

# A More Responsible Digital Surveillance Future

*Multi-stakeholder Perspectives and Cohesive  
State & Local, Federal, and International Actions*

**Ishan Sharma**

*February 2021*



Federation  
of American  
Scientists

*A Special Project on Emerging Technologies and  
International Security of the Federation of American Scientists*

<b>Executive Summary</b>	<b>6</b>
<b>Background</b>	<b>8</b>
<b>Stakeholder Synthesis</b>	<b>16</b>
<i>Harm Reduction Approach</i>	16
<i>Obstacles</i>	18
<i>Federal Coordination</i>	22
<i>Strategic International Policy Considerations</i>	23
<b>Stakeholder Recommendations</b>	<b>25</b>
<i>Academia</i>	25
<i>Civil Society</i>	25
<i>Law Enforcement</i>	27
<i>Government</i>	28
<i>Industry</i>	30
<b>Policy Recommendations</b>	<b>32</b>
<i>Federal Action</i>	32
1. Create a Digital Surveillance Oversight Committee (DSOC)	32
2. Create a Democratic Surveillance Accelerator	34
3. Establish Portable Acquisition Standards	35
4. Establish Federal Privacy Legislation	36
5. Condition Federal Grants	37
6. Develop Federal Judiciary Guidance on Surveillance	37
7. Empower Defense Counsel Symmetric Access to Digital Records	37
8. Reform Information Sharing and Collection Practices	38
<i>State &amp; Local Action</i>	39
10. Secure Citizens' Digital Rights in State Amendment, Contract, and Investment	39
11. Seek and Contribute Guidance with Neighboring Localities	40
<i>International Action</i>	40
12. Reform U.S. Export Control Regimes	40
13. Coordinate Multilateral Export Controls	42
14. Create an E.U.-U.S. Joint Digital Development Fund	42
15. Engage Diplomatically	43
<b>Appendix A: List of Stakeholders</b>	<b>45</b>
<b>Appendix B: Interview Questions</b>	<b>47</b>
<b>Appendix C: Sample Certification Questionnaire</b>	<b>48</b>
<b>Appendix D: Draft Executive Order</b>	<b>49</b>

## Acknowledgements

This report is the product of a groundswell of support from friends, colleagues, and mentors. Over 40 stakeholders—from police chiefs to executive directors of organizations, and many more busy professionals—generously devoted their time to this effort. A special thanks is owed to Dahlia Peterson (Center for Security and Emerging Technology), Kevin Wolf (Akin Gump LLP), Rachel Levinson-Waldman (Brennan Center for Justice), Albert Fox Cahn (Surveillance Technology Oversight Project), Courtney Bowman (Palantir Technologies), Esha Bhandari (ACLU), Hector Dominguez-Aguirre (Portland SmartCity PDX) and Maily Fidler (Reports Committee for Freedom of the Press) who, in addition to their participation, found time to offer meaningful commentary and edits for this report’s drafting.

The special Project on Emerging Technologies and International Security (PETIS) would not have been possible without the support of the Scoville Fellowship or the current and former members of the Federation of American Scientists: Kathryn Kohn, Mercedes Trent, Erik Martin, Priscilla Guo, Ali Nouri, and Dan Correa. Thank you for sharing your wisdom and lending your talents since the very beginning.

## About the Author

Ishan Sharma is a Herbert Scoville Jr. Peace Fellow of Emerging Technologies at the Federation of American Scientists. He holds a B.S. from Cornell University and has studied jurisprudence and international human rights law at the University of Oxford. At FAS, he leads a special Project on Emerging Technologies and International Security, which aims to counter digital authoritarianism. He is also staffed on the Disinformation Research Group and is a Project Advisor at the Day One Project, a policy incubator curating key science and technology ideas to inform the Biden-Harris Administration.

## Definitions

**Digital Surveillance:** a product or service marketed for or that can be used (with or without the authorization of the business) to detect, monitor, intercept, collect, exploit, interpret, preserve, protect, transmit, and/or retain sensitive data, identifying information, or communications concerning individuals or groups. The following is a non-exhaustive list of categories:

- **Sensors** (e.g., specialized computer vision chips, thermal imaging systems, electronic emissions detection systems, gunshot detection and location hardware and services, x-ray vans, surveillance-enabled lightbulbs, through-the-wall radar or similar imaging technology, and other products designed to clandestinely intercept live communications)
- **Biometric identification** (e.g., facial, voice, iris, emotion, gait, and other recognition software and databases, automated biometric systems, DNA mobile capture and rapid testing software)
- **Data analytics** (e.g., social media analytics software, predictive policing systems, data fusion technology, and other dataset analysis tools capable of deriving insights about identified or identifiable individuals)
- **Internet surveillance tools** (e.g., “spyware,” products with certain deep packet inspection functions, penetration-testing tools, products designed to defeat cryptographic mechanisms in order to derive confidential variables or sensitive data including clear text, passwords, or cryptographic keys, or any other software and hardware used to gain unauthorized access to a computer, computer service, or computer network)
- **Non-cooperative location tracking** (e.g., products that can be used for ongoing tracking of individuals’ locations without their knowledge and consent, cell site simulators, automatic license plate readers)
- **Recording devices** (e.g., body-worn or drone-based, network protocol surveillance systems, devices that record audio and video and can remotely transmit or can be remotely accessed)

**Due Diligence:** the process by which a business selling or a government entity employing surveillance technology works to identify, anticipate, prevent, mitigate, and account for how it addresses actual or potential adverse impacts on the civil and human rights and liberties of individuals.

**Mission Creep:** a gradual shift from initial objectives of policy or agency, due to changes in power, culture, or other operational decision-making processes.

**Harm Reduction Approach:** a recognition of the historically disproportionate impact of surveillance on certain communities and a commitment to greater transparency and accountability in the acquisition and use of surveillance technologies.

# Executive Summary

This report addresses the widening gap between domestic and international policy on the emergence of digital surveillance technologies. Advances in video data analytics, Internet spyware, artificial intelligence, among others have enabled unprecedented, granular surveillance at scale. The advent of digital surveillance has intersected with a global resurgence of authoritarianism, a weakening of democratic process and rule of law in the United States and abroad. In contrast, the digital authoritarian model has become more stable, accessible, and competitive than ever before.

These technologies are here to stay – and will only continue to proliferate and improve. Demand in the last few years has skyrocketed, with at least a hundred countries now applying some form of digital surveillance—from smart cities to real-time facial recognition. In this era, democratic governments must lead by example. As the second half of the world gains Internet access, promoting the more responsible use of surveillance technology will depend on finding a better, more democratic approach to digital surveillance in the United States and beyond. And yet, the United States’ roll-out of surveillance has been un-democratic at best: judicial accountability is estimated to be at least 10 years behind the deployment of new technology; police departments acquire technologies through opaque funding and public-private contracts protected by NDAs; marginalized communities endure an inequitable burden of the privacy costs, which are often viewed as a lost cause by a privileged society that has little incentive to organize.

Democracies must plan for the informatization of the 21<sup>st</sup> century. Fortunately, a patchwork of efforts across various municipal, federal, and international institutions have attempted to remedy some of these issues. Spanning academia, civil society, industry, law enforcement, and government, this report consulted a variety of stakeholders to amplify these reforms and locate a less-harmful, more democratically responsive approach to surveillance. Representatives working at NYU Policing Project, Palantir Technologies, the Oakland Privacy Advisory Commission, the DC Metropolitan Police Department, and 40 others provided a total of 41 observations for digital surveillance reform. The report concludes with a set of 15 policy recommendations to unite the state & local, federal, and international actions on digital surveillance reform agenda.

Stakeholders unanimously recognized that in the United States, certain immigrants and communities of color, dissent, nonconformity, and others continue to face immense oppression from surveillance operations. Some stakeholders were pessimistic about the possibility of achieving a responsible system of surveillance. Nonetheless, the overwhelming majority agreed that immediate reform is needed to reduce harm. Under this harm-reduction approach, entities acquiring and applying digital surveillance would take proactive steps—such as embracing better scrutinized warrant requests, testing technologies for bias, and implementing rigorous evaluation criteria during and after use—to reduce the disproportionate harm posed by digital surveillance

Stakeholders also identified three broad obstacles in the current system that continue to forestall harm-reduction: information asymmetries, destructive habits and beliefs, and testing and verification limitations. An absence of federal action to overcome these obstacles has led to only piecemeal efforts to guarantee citizens meaningful transparency and privacy with democratic oversight. Considering this and that decisions on the deployment of surveillance technologies in the United States will implicate racial justice,

economic, science and technology, as well as global security policy interests, nearly all stakeholders called for more guidance and coordination by the Federal Government. Governments and citizens would benefit from revised, privacy-protective federal acquisition standards and data privacy laws, while industry would appreciate greater demand-side signaling towards more responsible innovation. There was broad consensus that such federal action should not preempt state and local efforts.

Stakeholders also emphasized that the proliferation of these technologies represents a very serious threat to the future of democracy, human rights, and rule of law around the world. The unregulated global surveillance industry offers exporting companies an unvirtuous cycle of exploitative growth. Unless importing countries are careful, there is significant risk surveillance-tech companies will harvest biometric data at country-wide scale to further tailor their products and entrench technological dependencies. While there was healthy debate among stakeholders on the importance of U.S. competitiveness in the surveillance industry, many stakeholders agreed on the pressing need for setting universal operating procedures for companies. Some stakeholders encouraged moving the present discussion away from only blaming companies for their authoritarian countries of origin, as too many Western-based companies have also contributed towards the abuse of these technologies and human rights. Indeed, many stakeholders noted how the domestic “wild-west” of surveillance acquisition and use continues to create hypocrisy and undermine international policy efforts.

Stakeholders tended to offer observations and policy prescriptions consistent with their field of expertise. Academic stakeholders broadly considered surveillance to be a question of power, advocating for greater public knowledge over processes and a more cohesive blend between domestic and international policy. Civil society stakeholders urged the importance of centering the voices of historically surveilled communities in any discussion of reform and cautioned against municipalities developing technological dependencies with large companies. Law enforcement stakeholders stressed the importance of surveillance for public safety, but also that agencies should recognize the win-win from building trust with greater community input, transparency, and accountability processes. Government stakeholders emphasized the importance of new regulations dealing with 21<sup>st</sup> century surveillance, such as promoting trust-building oversight infrastructures. Industry stakeholders asked for greater innovation signaling from the Federal Government and were generally favorable towards sensible regulation if it meant avoiding a developmental race to the bottom, with increasingly invasive technologies.

The range of viewpoints and priorities suggest policymaking would benefit from greater collaboration among stakeholder types. This report surveyed these multi-stakeholder interests as an attempt to find initial common ground, for which there was a surprising amount. Nearly all stakeholders supported greater scrutiny for warrant applications, the creation of nuanced, multilateral export controls, and the construction of meaningful public engagement mechanisms for the acquisition and proportionate use of digital surveillance technologies.

Based on this mutuality, this report offers a set of actionable recommendations for reducing harm in the domestic and international use of digital surveillance technologies. The most pressing recommendations are the layout of a Digital Surveillance Oversight Committee to tackle certification for the dynamic, multilayered surveillance tech industry; a Democratic Surveillance Accelerator to offset privacy- and democracy-preserving costs in companies that can strategically export with installed technical oversight monitoring tools and provide democratic operational training; and a partial roadmap for integrating U.S. export controls regimes into the recently adopted E.U. cybersurveillance control regimes, by expanding authorities to consider end-use violations of human rights.

# Background

From ancient spies to the census, effective governance has always depended on responsive information. Now, digital surveillance has exponentially increased the value that can be derived public data. For example, an average of only two percent of all CCTV footage is ever observed, with even less analyzed.<sup>1</sup> Advances in artificial intelligence (AI) and video analytics have increasingly mitigated these limitations. One person can simultaneously monitor 100+ feeds of thousands of people, with the all-seeing AI fusing the data streams to sound real-time alarms in cases of “anomalous” or deviant behavior.<sup>2</sup> Equally possible is the surveillance of the “bidstream”—the digital advertising ecosystem of location and other mobile phone and app data—to pinpoint individuals in large areas with little other than their phone number.<sup>3</sup> In the Age of Information, there are untold means of surveillance emerging, for ends impossible to comprehensively assess. Some offer AI-powered social media monitoring,<sup>4</sup> predictive policing algorithms,<sup>5</sup> and persistent aerial footage,<sup>6</sup> while others promise to identify emotions,<sup>7</sup> sexuality, or individuals based on their perceived gait.<sup>8</sup>

As the market matures, demand will follow. An estimated one billion surveillance cameras will be in use by the end of 2021—one for every eight people.<sup>9</sup> Over 80 countries now apply some form of digital surveillance, with subnational actors like mayors, provincial governors, and public safety officials driving demand to solve a variety of municipal problems.<sup>10</sup> The promising examples include East Asian nations like South Korea and Taiwan, which complemented efficient testing strategies and social safety nets with proportionate and democratically-compatible advanced track and trace methods to control COVID-19 spread.<sup>11</sup> However, government surveillance during the pandemic has not been immune to mission creep, as once-lauded Singaporean officials declared their track and trace data would be repurposed for criminal law enforcement.<sup>12</sup> Still, nowhere else has state-of-the-art surveillance technology met Orwellian horrors more than the Xinjiang province of China: at least one million Uyghur Muslims and other Turkic ethnic minorities have been forced into labor concentration, or ‘reeducation’, camps, after having been surveilled for years through invasive digital means designed to ferret out “ideological viruses.”<sup>13</sup> Recent reports have

1 Tang, D., et. al. (2018). Seeing What Matters: A New Paradigm for Public Safety Powered by Responsible AI, Accenture Strategy and Western Digital Corporation, 4. [https://www.accenture.com/\\_acnmedia/pdf-94/accenture-value-data-seeing-what-matters.pdf](https://www.accenture.com/_acnmedia/pdf-94/accenture-value-data-seeing-what-matters.pdf)

2 Michel, A.H (2021), “There Are Spying Eyes Everywhere—and Now They Share a Brain,” *Wired Magazine*, February 4, <https://www.wired.com/story/there-are-spying-eyes-everywhere-and-now-they-share-a-brain/>; Allen, G. and Chan, T. (2017) Artificial Intelligence and National Security, (report, *Belfer Center for Science and International Affairs, Harvard Kennedy School*, Cambridge, MA, July. 93. <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf>; Stanley, J. (2019) The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy, June 17. <https://www.aclu.org/report/dawn-robot-surveillance>

