "smart city" trajectories, the science fiction work of Aldous Huxley, George Orwell, Ursula K. Le Guin, Ted Chiang, N.K. Jemisin and many others serve as ways for us to stretch our imagination of how society may rearrange itself as new technologies present themselves.

To support interventions like these in your community, discuss the examples listed above with your local community groups and local representatives and let the world know what has stretched your imagination.

270 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (2019).

271 Rediet Abebe et al., *Roles for Computing in Social Change*, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 252–260 (2020), https://arxiv.org/abs/1912.04883.

Technology and Public Purpose Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/TAPP

Printed in the United States of America