3 Brewster, T. (2020). Exclusive: Israeli Surveillance Companies Are Siphoning Masses Of Location Data From Smartphone Apps, *Forbes*, Dec. 11 <https://www.forbes.com/sites/thomasbrewster/2020/12/11/exclusive-israeli-surveillance-companies-are-siphoning-masses-of-location-data-from-smartphone-apps/?sh=727b990638fc>

4 Biddle, S. (2020). Twitter Surveillance Startup Targets Communities of Color for Police. *The Intercept*. October 21. <https://theintercept.com/2020/10/21/dataminr-twitter-surveillance-racial-profiling/>

5 Lau, T. (2020), Predictive Policing Explained. Brennan Center for Justice. April 1. <https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained>

6 Feeney, M., (2020). Judge Allows Warrantless Aerial Surveillance Over Baltimore. Cato Institute. April 29. <https://www.cato.org/blog/judge-allows-warrantless-aerial-surveillance-over-baltimore>

7 “Emotional Entanglement: China’s emotion recognition market and its implications for human rights,” *Article 19*, January 2021, <https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf>

8 Stanley, J. (2019) The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy, June 17. <https://www.aclu.org/report/dawn-robot-surveillance>

9 Kwet, M. (2020). The Rise Of Smart Camera Networks, and Why We Should Ban Them. *The Intercept*. January 27. <https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/>

10 Greitens, S.C. (2020). China’s Surveillance State at Home & Abroad: Challenges for U.S. Policy, Working Paper for the Penn Project on the Future of U.S.-China Relations, October 2020, [https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b732/files/2020/10/Sheena-Greitens\\_Chinas-Surveillance-State-at-Home-Abroad\\_Final.pdf](https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b732/files/2020/10/Sheena-Greitens_Chinas-Surveillance-State-at-Home-Abroad_Final.pdf)

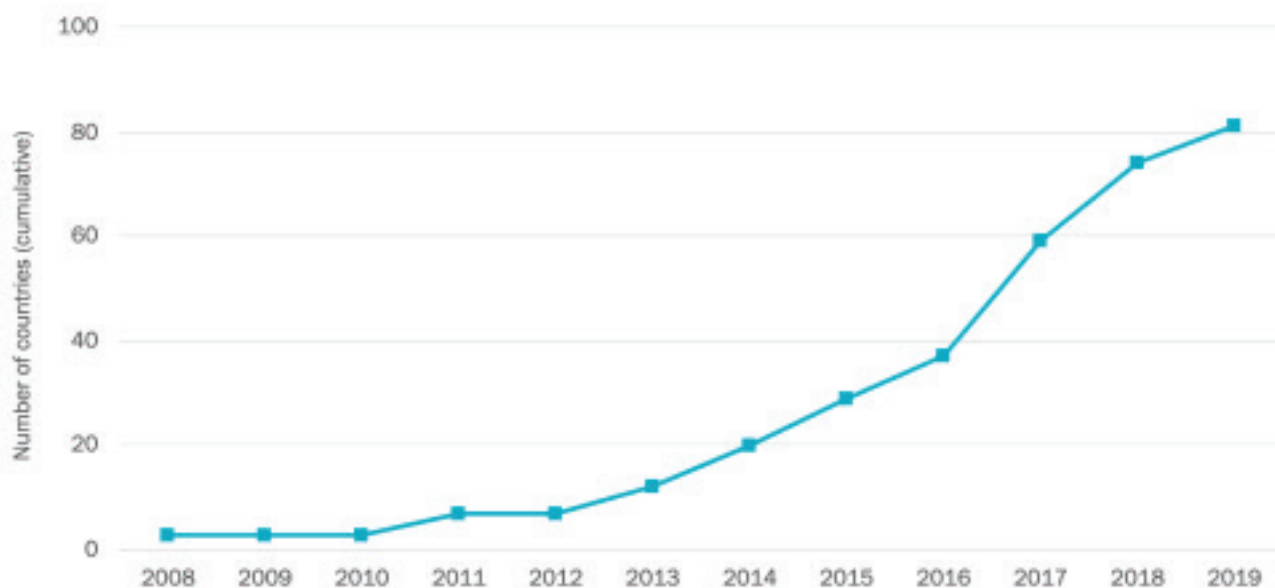
11 Greitens, S.C. (2020). Surveillance, Security, and Liberal Democracy in the Post-COVID World. International Organization. November 18. <https://www.cambridge.org/core/journals/international-organization/article/surveillance-security-and-liberal-democracy-in-the-postcovid-world/15CDF2C062ADCAAD6B5D224630F62B1D>

12 Illmer, A. (2021). Singapore reveals Covid privacy data available to police. *BBC News*. January 5. <https://www.bbc.com/news/world-asia-55541001>

13 Andersen, R. (2020). The Panopticon Is Already Here. *The Atlantic*. September. <https://www.theatlantic.com/magazine/archive/2020/09/china-ai->

uncovered facial recognition technology designed by Dahua,<sup>14</sup> Megvii, Huawei Technologies Co., and Alibaba offered targeted ethnic detection for Uyghur Muslims.<sup>15</sup> The range of companies offering similar Uyghur detection services is indicative of a response to customer demand. Some reports have estimated that companies based in China will own nearly half of the world's facial recognition market by 2023.<sup>16</sup> Indeed, as Figure 1 highlights, demand for Chinese surveillance and public security technology platforms has skyrocketed from 2008 to 2019. Regardless, the United States and allies have also been actively profiting off human rights abuses.<sup>17</sup> Recent reports indicate that E.U. aid money has been used to fund the acquisition of certain surveillance technologies and train officials in problematic uses across the Middle East, Northern and Western Africa, and the Balkans.<sup>18</sup> Many Western-based companies are aggressively vying for

### Adoption of Chinese Surveillance and Public Security Technology Platforms (2008-2019)



**Source:** Greitens, S.C. (2020). China's Surveillance State at Home & Abroad: Challenges for U.S. Policy, Working Paper for the Penn Project on the Future of U.S.-China Relations, October 2020, [https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b/732/files/2020/10/Sheena-Greitens\\_Chinas-Surveillance-State-at-Home-Abroad\\_Final.pdf](https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b/732/files/2020/10/Sheena-Greitens_Chinas-Surveillance-State-at-Home-Abroad_Final.pdf)

market share in Gulf Cooperation States.<sup>19</sup> The most prominent example is the NSO Group, a leading mobile phone surveillance software provider from Israel. The company, which offers “zero-click” hacking services (e.g. a victim does nothing but miss a voice call, which grants access into the phone), has also serviced the hacking of 1,400 WhatsApp phones and the targeting of civil society and political dissidents in Mexico, Saudi Arabia, and elsewhere.<sup>20</sup>

[surveillance/614197/](https://www.hrw.org/news/2020/12/09/china-big-data-program-targets-xinjiangs-muslims); China: Big Data Program Targets Xinjiang's Muslims. *Human Rights Watch*. December 9, 2020. <https://www.hrw.org/news/2020/12/09/china-big-data-program-targets-xinjiangs-muslims>

14 IPVM Team (2021), “Dahua Provides ‘Uyghur Warnings’ To China Police,” IPVM, February 9, <https://ipvm.com/reports/dahua-uyghur-warning>

15 Patenting Uyghur Tracking - Huawei, Megvii, More. IPVM Team. January 12, 2021. <https://ipvm.com/reports/patents-uyghur>

16 Wang, E. (2018). China to Take Nearly Half of Global Face Recognition Device Market by 2023. *China Money Network*. August 23. <https://www.chinamoneynetwork.com/2018/08/23/china-to-take-nearly-half-of-global-face-recognition-device-market-by-2023>

17 Woodhams, S. (2020). China, Africa, and the Private Surveillance Industry. *Georgetown Journal of International Affairs*. October 15. <https://muse.jhu.edu/article/766370/summary>

18 Surveillance Disclosures Show Urgent Need for Reforms to EU Aid Programmes. *Privacy International*. November 10, 2020. <https://privacyinternational.org/long-read/4291/surveillance-disclosures-show-urgent-need-reforms-eu-aid-programmes>

19 Mackenzie, L. (2020). Surveillance state: how Gulf governments keep watch on us. *WIRED*. January 21. <https://wired.me/technology/privacy/surveillance-gulf-states/>

20 Marczak, B. et. al, (2020). The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage ‘Zero-Click’ Exploit. *The Citizen Lab*. December 20. <https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/>

Despite these technologies providing massive updates to autocratic models, responsive international governance has been virtually non-existent. Placing accountability measures has been difficult, in part, due to the complex, internationalized surveillance industry. Industry responses to regulations suggest that, with a variety of global systems integrators and distributors as technology intermediaries, the initial manufacturer may never know the end-user.<sup>21</sup> At the same time, the international environment is rapidly codifying norms on new surveillance technologies. In the last three years, every submitted standard on facial recognition technology at the International Telecommunication Union (ITU), the 193-member UN international standards-setting body for surveillance and other technologies, has come from companies based in China.<sup>22</sup> These companies have promoted broad data

collection rights and application possibilities for government officials, including storage requirements for detected face features, like race and ethnicity, the ubiquitous surveillance of people in public spaces, and the persistent monitoring of employee attendance. ITU principles are often adopted throughout digitizing countries in Africa, the Middle East, and Latin America.<sup>23</sup> If China is successful in setting the normative, global standards climate, the global marketplace could very well “tilt” towards certain dangerous data collection methods and processes (e.g. racial and ethnic databases).<sup>24</sup> China-based surveillance technology would become more accessible, while privacy-preserving alternatives less attractive.

A recent report from mainland Chinese think tank *The Beijing News* offered insight into the broader development ecosystem of China-based facial recognition technology, for which surveillance companies are only a part. Out of 70 China-based apps analyzed only 7% had clear usage agreements and obtain prior consent.<sup>25</sup> The absence of privacy or consent highlighted by the report is mirrored by a recent patent application filed by Clearview AI, a U.S.-based facial recognition company that has serviced more than 2,200 law enforcement agencies, companies, and individuals across the world, and was found by Canada’s

## Surveillance state: how Gulf governments keep watch on us

Regional countries have deployed some of the world’s most advanced tech to keep tabs on what we do—from internet monitoring to facial recognition.



21 Erickson, D. (2020). Comment on FR Doc #2020-15416; Docket No. 200710-0186 [RIN 0694-XC063]. Security Industry Association responding to Bureau of Industry and Security Request for Public Comment. September 15. <https://www.regulations.gov/document?D=BIS-2020-0021-0018>

22 Gross, A. Murgia, M. and Yang, Y. (2019). Chinese tech groups shaping UN facial recognition standards. December 1. <https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67>

23 Ibid.

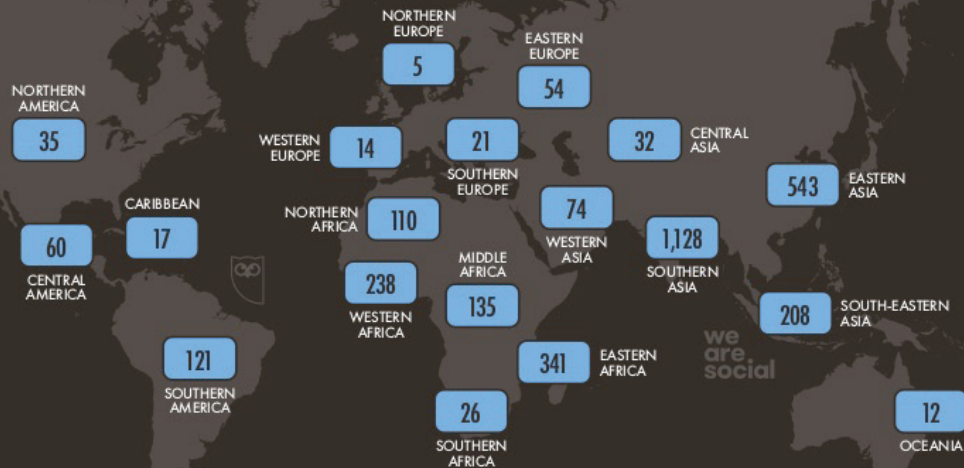
24 Greitens, S.C. (2020). China's Surveillance State at Home & Abroad: Challenges for U.S. Policy, Working Paper for the Penn Project on the Future of U.S.-China Relations, October 2020, [https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b/732/files/2020/10/Sheena-Greitens\\_Chinas-Surveillance-State-at-Home-Abroad\\_Final.pdf](https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b/732/files/2020/10/Sheena-Greitens_Chinas-Surveillance-State-at-Home-Abroad_Final.pdf)

25 Chunrui, W. (2021), “Nearly half of the evaluation apps did not solicit user opinions separately, and many scenic spots and communities forced to ‘brush their faces’” *The Beijing News*, January 26, [https://m.bjnews.com.cn/h5special/161161836815643.html?fbclid=IwAR0zZotuM2PDlp-X6A4mWsl\\_bYoOfIK4KY2ZskFEpvnPrjoyadrUtWnzks](https://m.bjnews.com.cn/h5special/161161836815643.html?fbclid=IwAR0zZotuM2PDlp-X6A4mWsl_bYoOfIK4KY2ZskFEpvnPrjoyadrUtWnzks) (see translation at <https://docs.google.com/document/d/1rWoqdwT6a52kO2Q-QVPfHdbtyoS8RkaWls5hbZRLB2M/edit#>)

JAN  
2021

## THE 'NEXT BILLION': UNCONNECTED AUDIENCES

THE NUMBER OF PEOPLE (IN MILLIONS) IN EACH REGION WHO ARE NOT CONNECTED TO THE INTERNET



31

**SOURCES:** KEPIOS (JAN 2021) BASED ON EXTRAPOLATIONS OF DATA PUBLISHED BY THE ITU, LOCAL GOVERNMENT BODIES, GWI, GSMA INTELLIGENCE, EUROSTAT, APIII, CNNIC, THE U.N. **ADVISORIES:** INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS. FIGURES ARE NOT COMPARABLE WITH DATA PUBLISHED IN PREVIOUS REPORTS. **NOTES:** FIGURES REPRESENT THE NUMBER OF PEOPLE (IN MILLIONS) WHO DO NOT USE THE INTERNET. REGIONS BASED ON THE UNITED NATIONS GEOScheme.

we  
are  
social

Hootsuite

**Source:** Kemp, S. (2021), "Digital 2021 Global Overview Report," DataReportal, January 27. <https://datareportal.com/reports/digital-2021-global-overview-report#:~:text=Internet%3A%204.66%20billion%20people%20around,now%20stands%20at%2059.5%20percent.>

federal privacy commissioner to have engaged in "mass surveillance" of millions of citizens.<sup>26</sup> Needless to say, China-based surveillance tech companies, who have gained outsized influence in setting global norms, would likely not offer more thorough data privacy or collection practices.

The worldwide threat to democracy and human rights from failed engagement over setting standards cannot be overstated, especially for surveillance technologies. **One-half of the world is still to come online; in the next decade, as over 90% of humanity gains Internet access, many countries will develop their digital norms and operating procedures.**<sup>27</sup> This digitizing world will decide if the technological abuse of surveillance power—one that can systematically silence free expression, delete dissidents from the information sphere, and scapegoats the most vulnerable with pseudoscience—will become commonplace.

For example, Huawei has installed a national CCTV system in Uganda with 83 monitoring centers, 522 operators, and 50 commanders. Pervasive location monitoring, facial recognition, biometric, and blanket data collection and retention practices are just some of the methods used to monitor political rallies and arrest dissidents. The deal originated as part of a classified contract between Huawei and Kampala authorities, and in 2019 Ugandan officials confirmed a price tag of \$126 million—more than the combined budgets of Uganda's ministries of Information and Communications Technology and Science, Technology, and Innovation. In January 2020, the second phase of installations began, integrating government agencies' surveillance efforts and expanding to over 2,319 municipalities.<sup>28</sup> A clear priority for the Ugandan

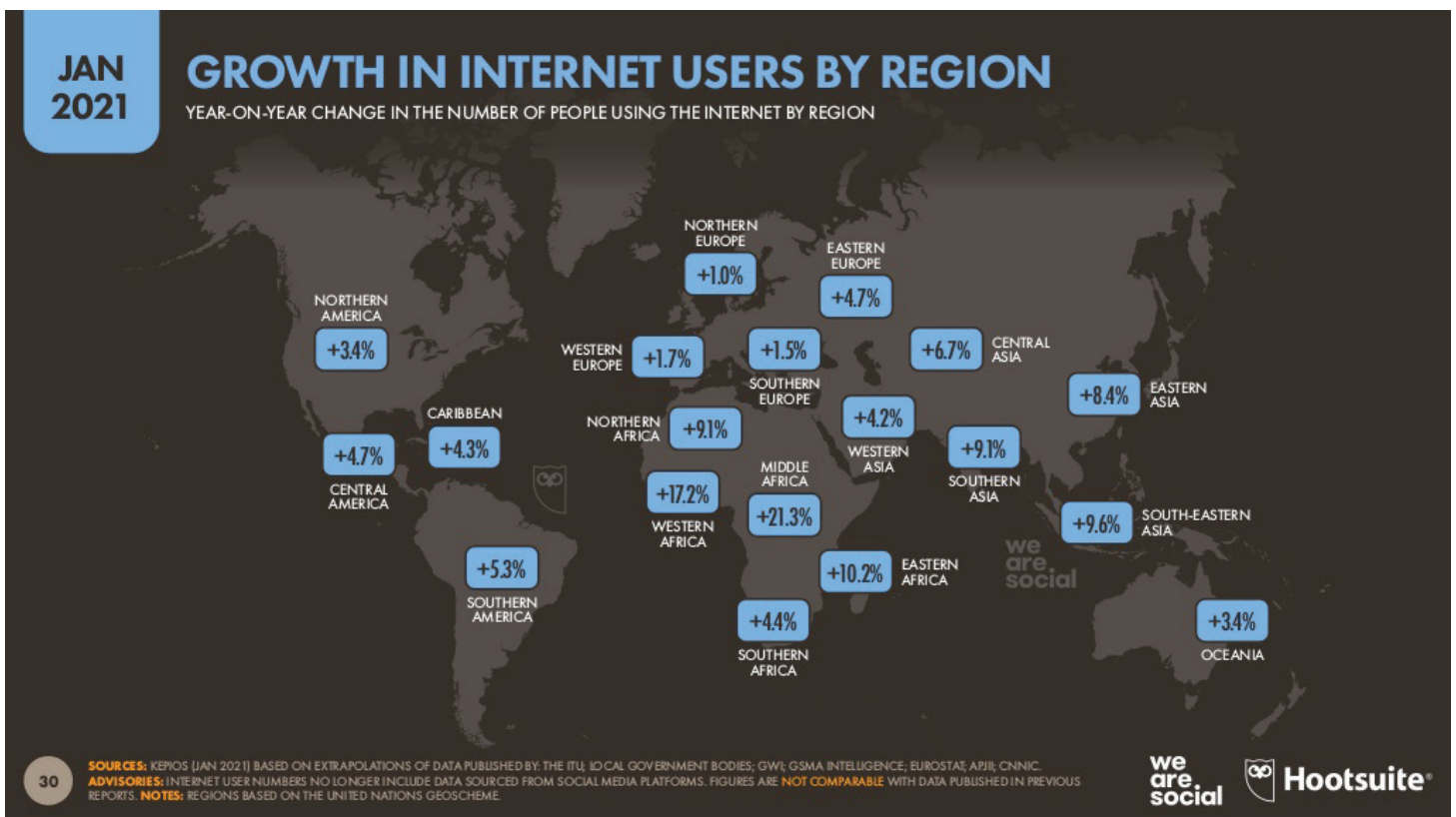
<sup>26</sup> Haskins, C., Mac, R., Sacks, B., (2021), "A Clearview AI Patent Application Describes Facial Recognition For Dating, And Identifying Drug Users And Homeless People," *BuzzFeed*, February 11, <https://www.buzzfeednews.com/article/carolinehaskins1/facial-recognition-clearview-patent-dating>

<sup>27</sup> Morgan, S. (2019), "Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion -- 90 percent of the human population, aged 6 years and older, will be online by 2030," *Cybercrime Magazine*, July 18. <https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/>

<sup>28</sup> Kafeero, S. (2020). Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests. *Quartz Africa*. November 27. <https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters/>

government, the installment and maintenance of such surveillance structures exemplify the potential for lock-in dependencies to develop.

A norms-setting game is afoot. China's global positioning—as both a provider of digital surveillance technologies and an entrepreneur of international norms—suggests the illiberal, digital authoritarian model will spread during and after COVID-19.<sup>29</sup> The pandemic has highlighted the benefits of this model. Chinese citizens have regained mobility and the luxuries of daily life, at the cost of complying with an intensive surveillance regime.<sup>30</sup> However, structural differences within the international community, such as federalism, partisan polarization, and toleration for individual deviance, may “limit the transmissibility of China's approach.”<sup>31</sup> As was evident in the African Union's Addis Ababa headquarters, additional concerns over secret, systems-based data siphoning, as was evident in the African Union's Addis Ababa headquarters, may create more hesitations in adopting technology from China.<sup>32</sup> At the moment, the spread of China's digital authoritarian playbook is, as Greitens (2020) argues, “not a foregone conclusion,” rather it will depend on a complex set of factors including geographic proximity, and regime type, among others.<sup>33</sup>



**Source:** Kemp, S. (2021), “Digital 2021 Global Overview Report,” DataReportal, January 27. <https://datareportal.com/reports/digital-2021-global-overview-report#:~:text=Internet%3A%204.66%20billion%20people%20around,now%20stands%20at%2059.5%20percent.>

**Leadership in this competitive, digital era must proceed by example—not by expectation or force.** Other countries cannot be expected to responsibly acquire or use surveillance technology if the United States and Western allies are engaged in or abetting the very same oppression. Fortunately, most democratic countries

<sup>29</sup> Greitens, S.C. (2020). Surveillance, Security, and Liberal Democracy in the Post-COVID World. International Organization. November 18. <https://www.cambridge.org/core/journals/international-organization/article/surveillance-security-and-liberal-democracy-in-the-postcovid-world/15CDF2C062ADCAAD6B5D224630F62B1D>

<sup>30</sup> Ibid.

<sup>31</sup> Ibid.

<sup>32</sup> <https://www.reuters.com/article/us-ethiopia-african-union-cyber-exclusiv-idUSKBN28Q1DB>

<sup>33</sup> <https://www.cambridge.org/core/journals/international-organization/article/surveillance-security-and-liberal-democracy-in-the-postcovid-world/15CDF2C062ADCAAD6B5D224630F62B1D>

using targeted surveillance, in principle, require some threshold of reasonable suspicion linking that person to a specific crime, and law enforcement must obtain independent authorization.<sup>34</sup> The intrusion on privacy must be limited in time and scope to the acquisition of evidence relevant to the crime under investigation.<sup>35</sup>

However, the application of these liberal principles has been weak and unaccountable, in the face of novel technologies. For example, a predictive policing algorithm, which calculates the probability of future crime from a person or a region based on historical, potentially biased criminal data, could infect the system of safeguards. Officers may make judgements about an individual's likelihood to reoffend based on the zip code they live in or how much they earn. Police may also become more suspicious of everyone in a particular geographic zone, increasing the warrants filed, cases investigated, and arrests made for certain communities. However, biased technology is only part of the problem. In general, despite the need to model a more democratically responsible approach to surveillance, **the example the United States has offered the world is characteristically un-American: a "wild-west" of morally bankrupt incentives overrun by opaque, "black-box" public-private partnerships.**<sup>36</sup> At the local level, there exists little to no check on the government's ability to bankroll surveillance barons' innovations. Judicial accountability is estimated to be at least 10-20 years behind the deployment of surveillance technologies.<sup>37</sup> Warrant requests filed for low-tech pen registers, which records all numbers called from a certain telephone line, end up granting the use of cell-site simulators capable of intercepting communications data.<sup>38</sup> Police reports, often due to non-disclosure agreements (NDAs) secured by the contracting surveillance company, will simply leave out any descriptions of the technologies altogether for the possibility of a court appearance. Citizens bear unequal costs from privacy intruded on by increasingly invisible surveillance, creating barriers to an organized public constituency.

Within this defunct system, one in two American adult citizens' faces are searchable within a law enforcement database and as of 2016 over 25% of the nearly 18,000 police departments had access to facial recognition tools.<sup>39</sup> From 2011 to 2019, law enforcement performed 390,186 facial recognition searches for over 150,000 individuals.<sup>40</sup> The New York Police Department (NYPD), for example, made nearly 3,000 arrests based on facial recognition searches in the first few years of use, while Florida law enforcement continues to run an average of 8,000 searches per month.<sup>41</sup> School resource officers in districts from Los Angeles to North San Antonio operate a Cellebrite UFED, a tool used to crack phones, in order to "recover deleted messages from the phone" of students.<sup>42</sup> In 2020, U.S. Customs and Border Protection applied facial recognition to over 23 million travelers, up from 19 million in 2019.<sup>43</sup> At the U.S.-Mexico

34 Dempsey, J. (2018). Privacy and Mass Surveillance: Balancing Human Rights and Government Security in the Era of Big Data. DIREITO, TECNOLOGIA, E INOVAÇÃO, Leonardo Parentoni, ed. [https://www.researchgate.net/publication/327824339\\_Direito\\_Tecnologia\\_e\\_Inovacao\\_-\\_v\\_I\\_Law\\_Technology\\_and\\_Innovation](https://www.researchgate.net/publication/327824339_Direito_Tecnologia_e_Inovacao_-_v_I_Law_Technology_and_Innovation)

35 Ibid.

36 Fidler, M. (2020). Local Police Surveillance and the Administrative Fourth Amendment. *Santa Clara High Technology Law Journal* 481. <https://digitalcommons.law.scu.edu/chtjl/vol36/iss5/2>

37 Ibid.

38 Ibid. See *United States v. Rigmaiden*, 844 F.Supp.2d 982 (D.Ariz.2012)

39 Garvie, C., Bedoya, A., and Frankle, J. (2016). The Perpetual Line-Up: Unregulated Face Recognition in America. Georgetown Law Center on Privacy & Technology. October 18. <https://www.perpetuallineup.org/findings/deployment>

40 Goodwin, G.L. (2019), "Testimony Before the Committee on Oversight and Reform, House of Representatives FACE RECOGNITION TECHNOLOGY DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains," *Government Accountability Project*, June 4, [https://www.gao.gov/assets/700/699489.pdf?utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=newsletter\\_axisofutureofwork&stream=future](https://www.gao.gov/assets/700/699489.pdf?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axisofutureofwork&stream=future)

41 Feldstein, S. and Wong, D. (2020). New Technologies, New Problems - Troubling Surveillance Trends in America. *Just Security*. August 16. <https://www.justsecurity.org/71837/new-technologies-new-problems-troubling-surveillance-trends-in-america/>

42 McKay, T. and Mehrotra, D. (2020). US Schools are Buying Phone-Hacking Tech that the FBI Uses to Investigate Terrorists. *Gizmodo*. December 11. <https://gizmodo.com/u-s-schools-are-buying-phone-hacking-tech-that-the-fbi-1845862393>

43 "CBP Trade and Travel Report Fiscal Year 2020," U.S. Customs and Border Protection, February 2021, <https://www.cbp.gov/sites/default/files/>

border, digital sentry towers apply persistent laser sensing and artificial intelligence to discern individuals from over two miles away, while Immigration and Customs Enforcement's (ICE) Enforcement and Removal Operations directorate share and collect information from "private data brokers and social networks to state and local government databases."<sup>44</sup> The day after the Capitol Hill insurrection, Clearview AI reported an overall 26% increase in law enforcement usage.<sup>45</sup>

**These technologies are expected to mature, making their use commonplace, with perhaps even more advanced capabilities.** Despite this, a "surveillance gap" weakens the efficacy and potential for data-driven public policy, as houseless, immigrant, and other "off-grid" communities rightfully fear inappropriate uses of collected data.<sup>46</sup> In contrast, welfare recipients consent to invasive government tracking and monitoring, under duress of hunger or health.<sup>47</sup> For formerly incarcerated individuals and others who have interacted with the legal system, criminal records data make it extraordinarily difficult to compete in the open labor market. BThe fact that only half of Federal Bureau of Investigation's (FBI) background checks fail to indicate the outcome of a case after an arrest, worsens this issue as individuals have no ability to dispute privacy-infringing information spread and purchased online.<sup>48</sup>

Digital surveillance has exacerbated injustices of privacy for immigrants and communities of color, dissent, nonconformity, or others with less representation. The landmark National Institute of Standards and Technology's (NIST) Face Recognition Vendor Test (FRVT) found some algorithms will misidentify minority individuals compared to white individuals by "factors of ten to beyond 100 times."<sup>49</sup> Robert Julian-Borchak Williams, the first known to be wrongfully accused by an algorithm, even had an alibi and still endured a several hours in jail after a humiliating arrest, despite having an alibi.<sup>50</sup> A less-publicized Williams may still be failing background checks for such an encounter, regardless of their release.

But even a perfectly unbiased technology can be misused. Already in the United States, some of these technologies have been disproportionately placed in black and brown communities.<sup>51</sup> A few commentators have gone so far as to draw direct parallels from China's model to the U.S. use of digital surveillance.<sup>52</sup> The lack of coordination between state and local agencies and the Federal Government over surveillance oversight has created a deeply unregulated environment and a discordant international agenda. Meanwhile, COVID-19 has accelerated the intrusive use of surveillance worldwide, often without transparency, independent oversight, or avenues for redress.<sup>53</sup> There are a multitude of surveillance technologies in use and more are coming.

[assets/documents/2021-Feb/CBP-FY2020-Trade-and-Travel-Report.pdf?utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=newsletter\\_axiosfutureofwork&stream=future](https://assets.documentcloud.org/documents/2021-Feb/CBP-FY2020-Trade-and-Travel-Report.pdf?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosfutureofwork&stream=future)

44 Feldstein, S. and Wong, D. (2020). New Technologies, New Problems - Troubling Surveillance Trends in America. *Just Security*. August 16. <https://www.justsecurity.org/71837/new-technologies-new-problems-troubling-surveillance-trends-in-america/>

45 Bhuiyan, J. (2021), "Facial recognition may help find Capitol rioters — but it could harm many others, experts say," *Los Angeles Times*, February 4, [https://www.latimes.com/business/technology/story/2021-02-04/facial-recognition-surveillance-capitol-riot-black-and-brown-communities?utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=newsletter\\_axiosfutureofwork&stream=future](https://www.latimes.com/business/technology/story/2021-02-04/facial-recognition-surveillance-capitol-riot-black-and-brown-communities?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosfutureofwork&stream=future)

46 Gilman, M.E. and Green, R. (2018), The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization. 42 *NYU Review of Law and Social Change* 253. May 3. <https://ssrn.com/abstract=3172948>

47 Ibid.

48 Lageson, S.E. (2020). *Digital Punishment*. Oxford University Press. June 24. <https://global.oup.com/academic/product/digital-punishment-9780190872007?cc=us&lang=en&>

49 Grother, P., Ngan, M. Hanaoka, K. (2019). Face Recognition Vendor Test Part 3: Demographic Effects. *National Institute of Standards and Technology*. December. <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>

50 Hill, K. (2020). Wrongfully Accused by an Algorithm. *New York Times*. <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>

51 Petty, T. (2020). Defending Black Lives Means Banning Facial Recognition. *WIRED*. July 10. <https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/>

52 Thompson, D. (2019). A Tale of Two Surveillance States. *The Atlantic*. May 30. <https://www.theatlantic.com/technology/archive/2019/05/the-us-and-china-a-tale-of-two-surveillance-states/590542/>

53 Shabbaz, A. and Funk, A. (2020). Freedom on the Net 2020: The Pandemic's Digital Shadow. *Freedom House*. <https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow>

Still, judges in Brazil, Estonia, Germany, and South Africa have managed to reduce government surveillance powers.<sup>54</sup> Moreover, some laboratories of American democracy hold promise for a new democratic model. Just over 14 municipalities have passed surveillance ordinances and reasonably succeeded at improving transparency and oversight in the acquisition and use of technology.<sup>55</sup> Meanwhile, 13 states have amended their constitutions to prohibit the unreasonable search and seizure of “the person, houses, papers, possessions, *electronic data, and electronic communications*” (emphasis added).<sup>56</sup> In January 11, 2021 the Federal Trade Commission settled its first case tackling facial recognition misuse and customer deception with Everalbum, Inc., a California-based photo app that agreed to delete facial recognition models, algorithms, and data.<sup>57</sup> However, specific attention is needed on the acquisition and use of digital surveillance in the United States and across the world.

This report is an attempt to amplify ongoing efforts and find common ground for a new democratic approach to surveillance. Democracies must offer a better path forward—one that can withstand the dynamism of emerging surveillance technologies and be emulated by the digitizing world.

---

54 Ibid.

55 Fidler, M. and Liu, L. (2020). Four Obstacles to Local Surveillance Ordinances. *Lawfare*. September 4. <https://www.lawfareblog.com/four-obstacles-local-surveillance-ordinances>

56 Ebert, A. (2020). Michigan Passes Warrant Requirements for Electronic Data Searches. *Bloomberg Government*. November 4. <https://about.bgov.com/news/michigan-passes-warrant-requirement-for-electronic-data-searches/>

57 Errick, K. (2021) “FTC Settles Facial Recognition Misuse Suit with Everalbum” *Law Street Media*, January 11, <https://lawstreetmedia.com/tech/ftc-settles-facial-recognition-misuse-suit-with-everalbum/>

# Stakeholder Synthesis

This report involved interviews with 40 out of the 53 contacted stakeholders across government, academia, civil society, industry, and law enforcement (See Appendix A for list of participants).<sup>58</sup> Average interview length was estimated at 51 minutes. Stakeholders were asked to discuss generally their vision for a more responsible, democratically accountable surveillance model, the transparent acquisition and accountable use of surveillance technology, and innovation and global competition challenges (See Appendix B for complete list of questions).<sup>59</sup> Representatives spoke freely and with the understanding that their shared perspectives would be aggregated under the applicable stakeholder category and that the report's policy recommendations did not necessarily reflect their own viewpoints. Several stakeholders provided feedback to an initially synthesized draft.

This section first provides a summary account of four key discussion areas that developed in interviews: a harm-reduction approach to surveillance, obstacles to the democratic accountability of surveillance, suggestions for greater federal leadership and coordination, and strategic, international policy concerns. Second, this section represents a total of 42 insights and recommendations for surveillance reform, specified to each type of stakeholder.

## **Harm Reduction Approach**

Surveillance undermines the privacy of everyone, but not equally. Marginalized communities have endured the brunt of government surveillance, which is why most citizens remain unaware, unaffected, or disinterested in the acquisition and use of surveillance. A white, wealthy or other privileged individual has not and will not experience comparable intrusions on privacy from a system of surveillance that indigenous and people of color, formerly or currently incarcerated, dissident, nonconforming, activist, welfare populations, and other less-privileged communities have been forced to become accustomed to. Civil society and academic stakeholders said that these disproportionate costs have never been borne equally, dating back to even before the first "lantern laws" that required black and indigenous bodies to remain illuminated at night in 18<sup>th</sup> century New York City.<sup>60</sup>

With this context, many civil society stakeholders were skeptical over the possibility of a responsible system of surveillance. One stakeholder explained that there are very few occasions where civil society has gained access to government procurement and use of surveillance technologies; in every circumstance, the uncovered operations have mapped exactly onto the racial overlay of the cities—as specific as the railroad track dividing a surveillance-free white community from a black neighborhood. The same is true online, where the dividing line becomes certain social media hashtags like "#BLM" instead of "#MAGA." Another stakeholder maintained that surveillance can never be legitimate as it is a process fundamentally designed to exact violence; surveillance operates within the context of a broader, oppressive white supremacist hierarchy and will therefore always be used to track black and brown bodies. In contrast, law enforcement stakeholders viewed the deployment of surveillance as confounded by a catch-22. Justifying the use of surveillance technologies in suburban neighborhoods, which are comparatively much more spread apart

<sup>58</sup> Some interviewed stakeholders asked to remain unlisted.

<sup>59</sup> A full list of questions can be found in Appendix B.

<sup>60</sup> Garcia-Rojas, C. (2016). The Surveillance of Blackness: From the Trans-Atlantic Slave Trade to Contemporary Surveillance Technologies. Truthout. March 3. <https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police/>

and concerned with less-serious parking or noise complaints, is quite difficult, especially when urban or minority communities are requesting better monitoring to reduce crime.<sup>61</sup> Still, there was recognition among law enforcement stakeholders that the surveillance system—perhaps policing overall—needs to change to involve greater public input. For far too long, law enforcement has policed communities the way it believes communities should be policed, rather than the way the community has asked to be policed.

While one civil society stakeholder advocated against reform by emphasizing that only the abolition of surveillance could ensure violence does not persist, the overwhelming majority of stakeholders subscribed to the pressing need for a more immediate, harm-reduction approach to designing a liberal-democratic surveillance system.

This alternative must be rooted in the protection of people, and must firmly distinguish between targeted and mass surveillance, the latter of which should be banned outright. Targeted surveillance would require the government to meet specific warrant standards based on individualized, fact-based suspicion of wrongdoing that is proportionate to the requested intrusion on privacy. Warrant requests would be judicially reviewable and, in time, unsealed for public scrutiny to create transparency on how the surveillance request was interpreted, what was authorized, and what was ultimately performed. Novel warrant types, such as sweeping geofence warrants, should merit additional scrutiny and narrow tailoring. Biometric identification through surveillance technologies should not suffice to justify an arrest, but rather be treated as an investigative lead to be corroborated by independent evidence.



Government use of surveillance technologies should be disclosed by police and prosecutors. Adequate, independent reviews and assessments prior to and after use should be performed. Industry stakeholders recommended that to heighten trust, vendors should provide complete transparency over where data is routed and stored. **Law enforcement stakeholders emphasized that it is in the best interests of the 18,000**

<sup>61</sup> Several law enforcement stakeholders cited specific instances where neighborhoods asked for cameras to ‘clean up the drugs and guns’ and they resulted in a series of arrests, a reduction in crime, and positive response from the community.

**law enforcement agencies to strive to inform the public as much as possible without compromising investigations;** surveillance comes at the cost of the taxpayer, and there are duties to install strong policy, training, and accountability as guardrails rooted from the perspective of other community stakeholders. Civil society and academic stakeholders emphasized that such a system of surveillance must center the voices of historically surveilled communities in any policy of reform. Meaningful community representation is the only way to navigate the diverse ethics and effects at play.

Any entity using surveillance should be required by law to inform and seek the input of the public on clearly defined use-policies and intended use-cases (i.e. which community problems are being solved), how data will be stored, retained, and secured, and what independent auditing and performance-review procedures are in place. Rather than one single actor, a range of local actors—the mayor, city council, police chief, public advocates, and others—should be informed and charged with some responsibility for public communication. This would protect against institutional capture and empower each actor to be an honest broker of information, even if they disagree with policies in place.

### **Obstacles**

All stakeholders identified a variety of obstacles contributing to or preventing the reduction of harm in the surveillance technology acquisition and use process.

**Information Asymmetries:** Three types of information asymmetries currently preclude transparency and democratic accountability.

- » **Technical:** A gap in understanding exists between industry and society over how surveillance technologies operate and what is possible.

Government, law enforcement, academic, and industry stakeholders noted that police and city officials are often not technology professionals and may not be equipped to comprehend the impact of new technologies. Surveillance vendors can sensationalize their tech to persuade comparatively less-informed law enforcement to adopt this technology in order to stay modern and relevant. Despite a large source of demand coming from government use, the surveillance market is supply-driven, occurring often by sole-sourced contracting (i.e. where municipalities operate under the assumption—or operational constraint—that only one company can meet agency needs).

**Some industry stakeholders said self-regulation within the current competitive environment will not work,** as companies will capitalize on these information asymmetries and promote a sense of technology solutionism even when it may be harmful for keeping long term demand alive. Other industry stakeholders asserted that the societal gap in technical understanding has created hysteria that does not reflect the actual state of the technology, resulting in short-sighted bans.

Civil society stakeholders also highlighted how consumers understand little about the downstream data flows that arise from private data brokers (e.g. advertising tech companies, business IT, risk data aggregators etc.) selling user data to government entities.

- » **Contractual:** The acquisition and use process contains very little inherent or obligated transparency.

Law enforcement, academic, civil society, and government stakeholders emphasized how the presence of NDAs, trade secrecy claims, and non-existent reporting requirements in public-private contracts reduce oversight. Police reports will often leave out the specifics of technologies

utilized in an investigation, preempting possible court appearances and creating additional barriers to effective defense of the accused.

Government stakeholders explained that there are only four local levers of transparency: anti-corruption rules, federal grant transparency requirements, Freedom of Information Act (FOIA) requests, and surveillance ordinances. While FOIA requests and surveillance ordinances, are either profoundly slow and burdensome to requesting parties or are not in widespread use, respectively, the other two levers have provided transparency by accident. First, anti-corruption rules require city council signoff in sole-source contracts have heightened oversight over surveillance technology acquisitions.<sup>62</sup> But as the market for surveillance grows with more vendors, the assumption that only one company can meet agency needs will decrease, along with sole-source contracting and mandated city council signoff. Second, federal grants sometimes shed light on local acquisitions, but they are far from intended to introduce transparency.

**All stakeholders acknowledged that due diligence assessments can play a better role.** At present, these assessments are trust-building exercises, an impetus for thinking about specific issues like disparate impact, but not meaningful rights-protective guarantees. Civil society stakeholders called for more assessments earlier in the design and use process, while industry stakeholders explained that many companies will not think about these assessments because they are not required for design. There is also a fundamental gap in the cost-benefit framework needed to truly evaluate these technologies. More synchronous information between use-policy and use-case is needed to evaluate surveillance operations' ability to solve community problems.

- » **Legal:** The legal system is not an effective oversight mechanism, partly due to asymmetric information flows.

Nearly all stakeholders agreed that the warrant process is not equipped for modern day technologies. The highest warrant standards are required for wiretapping, which includes a warrant and a showing that other less intrusive methods have been exhausted. However, email access, location tracking, and other hi-tech surveillance technologies do not entail similar safeguards. Some methods, such as a 'tower dump', which grants access to the location and other data of phones connected to the cell tower, do not require any warrants. Moreover, approved warrants often fail to adequately describe the technologies in use. One industry stakeholder pointed out that practical obscurity is disappearing with new technology, and there are severe risks of overcollection and downstream data misuse.

Most stakeholders felt that judges are not playing the role they should be in terms of scrutinizing warrant applications, in large part because they lack more technical understanding and do not involve trusted third-parties who may provide more perspective, such as the use of tech-savvy amici or clerks.

Academic stakeholders described how, under the auspices of protecting the sanctity of ongoing investigations, most warrant applications remain sealed. However, these warrants continue to be sealed even after the trial has ended, limiting any oversight offered by FOIA requests. With FOIA statutes already containing strong law enforcement exceptions, accessing these warrant applications is nearly impossible.

Civil society and academic stakeholders also pointed out that, in tandem with the widespread use of NDAs in public-private contracts, the Supreme Court's ruling on Exemption 4 for FOIA requests in *Food Marketing Institute v. Argus Leader Media* (2019) strengthened the government's ability to deny requests that may uncover "trade secrets and commercial or

<sup>62</sup> Salac, L. S. (2008). Terms and conditions to winning a contract with government projects. Paper presented at PMI® Global Congress 2008—Asia Pacific, Sydney, New South Wales, Australia. Newtown Square, PA: Project Management Institute.

financial information obtained from a person [that is] privileged or confidential.”<sup>63</sup> Thus, already burdensome FOIA efforts may have an even higher likelihood of denial with respect to surveillance technologies.

Academic stakeholders also pointed to the existing Department of Justice’s (DOJ) interpretation of the Stored Communications Act (SCA), the key privacy law for the Internet, which precludes criminal defendants, not prosecutors, from accessing online communications, even if such data could exonerate the wrongfully accused.

**Destructive Habits and Beliefs:** Five commonplace beliefs and actions militate against reform.

- » **Failure to Appreciate Next-Gen Surveillance Technology’s Transformational Nature:** The legal and political systems have not grappled with the new state of play within which these technologies are proliferating. As industry stakeholders highlighted, **surveillance technologies are getting better, cheaper, and easier to use every year.** One industry stakeholder reminisced that it used to be that only elite, well-funded organizations were using facial recognition technology and, ostensibly, these organizations had far more sophisticated identification units to use the technology more properly. Now, startups can build and supply this technology, even by illegal means, to a far less advanced operating criteria, while oversight measures are only just starting to truly appreciate these issues.<sup>64</sup> Still, **the surveillance industry is complex and multilayered—there may be three, five, or more companies involved before the technology reaches the end-user.** It is also an internationalized industry, and there is little attention paid to the supply chains of U.S. surveillance imports. One industry stakeholder pointed out that leading companies may be using Russian subcontractors, which creates an additional set of vulnerabilities for malicious state actors seeking to undermine American security and privacy.

The overwhelming majority of stakeholders agreed that the legal system has fallen 10-20 years behind sound regulation of technology. One academic stakeholder pointed out that the commercialization of data has created end-runs around privacy laws, with government access through third-party leakage, leading Senator Ron Wyden to recently introduce legislation dubbed “The Fourth Amendment Is Not For Sale.”<sup>65</sup> Moratoria on certain technologies are a great start for several stakeholder types, but still, to most, these bans are a short-term fix. **The social costs of surveillance technology’s misuse—by operation or design—are enormous and can ruin lives, and yet very little regulation exists to rein in the incentives of surveillance capitalists.**<sup>66</sup> If there is no common framework for addressing new technologies, then the vague set of ethical constraints on a widening, uneven playing field will continue to proliferate undemocratically.

- » **Mission Creep and Corruption:** Academic and civil society stakeholders pointed to history, in which there are countless examples of one administration standing-up ostensibly sound process safeguards, only for the policy or legal structure to be misused or eliminated by a later agency or eliminated by a later administration.<sup>67</sup> The development of a better surveillance alternative will likely be no different. **A responsible system must endure changes in power or culture by the will of the people and communities most affected.** The recent decision by Singapore to use COVID-19 track-and-trace data for law enforcement purposes highlights the ease by which democratic oversight can disintegrate.

63 See *Food Marketing Institute v. Argus Leader Media*, 139 S. Ct. 2356 (2019).

64 Errick, K. (2021) “FTC Settles Facial Recognition Misuse Suit with Everalbum” *Law Street Media*, January 11, <https://lawstreetmedia.com/tech/ftc-settles-facial-recognition-misuse-suit-with-everalbum/>

65 Canales, K. (2020) “Sen. Ron Wyden is introducing a privacy bill that would ban government agencies from buying personal information from data brokers,” *Business Insider*. August 4, <https://www.businessinsider.com/ron-wyden-fourth-amendment-is-not-for-sale-privacy-2020-8>

66 Zuboff, S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, (New York City: PublicAffairs, January 15).

67 A recent example was the Trump Administration’s use of Obama-era Homeland Security Advanced Research Projects Agency’s surveillance infrastructure for more invasive immigration enforcement.

» **Public Apathy:** As one law enforcement stakeholder pointed out, “most individuals are not affected by surveillance.” Government, academic, and civil society stakeholders said this unequal interaction results in the tendency for citizens to underappreciate the truly invasive potential of surveillance technologies. As the surveillance market develops, the technologies may become less visible, or at least less of an issue to those unaffected. Meanwhile, many believe that government cannot adequately ensure the digital rights and liberties of citizens against Big Tech, disincentivizing organizing efforts.

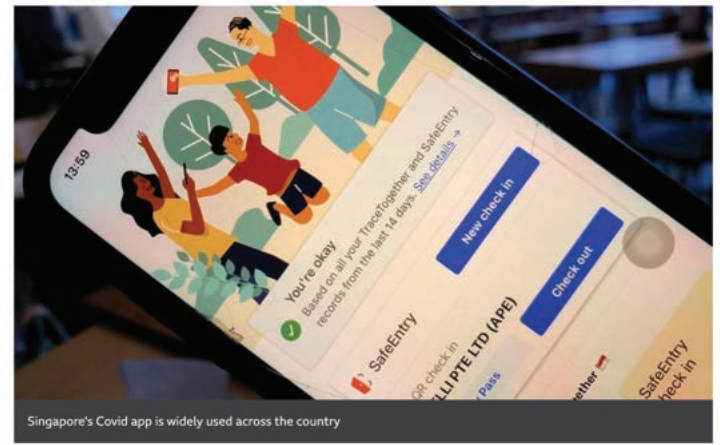
- » **Top-down Policing:** Law enforcement stakeholders, along with all others, highlighted the need for increased community input in making decisions, especially on surveillance. They stressed that public trust is essential for achieving public safety. But trust has been shattered by immense public scrutiny and criticism in part because of a failure to involve the community in rolling out initiatives. Still, across the 18,000 U.S. police departments, often with surveillance data and other types of support from agency partners, many still believe that secretly deploying technologies and failing to include opposing viewpoints is the best approach.
- » **Permissionless Innovation:** As industry stakeholders noted, whether in the training phase or in the deployment phase, there are opportunities for bias to creep in. **With newer companies entering competition, it has become more important than ever before to verify the developer.** And yet, many companies operate without—or cannot afford—ethics review or similar oversight and advisory boards. A cottage industry of tech-verification companies has cropped up, filling in the gap left by the government with rubber stamps. Civil society stakeholders pointed out that, even in companies that do have oversight processes, they are often not centered in the design stage or are not representative of the communities who will be impacted by their technology.

## Singapore reveals Covid privacy data available to police

By Andreas Illmer  
BBC News, Singapore

5 January

Coronavirus pandemic



Singapore's Covid app is widely used across the country

Singapore has admitted data from its Covid contact tracing programme can also be accessed by police, reversing earlier privacy assurances.

**Development and Verification Limitations:** Existing evaluation processes are insufficient to ensure equitable outcomes.

- » **Measurement Process Limitations:** While all stakeholders acknowledged the need for improved transparency and due-diligence assessment requirements, several civil society stakeholders noted that adequate measurement may be a limited possibility. Facilities designed to monitor algorithms suffer from domain transfer issues; algorithms are tested in labs, a completely different setting than the lighting, angle, and other conditions of live-feed footage from a bridge. **The ability to transfer insights from the lab to the real world remains quite difficult.** Industry stakeholders emphasized that current testing is limited to object code verification, which evaluates the code structure of algorithms, and does not provide sufficiently secure structures for companies to hand-over their source code (i.e. the valuable training architecture and data) for review.
- » **Absence of Cost-benefit Analysis:** Academic, civil society, and government stakeholders were vocal about the absence of methods to formally assess the benefits of surveillance technologies. Metrics are not defined universally, making it increasingly harder to ensure consistent oversight and accountability.

## Federal Coordination

Considering the piecemeal roll-out of surveillance ordinances, most stakeholders acknowledged the potentially important role of the Federal Government to expand protections to citizens. While direct federal involvement in the police activities of states and localities is constitutionally restricted, a range of actionable solutions were identified by stakeholders. Academic, government, and civil society stakeholders also highlighted that Federal Government coordination has historically posed an existential threat to a democratically accountable surveillance system. One civil society stakeholder explained how the massive federal and state law enforcement information-sharing web (e.g. Homeland Security Information Network, Law Enforcement Online, FBI Guardian etc.) has created an inefficient, “collect-it-all” mentality with respect to gathering data. Moreover, there is reasonable risk that industry or law enforcement lobbying could capture federal policy and preempt stronger oversight at the state level. Still, government stakeholders expressed frustration at the piecemeal progress of surveillance oversight, as it takes immense resources to engage other localities one-by-one. **Even for municipalities with technology hubs and tech-savvy labor forces, ensuring the digital justice of citizens has been a heavy lift.** All stakeholders in favor of greater coordination, including law enforcement stakeholders, emphasized the vital importance of the Federal Government in setting a floor, rather than preempting stronger oversight efforts in municipalities.

- » **Standards:** All stakeholders believed that the Federal Government could provide harm-reduction value by introducing soft-law standards, which often trickle down to municipalities. Standards can level and reorient the playing field towards privacy-preserving considerations. A non-exhaustive list might include guidance through deidentification toolkits, data security and retention protocols, clarifying training requirements and use-case bright lines, evaluation mechanisms for surveillance technologies as a verifiable forensic tool, standardized prohibitions of NDAs in public-private contracts for technologies proliferating at municipal levels, and an ethical component to placement decisions on the FBI preferred vendors list. Industry stakeholders said that having a floor would help innovate with direction. For example, companies could benefit from clearer guidelines on handling erroneous capture of data and appropriate deletion and retention policies.
- » **Conditioning Grants:** All stakeholders recognized the large proportion of funding from federal grants such as the Department of Homeland Security’s Urban Areas Security Initiatives (UASI), DOJ’s Justice Assistance Grants (JAGs), and Operation Stonegarden. Academic, civil society, and government stakeholders promoted the idea of conditioning these grants on the installation of meaningful surveillance oversight infrastructure, or at least creating more follow-up on the use of federal money. As many existing oversight efforts are staffed by volunteers, like in the City of Oakland, stakeholders suggested apportioning part of the grant funding towards standing up accountability infrastructures.
- » **Privacy Laws:** Academic and government stakeholders emphasized that appropriately securing a transparent, accountable system of surveillance across the country will require data privacy legislation fit for the 21<sup>st</sup> century. Some stakeholders stressed the importance of comprehensive legislation and made references to both Republican- and Democratic-held Senate bills.<sup>68</sup> However, they also appreciated that partisan issues related to an individual private right of action and state preemption have held up legislative action. While many stakeholders were hopeful for comprehensive legislation in the coming months, many also suggested more immediate oversight via more sector-specific and bipartisan biometrics data privacy legislation.
- » **Realigning Innovation Incentives:** While industry stakeholders were wary of increased regulation, many felt that the market would stabilize around a sensible realignment towards privacy-preserving considerations. Nearly all stakeholders agreed that the Federal Government could at least provide more signals to industry for innovating responsibly, if not prohibiting problematic technologies altogether. Banning indiscriminate mass surveillance is a great place to start; it would set the tone against a competitive race to the bottom. The Federal Government could also leverage competitions

<sup>68</sup> Republican: Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act (S.3663); Democrat: Consumer Online Privacy Act (S.2968)

and contests towards certain privacy-preserving ends. **As an internationalized surveillance market makes trustworthy verification of the algorithms more important, it may become necessary to design new methods of review.** Having a clearinghouse to verify products and handle the range of actors and explosive demand within the surveillance industry is the future. However, without a safe, reliable reviewing organization, companies will be loath to accept certification oversight.

### **Strategic International Policy Considerations**

Almost all stakeholders acknowledged the grave threats to democracy and human rights posed by the worldwide proliferation of surveillance technologies. Below are a set of key concerns from different stakeholders:

- » **Competing for International Standards:** Government stakeholders explained how too much of the surveillance-proliferation conversation has focused on the country-sources of rights violations, instead of universal, standards-setting efforts. Such conversations often ignore that many Western countries—Italy, Israel, Japan, Britain, the United States, and perhaps more—are home to companies that have also contributed to the export and abuse of surveillance technologies around the world. Meanwhile, in the United States, the use of surveillance has been oppressive towards marginalized communities without much, if any, democratic oversight. Such hypocrisy continues to undermine Western leadership for promoting the responsible use of surveillance, especially since mistrust in the United States is still palpable from Snowden’s 2013 domestic and global surveillance revelations.<sup>69</sup> Still, industry stakeholders were particularly fearful of the normative standards to come from the emerging market dominance of countries like Russia and China. They pointed to particular concerns over countries exporting this technology and offering installation and training services for “free,” in exchange for importing countries’ biometric data. China-based companies have proposed standards over storing results from the analysis and recognition of traits of race in the use of surveillance technologies without any serious competition from Western-based companies.

According to government and academic stakeholders, rather than shaming companies from certain countries, **a better approach would be to create a visible, gold-standard use-case operating procedure and governance structure. Companies then, with clarity, be held responsible and innovate safeguards with appropriate frameworks in mind.** Some academic stakeholders also referenced how COVID-19 has revealed democratically compatible use-cases of surveillance when proper oversight procedures are in place, like in Taiwan and South Korea. Some civil society stakeholders saw a larger role for U.S. companies, such as providing protective nudges against misuse as the second half of the world comes online. Should the United States become a player, then standards-setting efforts would carry more weight. Additionally, America could raise the industry bar in terms of proliferating shared knowledge, more consideration of human rights and ethics, and the upskilling of employees. However, industry stakeholders suggested that there is a lack of information impeding effective, global accountability. Considering the range of systems integrators and international distributors, the initial manufacturer of surveillance technology may never know the end-user.

- » **Remaining Non-Competitive:** Other civil society and academic stakeholders disagreed. Unless there is some reason to believe in unique use-protections built into Western surveillance tools, the U.S. surveillance industry should not attempt to compete in this market. One civil society stakeholder viewed the fears of growing authoritarianism as a tool of imperialism to corner markets. They advocated for another approach, namely promoting local organizing in a domestic and international context, by setting a precedent and generalizing lessons learned from these efforts. However, industry stakeholders explained that there may be unique design controls to prevent abuse, as companies will have to make decisions over who has access and control over data, which data is stored and for how long, and what are appropriate use-cases and controls for their technology.

69 Hayden, M. (2014). Is Internet in danger of becoming ‘splinternet’. CNN Opinion. February 14. <https://www.cnn.com/2014/02/14/opinion/hayden-splinternet-snowden/index.html>

- » **Data Harvesting for Market Advantage:** Academic stakeholders said there is vast heterogeneity within the data ownership and other provisions in international contracts. The asymmetry in technical product expertise plaguing U.S. police departments is also apparent in countries importing this technology. **Unless countries are careful in how contracts are written, there is significant cause for concern over the siphoning of countries' biometric data at mass scale.** Industry stakeholders emphasized the market incentives for harvesting data are immense and offer a virtuous cycle of growth to exporting companies, who can continue to refine and profit from products tailored to particular end-users. At the national and international level, more efforts should be made to promote legal and technical frameworks that govern surveillance through meaningful considerations of proportionality and democratic oversight.
- » **Siloed Policy Efforts:** Government and academic stakeholders also acknowledged that policy and research are often siloed, especially within each domain. For example, State Department efforts aimed at internet freedom and digital rights, cyber conflict and security diplomacy, countering disinformation, or international AI standards operate with tangential but little coordination. The Department of State's recently approved Bureau of Cyberspace Security and Emerging Technologies (CSET) bodes well for strategic coordination.
- » **Careful, Nuanced Multilateral Efforts:** All stakeholders who commented on foreign policy agreed that careful, thoughtful coordination among allies is needed. Some stakeholders advised on the multilateral, non-mandatory approach of export controls in the Wassenaar Arrangement (WA). Others noted that previous implementation of controls through the WA regime suffered from poor definitional efforts and remain ill-equipped to handle the nuanced, rapid spread of this technology. Indeed, government and academic stakeholders pointed out that subnational actors appear to be a large driving source for demand of this technology. **High-level principles or codes of conduct may be unlikely to affect decisions made at this subnational level, where one person's "surveillance" may be another person's solution to traffic congestion, waste management or crime.** The best approach is designing a better modus operandi: if surveillance solutions entail the use of data analysis and acquisition, identify parts can be done in ways that don't violate civil liberties and human rights.

# Stakeholder Recommendations

## Academia

Academic stakeholders provided **six** specific insights and recommendations for reducing harm in the acquisition and use of surveillance technology.

- 1. Improving Transparency:** The burden of public information access should be moved off the shoulders of entrepreneurial journalists and activists filing public records requests. Government should publicly display documents such as memorandums of understanding (MOUs), contracts, and licensing agreements.
- 2. Leverage the Power of the Purse:** City councils should demand that public-private contracts are written without the use of NDAs, except in extremely rare cases. City lawyers should ensure that such contracts do not cede the power of data away from citizens. Some stakeholders believed the municipality itself should become the data holder. Others were concerned about the ability of the government to ensure data security and believed, with limitations and access guarantees, outsourcing to private enterprises was the best option. No academic stakeholders believed police departments should be the sole data holder.
- 3. Citizen Access to Data:** Governments should provide a single-source access and a mechanism to verify their non-investigative criminal records data, such as pre-conviction mugshots. Otherwise, the surveillance most felt by individuals—the lack of accurate expungement after arrest—will continue to unnecessarily contribute to structural disadvantages in background checks, housing, and employment.
- 4. Private Right of Action:** The right to sue is essential to the successful enforcement of surveillance ordinances, and could take place through class-action lawsuits, for example, in the event of the breach, misuse, sale, or overcollection of public surveillance data.
- 5. Portable Oversight and Governance Designs:** Companies should engineer legal and technical firewalls to increase oversight and protection against abuse, gain market advantage by offering guarantees of data privacy, and enable the technology to become *more* compatible with the principles of liberal democracy.
- 6. Multilateral Export Controls:** Some measure of export controls is needed to gain more of a grip on the spread of digital surveillance technology's misuse. As the United States is not the *de facto* global leader of surveillance technology, there was consistent agreement that such approaches will depend on relationships with other leading nations such as Israel, Italy, Japan, and France.

## Civil Society

Civil society stakeholders provided **eight** specific insights and recommendations for reducing harm in the acquisition and use of surveillance technology:

- 1. Limiting Data Retention:** Once data is persistently accessible, it matters little if the conversation is listened to instantaneously or at a later date. Surveillance in its present form will change the behavior of all, especially marginalized citizens; it can and will be used to target whistleblowers and political dissidents to find something to charge them with and can be repurposed from counterterrorism to immigration. Limiting the retention of data is essential to maintaining freedom of expression. From privacy and security perspectives, too centralized storage of too much data could easily create jackpots for public interest,<sup>70</sup> malicious, or foreign government hacking. Most, if not all, civil society stakeholders were wary of law enforcement as the sole public surveillance

<sup>70</sup> See 'BlueLeaks' hack of a law enforcement's data-sharing portal contractor, in which ten years of data across 200 police departments, fusion centers, and law enforcement facilities were publicly released.

data holder. Preferably, a neutral, non-profit third party capable of guaranteeing the security of surveillance data should become the data holder. Alternatively, companies should hold data, with explicit guarantees of limited retention and no-repurposing, including for commercial use or for agencies not enumerated in the contract.

- 2. Resist Technology Dependencies:** When large companies offer products for free, and even abstain from repurposing data, there is still a real risk of dependencies and contractual lock-in developing. Agencies may find themselves dependent on these technologies for operations, and the private incentives that exist are far from privacy-preserving. In fact, financial incentives may encourage the overcollection of data. A stakeholder noted how one company provided free Automatic License Plate Readers (ALPRs) to locate and require the onsite payment of individuals with outstanding government fees, for which the company receives a \$40 cut. To this extent, it is imperative that there isn't only one dominant vendor in each sector of the surveillance supply-chain—from cloud infrastructure to operational hardware.
- 3. Set the Tone for Oversight:** City councils should pass moratoria on digital surveillance technologies including but not limited to facial recognition, police drones, and others. They should also adopt surveillance ordinance legislation. Elected officials should take the budgetary opportunity seriously and use it to ask questions that create more of a transparent culture. They should also work with the public and police departments to set the tone, structure, investment, and resources for a developed oversight system that would last beyond any single administration. The bare minimum would be to establish notice-and-comment rulemaking and periodic audits to evaluate how information is shared and if civil rights and liberties are violated. Cities should ban the use of NDAs in public-private contracts, except for highly specific cases as defined by the legislature.
- 4. Require Effective, Public Due Diligence:** Systems should be required to undergo annual, public assessments. More synchronous information between use-policy and use-case is needed to effectively evaluate surveillance operations. On the industry side, a pilot study proving efficacy and a longer pilot equivalent confirming non-discrimination would be very useful. On the government side, evaluation of the intended and implemented use cases, proposed benefits and empirical crime reductions, and privacy and civil liberties intrusions across racial and socioeconomic spectrums should become routine.
- 5. Warrant Applications Need More Scrutiny:** Judges should ensure the information in warrant applications is accurate and work to improve their appreciation for the new, invasive potential of surveillance technologies. They should be willing to invite trusted third parties to brief warrant applications, entertain suppression of evidence challenges, support conferences aimed at improving edification, resist sealing warrant requests that indicate the scope of surveillance, and do away with parallel construction procedures. One civil society stakeholder pointed out, however, that solving all of these issues is likely outside the authority of judges. For example, they recommended a smarter approach may be to incentivize law enforcement to avoid or ban parallel construction.
- 6. Private Right of Action:** Citizens should not be burdened with the responsibility of ensuring their own rights and liberties are protected, especially in the recovery from COVID-19. However, those with the resources and time should be empowered with legal standing to ensure agency adherence to established guardrails, including in the event public surveillance data is compromised. Citizens should have visibility over the collective set of grievances and a clear path to address them. This also requires having the rights to access and delete public surveillance data about themselves, paralleling the General Data Protection Regulation's (GDPR) right to erasure.<sup>71</sup>

71 "Guide to the General Data Protection Regulation" *Information Commissioner's Office*, January 2021, <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf>

- 7. Ethics and Equity in Product Design:** Companies should bake ethics and equity into engineering or adjacent development teams via installed product safeguards, proposed use cases, and increased privacy and civil liberties perspectives. Given the invasive potential of these technologies, an ethics board should become a requirement of public-private contracting. Companies should also support and participate in transparency by ensuring sufficient knowledge about capabilities and limitations of their systems and granting access to data when requested by the right parties.
- 8. Multilateral and Better-informed Export Controls:** Controls should be enacted in partnership with the E.U. approach as the regimes are not coordinated. At present, AI firms have very little restrictions with gaining funding or developing other partnerships with bad actor nations. The Department of Commerce's Bureau of Industry and Security (BIS) should also publicly disclose knowledge of supply chains for entity-listed companies to increase efforts aimed at discerning potentially alternative means of developing the technology.

## **Law Enforcement**

Law enforcement stakeholders shared **ten** specific insights and recommendations for reducing harm in the acquisition and use of surveillance technology:

- 1. Surveillance is Important for Public Safety:** Surveillance is a crucial component of the ability to deter and chase crime. If there is reasonable suspicion or probable cause to believe a criminal act is being committed, then it becomes important to be able to use tools of surveillance. But it would be a waste of resources to randomly surveil the population. Most individuals are not affected by surveillance, and most officers do not go out with the intent to cause harm. They are making quick decisions in response to rapidly changing environments that will and should be reviewed for misconduct and lessons. Retaining the supervisory ability to review, through immutable footage records, is an important part of the oversight process.
- 2. Transparently Tie Acquisition to Use Policies:** Law enforcement should state publicly what technologies are in use, which vendor(s) are being considered and are selected, generally when and where deployment is taking place, and how the data will be managed. Certain information, such as the particulars of a system or their exact locations, might need to be made confidential to avoid vulnerabilities via hacking or crime relocation. Still, the government should provide sufficient time and avenues for public discussion prior to the acquisition and use of the technology. In circumstances when law enforcement has created policies with civilian input, there has been more credibility and less tension.
- 3. Public and Equitable Accessible to Information:** Some stakeholders recommended publishing information on types of equipment and use policies online, but also providing alternative information sources like calls and public meetings for communities without reliable Internet access.
- 4. Leverage Market Demand:** Law enforcement should require companies to meet threshold requirements based on community input. For example, public-private contracts might require unfettered access to public surveillance data without additional fees and ensure this data is machine-readable and easily exportable. Law enforcement may choose to procure only from companies who have public interest or ethics boards and are willing to participate in transparency measures with the community.
- 5. Public Surveillance Data is Sensitive and Should be Secured:** Data access should require background checks and should only occur in "read-only" format. If companies are the data holders and a breach occurs, a civil remedy should follow; if law enforcement are the data holders and intentional misuse occurs, penalties such as loss of employment should be considered. Decisions about when to release data can involve other stakeholders, but the authority should ultimately reside within the police agency. An MOU would be needed to clearly delineate the process of evidentiary release.

- 6. More Judicial Oversight:** Judges should be knowledgeable about what constitutes responsible surveillance and what does not, from a standpoint of probable cause and proportionate use that considers an individual's actual expectation of privacy.
- 7. Surveillance Ordinances and Collaboration Can Help:** City councils can and should pass surveillance ordinances. Elected officials should also be knowledgeable and prepared to ask tough questions and collaborate with law enforcement on promoting civic engagement and designing a more responsible use policy. Oversight boards could become more mainstream but should be careful not to compel the release of information that could damage an investigation.
- 8. Private Right of Action:** Citizens should be able to directly hold the government accountable, but this should be reserved for egregious cases (e.g. successful suppression of evidence should not entitle a right to sue). There should not be a new legal regime for surveillance violations, but some stakeholders suggested a surveillance complaint system overseen by an independent body.
- 9. Companies Must Meet Public Interest Concerns:** Companies should welcome transparency at the forefront, inviting stakeholders to learn how decisions and products are made. Industry should orient surveillance technologies to be instructive upon review, so officers might be able to improve decision-making not under scrutiny of a trial-stand but in a conducive training environment.
- 10. Nuanced Due Diligence:** Due diligence should measure the disproportionate impacts to marginalized communities from surveillance, and this information should be paired with knowledge on which communities requested and approved surveillance. Assessments should become a requirement of the due diligence concerns; this effort would be served well by engaging other stakeholders in a collaborative, non-adversarial role.

## Government

Government stakeholders shared **nine** specific insights and recommendations for reducing harm in the acquisition and use of surveillance technology:

- 1. New Frameworks for the Digital Age:** New surveillance statutes are needed to adequately process the tradeoffs posed by modern technologies for bystanders, targeted communities, the global Internet ecosystem, and diplomatic relationships. The Executive Branch needs a framework to handle these and more tradeoffs, because law enforcement is not equipped to represent all sides.
- 2. Municipalities Should Adopt Surveillance Ordinances:** Several stakeholders pointed to the ACLU's Community Control Over Police Surveillance (CCOPS) model, which entails mandatory transparency, annual reporting obligations, understanding of how the equipment will be used, and evaluation metrics.<sup>72</sup> There has not been a new objection to this model in years—it's always either an onerous administrative burden or concern that increased transparency will interfere with investigations. No department has made a formal request for budget increases, and many have produced requested information and reports within a single business day. In general, city councils should require and scrutinize surveillance accountability reports closely for disparate impact or any other disproportionate and material harm to the communities they serve. They should use the power of the purse to enforce proper behavior with respect to procurement and use of surveillance technology, resisting the influences of police or affluent community capture. Where possible, they should stand-up oversight infrastructures accountable to and representative of the community's interests, like a privacy advisory commission or a privacy office.

<sup>72</sup> Marlow, C. (2020). Instructions for Turning CCOPS Model Bill Into CCOPS + Facial Recognition Ban Model Bill (CCOPS + FR), CCOPS + Militarization Model Bill (CCOPS + M), or Both (CCOPS + FR/M). ACLU. August. <https://www.aclu.org/other/instructions-turning-ccops-model-bill-ccops-facial-recognition-ban-model-bill-ccopsfr-ccops>

- 3. Due Diligence Tied to Political Accountability:** Due diligence should be completed before requiring political signoff on the acquisition and use-policy of a new technology. In this way, if an elected official approves something contrary to the findings of a due diligence assessment, there is more potential for accountability.
- 4. Oversight Infrastructures Build Trust:** Law enforcement should recognize that successful crime prevention requires the legitimacy of the community. To this end, one stakeholder explained how the relationship between citizens and police is especially toxic, as the City of Oakland enters their 18<sup>th</sup> year of federal oversight. However, the Oakland Privacy Advisory Commission (OPAC) has been a candid forum to build trust and dispel rumors; it has already changed the conversation. In producing their annual reports, OPAC can—with implementation experience and real-world data—reduce the “sweet-talking” over a technology’s efficacy and the “bad-mouthing” of those who would never believe a word of the police.
- 5. Municipalities are not the Original Customer:** The most expensive surveillance technologies are first contracted to the military and intelligence community then federal law enforcement, and then state and local law enforcement. Municipal law enforcement agencies have been held responsible by other surveillance customers for drawing public attention to the gross misuse of digital surveillance technologies. There has since been a concerted effort to keep municipal law enforcement behind on the acquisition of new technologies. Within this dynamic, some companies choose to sell only to the military and intelligence agencies or federal law enforcement, to recover intensive research and development costs with expensive product prices. Other companies will sell less-advanced products to small-to-medium countries with a checkbook or municipal law enforcement.
- 6. Federal Judiciaries Should Offer Guidance to State and Local Judges:** Toolkits on current and emerging technologies, their tradeoffs, and other materials would better inform local legal oversight. Ideally, federal courts would maintain a list of suitable amicus curiae for judges at the state and local level to call upon on as needed. This resource should encourage judges to move away from approving warrant applications via *ex parte* proceeding.
- 7. Move Away from the Davis Good Faith Exception:** Perhaps the most difficult step towards a more responsible, democratically accountable system of surveillance is departing from the Davis Good Faith Exception<sup>73;74</sup> to the Fourth Amendment’s exclusionary rule. Considering the lack of substantive, responsive precedent on hi-tech surveillance technologies, already costly litigation challenges to suppress illegally obtained evidence have not been protected by the Fourth Amendment. The system is without meaningful checks and balances.
- 8. Citizens Providing Elected Officials Political Coverage:** The lack of an organized constituency has made it difficult to ensure appropriate oversight over acquisition and use. Citizens can play a role in creating the motivation for reform and ensuring elected officials can make the appropriate oversight decisions.
- 9. Plan for Data Governance Before Acquisition:** Municipalities and their police departments need to have a plan for data that may involve external data holders but ultimately enables the community to be the primary owner. It should also require probable cause before database access, whether in private hands or not. Absent federal legislation, communities may look to the EU’s recently published draft of regulating data governance following-up on the General Data Protection Regulation (GDPR).<sup>75</sup>

<sup>73</sup> If officers had reasonable, good faith belief that they were acting according to legal authority, such as by relying on a search warrant that is later found to have been legally defective, the illegally seized evidence is admissible under this rule.

<sup>74</sup> See *Davis v. United States*, 564 U.S. 229 (2011)

<sup>75</sup> See European Commission Publishes Draft Data Governance Act. Hunton Andrews Kurth LLP. December 2, 2020 <https://www.huntonprivacyblog.com/2020/12/02/european-commission-publishes-draft-data-governance-act/>

## Industry

Industry stakeholders shared **nine** specific insights and recommendations for reducing harm in the acquisition and use of surveillance technology:

- 1. Transparency is the Best Disinfectant:** Transparency should be institutionalized as a trust-building part of the surveillance system. In cases where agencies were more transparent, the payoff was tremendous; the same is true for industry, who should stop abusing trade secrets, though this can be difficult in competition. To this end, more consistent, meaningful annual assessment reports, enhanced FOIA laws or clearer disclosure processes, and awareness over agency acquisition and use should become visible requirements of a more responsible surveillance model. Points of accountability can and should be inserted into the supply chain. For example, companies' algorithms should go through verification stages measuring bias and fairness.<sup>76</sup> Once satisfied, procuring agencies' use-policies and use-cases should be assessed. The Chief of Police should communicate the roll-out and reason for the technology, the safeguards in use and guarantees over appropriate training, and the backing from independent auditing.
- 2. Surveillance Proportionate to the Severity of the Crime:** Data gathered should be commensurate with the task at hand. A facial recognition search, for example, should be within the grounds of reasonable suspicion that a crime has occurred and proportionate to the severity of the crime (e.g. for a violent crime or child abduction, not for jaywalking or loose cigarettes). Identification should not constitute probable cause for arrest, but rather an investigative lead to be corroborated by independent evidence.
- 3. Liability Should Clearly Differentiate Between Actors:** With respect to holding actors liable for misuse, there was some disagreement among industry representatives. Some stakeholders viewed a private right of action as a total catastrophe, as it was unclear if a new "terms of service" paragraph materially improved the rights and civil liberties of everyday people. Others viewed it as a central feature of systematic accountability, in line with established principles of the privacy community on the right to seek redress. All agreed, however, that in order to assign liability to the right agent, it is necessary to create clarity over differing development and deployment contexts. Outside of fraudulent or negligent actions from a vendor, integrator, or other party, the end-users of the system are ultimately responsible for using the system appropriately.
- 4. Ensuring Biometric Security and Privacy:** This involves baseline protections against hacking, but also liability in the instance of misuse or negligence. If the government is the data holder, authority over the use and release of the data should reside with the agency gathering the data, but this should take place in a controlled framework. Independent oversight into how data is used would be useful, and, where possible, it should happen via well-funded, multi-stakeholder, and resourced data privacy and protection authorities accountable to civil society. If the private sector is the data holder, they should ensure the partnering agency and respective oversight authorities are the only actors with access to the public surveillance data. Data should not be repurposed for commercial use without the informed consent of the subject.
- 5. Rethinking Warrant Regimes:** Warrants could include specific restrictions around the method, timeframe, and applicability of surveillance-tech captured data. For example, one-time searches which run through trained experts at real-time crime units may not be held to the same standard as 48-hour surveillance requests or sting operations. Judges should seek to cultivate an understanding of the state of the art of such technologies.
- 6. Promote Public Insight into the Acquisition and Use Process:** City councils might consider a local, executive analog to the federal Privacy and Civil Liberties Oversight Board (PCLOB), which would be empowered with a specialized understanding of digital surveillance issues and a responsibility to ensure citizens are represented. This might involve regular evaluations and programs to review

<sup>76</sup> E.g. for facial recognition, meeting a certain score marked by the NIST Facial Recognition Vendor Test could be required in order to contract with government

instances of misuse and abuse, detailed information on how many searches were performed, how many identifications resulted in arrest or false arrest, and what were the downstream results.

- 7. Companies Should Creatively and Willingly Meet Public-interest Obligations:** Companies might want to consider developing broad sets of principles that can flexibly configure to the varying local, state, and federal requirements over data governance and surveillance use. For example, a video management software monitoring 100 CCTV feeds on a college campus might have four categories of consent—those who have refused consent, who have given consent, the “bad actors” with previous history of committing offenses on-campus, and the unknowns who have never encountered the system before. Each group would have different privacy treatments: companies could destroy templates of non-consenting individuals, retain short-term templates of consenting and unknown individuals, and maintain bad actors’ templates over a longer retention period. Companies should also consider proactive approaches towards normalizing these considerations, such as an industry-wide association devoted to standards and ethics, which might be the best chance for sensible, innovation-friendly regulation.
- 8. Import Controls too:** Export controls are important—Western-based firms should not be profiting off human rights violations across the world. However, controls over dual-use technologies are difficult to construct as they must factor in near-impossible distinctions between civilian and government applications. Considering the internationalization of the surveillance industry, the Federal Government might consider import controls or some verification measures to limit vulnerabilities from foreign surveillance technology operating in the United States.

# Policy Recommendations

Based on the range of considerations offered by each stakeholder type, this section offers **fifteen** policy recommendations. Each is geared towards promoting the responsible use of surveillance technology with suggestions for federal, state & local, and international action.

## Federal Action

The Federal Government should lead the effort to establish a visible, cohesive, and responsible governance and oversight approach to digital surveillance. Below is an initial list of federal policy recommendations, accounting for the Constitutional restrictions precluding direct involvement in the municipal acquisition and use of surveillance technology.

### 1. Create a Digital Surveillance Oversight Committee (DSOC)

- » **Action:** Create a multi-stakeholder review panel to establish certification and recertification processes for current and emerging surveillance technologies, inform nuanced export control and strategic decisions, and compile appropriate use-cases and other relevant considerations.
- » **Description:** Numerous stakeholders called for greater federal coordination in the municipal use of technology. Rather than overstepping Constitutional boundaries by dictating state & local agency operating procedures, the Federal Government should engage in the more effective, needed approach of establishing sensible baseline regulations for the complex, multi-layered, and global surveillance industry.
- \* **Certification:** DSOC will solicit, review, and certify surveillance technology proposals from industry based on answers to an objective questionnaire (See Appendix C for working draft of questionnaire), efficacy evaluations, existing, less-invasive alternatives, risk assessment frameworks (e.g. systems' impact on privacy, potential for errors or hacking, susceptibility to unfair bias), technical product specifications, secure source-code, object-oriented, and training data audits, intended and potential use-cases, due diligence processes and designed safeguards against abuse, and product supply-chain security. Certification should become a requirement, though it need not be and could trend towards a publicly recognized expectation in localities intending to purchase surveillance technologies.
- \* **Recertification:** Every three years, companies will renew their product's certification, including any materially different updates to their technology. Recertification will be based on companies Portfolios of Operation—the better the portfolio, the faster the process.
  - o **Domestic Portfolios** might include empirical use-cases and effectiveness (including but not limited to the number of false positives and false negatives, measured crime reductions from use, disparate impact, and misuse), the effectiveness of due diligence processes, any data breaches, misuse of public surveillance data or other civil society complaints, level of transparency and public engagement, additional third-party evaluations.
  - o **Foreign Portfolios** might include entities in receipt of technology (systems integrators, international distributors, or end-users), recorded end-use violations of the technology, and installed oversight safeguards.
- \* **Centering Diverse Stakeholder Voices:** For the certification and recertification process to remain effective, members most affected by surveillance must have meaningful input. A wealth of knowledge rests with historically surveilled communities, human rights, privacy, and tech-ethicist scholars, retired law enforcement and industry professionals, and leading civil society organizations. Any trustworthy review mechanism should draw on this expertise.

- \* **Empowering Meaningful Due-Diligence:** As a clearinghouse for reviewing a range of oversight measures submitted by industry and other public stakeholders, DSOC would help revitalize due-diligence measures—a need identified by many stakeholders. It would also develop its own metrics and evaluation tools to augment more effective assessments, perhaps specific to each type of technology or something else entirely. For example, disparate impact assessments could compare the activation of facial recognition technology in cases of minority offenders to cases of white offenders, categorized by the severity of crime committed.
- \* **Compiling Intended End-Uses:** DSOC would create a repository of end-users and intended use-cases from companies' certification proposals. Over time, this would provide additional, standardized guidance to the government use of surveillance technology, creating clear bright-lines for acceptable and non-acceptable use-cases. Moreover, such a repository would create clarity over which subnational actors are driving demand for surveillance technology, ideally providing insight into demand criteria and potential engagement strategies.
- \* **Informing Export Controls and Strategic Decision-making:** DSOC would advise the Department of Commerce's Bureau of Industry and Security on targeted controls, based on its compiled set of end-use cases. This would complement public comment efforts by BIS and would provide needed information for defining end-use and end-user export controls. Over time, this could enhance BIS' capacity to exact list-based controls for certain prohibited technologies that enable particular end-uses. With greater information on export customers and end-users, it would become easier for the Department of State's Bureau of Democracy, Human Rights, and Labor (DRL) to monitor compliance with its due diligence guidance<sup>77</sup> and coordinate more targeted multilateral controls.

» **Implementation:** *Executive or Legislative*

- \* **Option 1 (Immediate):** Executive Order establishing the Digital Surveillance Oversight Committee

Gerald Ford's 1975 Executive Order created the Committee on Foreign Investment in the United States (CFIUS) to tackle the complex security threats posed by foreign investment. The Administration could similarly execute an Executive Order (See Appendix D for Draft Executive Order) commissioning the DSOC. The Secretary of Commerce would appoint the Under Secretary of Commerce for Standards and Technology to be chairman of the Committee. The Chair of the Privacy and Civil Liberties Oversight Board, the Attorney General, the Secretaries of Commerce and State would also appoint representatives from each of the following agencies:

- o **Privacy and Civil Liberties Oversight Board:** All members would be appointed with the responsibility of advising Committee decisions solely on executive branch use of surveillance technologies for civil liberties and terrorism related concerns.
- o **Department of Justice Office of Civil Rights (OCR):** This representative(s) would be responsible for engaging public stakeholders including historically surveilled communities, privacy, human rights, and technology ethics scholars, law enforcement officials, and industry to evaluate the range of civil rights and civil liberties concerns from the proposed surveillance technology.
- o **Department of Justice National Institute of Justice:** This representative(s) would contribute insights from the Developing Performance Standards and Testing Equipment program towards digital surveillance technologies.
- o **National Institute of Standards and Technology:** This representative(s) would provide recommendations based on software and hardware audits, such as secure reviews of

<sup>77</sup> U.S. Department of State Guidance on Implementing the "UN Guiding Principles" for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities, Department of State Bureau of Democracy, Human Rights, and Labor, September 30, 2020. <https://www.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/due-diligence-guidance/>

training data, source code and object review, and vulnerabilities and backdoors to data siphoning.

- o **Bureau of Industry and Security:** This representative(s) would review the integrity of proposed technologies' supply chains for security or sustainability threats.
- o **Bureau of Democracy, Human Rights, and Labor:** This representative(s) would review proposals seeking to export technology and evaluate end-use violations in recertification cases.

- \* **Option 2 (Preferred):** Legislative action to amend 42 U.S.C. § 2000ee to grant PCLOB the authority to regulate the development of digital surveillance technologies.

While PCLOB represents the perfect, agency-level vehicle for ensuring broader oversight over the acquisition and use of surveillance technologies, its competencies remain strictly limited to executive branch surveillance of terrorism. The scale of harms propagated from this issue demands immediate attention. However, over time, and legislative action permitting, the DSOC could grow into an agency-level mission under PCLOB. Membership structure should be consistent with Option 1, except with the responsibilities of chairman vested in the Chairman of the PCLOB.

**Discussion:** Many academic and civil society stakeholders cautioned against a certification regime out of fear of rubber stamping the approval of invasive technologies. Some civil society advocates, however, acknowledged that certification may be the only path forward past moratoriums, and urged technology-specific certification measures. Ultimately, all stakeholders identified the crucial need to represent the broad range of interests at play, especially for marginalized communities. Industry stakeholders viewed the DSOC, if not particularly onerous or time-consuming, as a hub for leveling the industry playing field on the basis of objective due diligence requirements.

## 2. Create a Democratic Surveillance Accelerator

- » **Action:** Design a competition-based accelerator to augment surveillance industry efforts aimed at creating portable, privacy-preserving safeguards, data governance, and end-use training and oversight measures.
- » **Description:** Coordinated export controls on surveillance technologies will not prevent the autocratic entrenchment and misuse of this technology in countries facing democratic backsliding. A more tailored, competitive approach is needed to expand liberal-democratic governance methods via market-based incentives for importing countries. This accelerator would encourage installing a set of technical firewalls and oversight measures in the surveillance technologies.<sup>78</sup> In addition to funding, 5-6 selected companies would benefit from enhanced domestic market access and provide an expedited export license to potentially backsliding countries, under a set of positive conditions. The Democratic Surveillance Accelerator is not intended to catapult U.S. leadership in the global surveillance industry. Rather, it provides an opportunity to signal to U.S. industry on certain valued design criteria, while also introducing more baseline accountability into expectations for exporting digital surveillance technologies. Export controls with these conditions would ensure that companies adhere to these values, so as to monitor and limit the contribution of U.S. technology towards rights-abusive ends.
- \* **Domestic Market:** Accelerator selection would add companies to the FBI's preferred vendors list and expedite public-private municipal requests for federal grants.
- \* **International Market:** Accelerator selection should be partial to companies with the capacity to export internationally. While all companies, Accelerator or not, would have access to global

78 O'Neal, S. O. and Clark, J. (2020). Microsoft and Open AI Comment on Advance Notice of Proposed Rulemaking (ANPRM) for the Identification and Review of Controls for Certain Foundational Technologies. Uploaded to Bureau of Industry and Security BIS-2020-0029. November 9. <https://www.regulations.gov/docket?D=BIS-2020-0029>

markets within the confines of export controls, selected companies would have the opportunity to compete in countries that may be at risk of backsliding. In addition to meeting State Department's DRL guidance to industry, like license agreements with human rights safeguards language and preventative frameworks to revoke usage rights when necessary,<sup>79</sup> the conditions for the export license to such countries should also include:

- o **Technical Firewalls:** Software features enabling real-time controls through identity verification systems and information flow controls, robust hardware requiring authorization for access (i.e. hardware identity verification through co-processors<sup>80</sup>), tamper-resistant tools, and artificially intelligent techniques designed to continuously learn, monitor misuse and lock operation where applicable.
- o **Operational Training:** Consistent with DSOC recommendations, companies should be able to provide portable and meaningful privacy and civil liberties governance training after export. This would contrast the free installation, servicing, and training provided by many companies based in China.<sup>81</sup>
- o **No Data Siphoning Guarantees:** Many digitizing countries already are walling-off digital borders to keep data in-house.<sup>82</sup> There is immense potential for U.S. companies to gain market advantage with digitizing countries by guaranteeing the security and privacy of their data.

» **Implementation:** *Legislative*

- \* Within future R&D spending, Congress should authorize an initial total of \$30 million to invest in 5-6 companies capable of meeting the demands of the Accelerator. Funding would be available only for companies shortlisted by the DSOC and selected by NIST and Defense Advanced Research Projects Agency (DARPA) based on Accelerator requirements.
- \* The FBI would update its "List of Approved Channelers" for Criminal Justice Information Services or create a new category reserved for digital surveillance technologies.
- \* BIS would grant expedited export licenses with enumerated conditions. DSOC would review, every three years, companies' Portfolios of Operation to ensure compliance with export license requirements.

### 3. Establish Portable Acquisition Standards

- » **Action:** Identify a set of key principles and standards within public-private contracts as a model for municipalities who may not have the resources and time to adequately secure relevant interests.
- » **Description:** The Federal Government retains more resources than municipalities to secure and protect democratic interests. Indeed, the gap in technical knowledge at the state & local level of government has enabled a supply-driven market for surveillance technologies. To move towards more of a demand-controlled scenario, the Federal Government should develop portable baseline requirements in their contracts with surveillance companies. Here is a sample, non-exhaustive list of such standards:

79 U.S. Department of State Guidance on Implementing the "UN Guiding Principles" for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities, Department of State Bureau of Democracy, Human Rights, and Labor, September 30, 2020. <https://www.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/due-diligence-guidance/>

80 Ibid. "Most mobile phones today include a secure co-processor with a hardware identity to facilitate secure payment. Gaming consoles have long used security co-processors to secure the console itself against unauthorized modification, to protect game authors' creations from unauthorized duplication, and to prohibit in-game cheating."

81 Clarke, R.A. and Knake, R. (2019). The Internet Freedom League: How to Push Back Against the Authoritarian Assault on the Web. *Foreign Affairs* 98.5 (2019): 185. <https://www.foreignaffairs.com/articles/2019-08-12/internet-freedom-league>

82 Sharma, I. (2020), "China's Catch-22 and the fate of the world wide web," *Responsible Statecraft*, November 11, <https://responsiblestatecraft.org/2020/11/01/chinas-catch-22-and-the-fate-of-the-world-wide-web/>

- \* Banning NDAs for any technologies also in use at the municipal level.
- \* Provision secure data governance policies, including baseline security requirements, limited retention, and no re-use or third-party use.
- \* Require performance security guarantees and companies to possess ethics review boards or other continuous due diligence processes sufficiently integrated into the design and sale process.
- \* Enable requests for companies' public disclosure of due diligence evaluations, any risks, bias, or other ethical gaps uncovered, data retention, use, and sharing policies.

» **Implementation:** *Executive*

- \* The FBI can begin creating universal contract standards in their acquisition from surveillance companies. Other agencies at the federal or municipal level applying surveillance technology can choose to follow these contract floors or create more protective and specific standards to their use-cases.

## 4. Establish Federal Privacy Legislation

**Action:** Congress should pass a federal data protection framework for how governments collect, store, and share citizen data.

- » **Description:** America has only a patchwork of sector-specific privacy laws, which creates an immense gap in regulation for the proliferation of data in the 21<sup>st</sup> century. Indeed, a failure to guarantee data privacy has led the E.U. Court of Justice to dissolve the Privacy Shield, which permitted the unrestricted data flows between the E.U.-U.S.<sup>83</sup> Several bills have been proposed but have been mired by partisan issues related to the establishment of a private right of action and the issue of federal preemption of stronger state-level privacy laws. Still, a responsible system of surveillance depends on the protection of citizens' public surveillance data.

» **Implementation:** *Legislative*

- \* The Federal Trade Commission should be mandated as the primary enforcer of data privacy legislation, in order to balance the range of economic and consumer interests.

- \* **Option 1:** Comprehensive Federal Privacy Legislation

Resolving contentious issues of state-level preemption and private right of actions may take some time, however, comprehensive legislation would introduce general requirements necessary to handle the advent of data in multiple sectors. Several bills have been or are at various stages in Congress.<sup>84</sup>

- \* **Option 2:** Biometric Privacy Legislation

If comprehensive legislation proves to be difficult to secure, a more narrowly tailored set of protections should be passed to secure citizens' biometric data. While such a legislation might ignore communications data, it would, at the very least, introduce more legal protection over the use of surveillance technologies like facial recognition and other devices. The National Biometric Information Privacy Act of 2020 was recently introduced in the Senate.<sup>85</sup>

83 See Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("*Schrems II*")

84 Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act (S.3663); Data Accountability and Transparency (DATA) Act of 2020; Data Protection Act of 2020 (S.3300); Consumer Online Privacy Act (S.2968); Online Privacy Act of 2019 (H.R. 4978); Bipartisan "Staff Draft" in House Energy and Commerce Committee

85 National Biometric Information Privacy Act of 2020, S.4400, 116th Cong. (2020)

## 5. Condition Federal Grants

- » **Action:** Federal grant funding for state & local acquisition of surveillance technologies should be conditioned on the establishment of transparency and oversight infrastructures.
- » **Description:** Federal Government grants (UASI, JAG, etc.) represent a major source of funding for municipal acquisition of surveillance technologies.<sup>86</sup> Still, many municipalities either are not incentivized nor cannot afford oversight infrastructures. Stakeholders discussed the heavy lift of convincing municipal governments one-by-one, as only 14 localities have passed surveillance ordinances. Conditioning federal grants represents the perfect opportunity to improve democratic oversight and transparency for all citizens where there are digital surveillance technologies in use. Grant writing processes could provide an incentive source for localities to adopt even more protective privacy features, as greater money is tied to greater oversight. Funds could also be made available for municipalities to purchase expensive, but secure data storage capacities.
- » **Implementation:** *Executive*
  - \* An Executive Order requiring grant applications to contain elected representative approval, impact assessments, and public oversight would pass Constitutional muster, based on precedent in *South Dakota v. Dole* (1987).<sup>87</sup> Federal grants account for a small share of police budgets,<sup>88</sup> and there is a germane federal interest in protecting the privacy and civil liberties of U.S. citizens.

## 6. Develop Federal Judiciary Guidance on Surveillance

- » **Action:** Federal judiciaries should create advisory resources, best practices, and other guidance for state & local judges seeking to improve regulation over emerging surveillance technologies.
- » **Description:** Many stakeholders noted that judges are becoming increasingly aware of the transformational nature of new age surveillance technologies. Still, many lack the tools and resources needed to make an informed decision about the reasonable and proportionate use of surveillance—in both the warrant processes and civil and criminal procedures. Better-resourced federal judges could aid in the national effort for increased transparency and democratic accountability by creating toolkits as new technologies and legal principles emerge. A perfect starting place would be to develop a trusted list of amicus curiae for judges to consult as needed. Advisory materials might also suggest reinterpretation of the Davis Good Faith Exception, identified by many stakeholders.
- » **Implementation:** *Judicial*
  - \* A Judicial Conference Committee should be commissioned to create an official list of amicus curiae on topics related to surveillance, evaluate and develop advisory materials on the Davis Good Faith Exceptions' implications on Fourth Amendment protections, and create a set best practices for rethinking warrant regimes, including potentially increasing specificity of geofence warrants and establishing warrant standards for social media monitoring tools.

## 7. Empower Defense Counsel Symmetric Access to Digital Records

- » **Action:** Privacy laws and regulations, such as the Stored Communications Act, should be developed and interpreted towards symmetrical access between defendants and prosecution.
- » **Description:** The SCA grants law enforcement access to citizens' digital records held by Internet companies, while the current DOJ interpretation of the SCA bars criminal defense counsel subpoena access to

<sup>86</sup> Crump, C. (2021). Democratizing Police Adoption of Surveillance Technology. January 2021. <https://www.dayoneproject.org/post/democratizing-police-adoption-of-surveillance-technology>

<sup>87</sup> Yeh, B.T. (2017), "The Federal Government's Authority to Impose Conditions on Grant Funds," *Congressional Research Service*, March 23, <https://fas.org/sgp/crs/misc/R44797.pdf>

<sup>88</sup> "Criminal Justice Expenditures: Police, Corrections, and Courts," *Urban Institute*, 2020, <https://www.urban.org/policy-centers/cross-center-initiatives/state-and-local-finance-initiative/state-and-local-backgrounders/criminal-justice-police-corrections-courts-expenditures>

potentially exonerating information. Moreover, new federal privacy laws continue this asymmetry with exemptions built-in for law enforcement. Several stakeholders emphasized how this inequity heightens the risk of wrongful convictions and undermine fairness in judicial proceedings.

» **Implementation:** *Legislative and Executive*

- \* Federal privacy legislation discussions should add to each bill a “symmetrical savings clause” that reads:

*“Nothing in this Act shall be construed to prohibit a good-faith response to or compliance with otherwise valid warrants, subpoenas, or court orders, or to prohibit providing information as otherwise required by law.”<sup>89</sup>*

- \* U.S. attorneys should file amicus briefs advising courts to grant subpoena power to defense counsel and set aside the DOJ’s interpretation of the SCA that “prohibits service providers from disclosing the contents of electronic communications in response to a defendant’s trial subpoena.” In addition, the DOJ Chief Privacy and Civil Liberties Officer (CPCLO) and the DOJ Computer Crime and Intellectual Property Section (CCIPS) can partner with other DOJ offices to issue a General Counsel memo advising U.S. attorneys nationwide of any changes in policy.<sup>90</sup>

## 8. Reform Information Sharing and Collection Practices

- » **Action:** The Federal Government should ban “two-hop collection”, withdraw funding from Department of Homeland Security (DHS) Fusion Centers, and commission a transparency map to track the flow of information between federal agencies and municipal enterprises.

- » **Description:** Existing privileges enable the NSA collection of foreign nationals’ contacts and their contacts (“two-hop collection”), sweeping millions more digital records from non-suspect U.S. citizens than initially intended. The fusion-center network was developed after the 9/11 terrorist attacks to coordinate information-sharing efforts on potential terrorist threats. However, several government reports indicate fusion centers are largely ineffective,<sup>91</sup> with “Suspicious Activity Reports” disproportionately filed on members of ethnic and religious minorities and over 50% of cases containing nothing of value.<sup>92</sup> Furthermore, stakeholders noted how, beyond fusion centers, a vast, non-transparent information sharing network exists between the Federal Government and municipal law enforcement. Often, this network suffers from data overflows, creating inefficiencies in responsiveness.

» **Implementation:** *Legislative*

- \* Congress should:
  - o Prohibit the collateral “two-hop collection” of telephone or communications records of American citizens, including banning collection of communications “about the target” and the use of National Security Letters to subpoena information;<sup>93</sup>
  - o Consider the creation of an independent Constitutional Advocate with the competency to argue for declassifying FISA Court decisions and allowing Constitutional challenges to federal court decisions;<sup>94</sup>

89 Wexler, R. and Villasenor, J. (2021). Privacy Laws Should Help, Not Harm, Criminal-Justice Reform. Day One Project. January. <https://www.dayoneproject.org/post/privacy-laws-should-help-not-harm-criminal-justice-reform>

90 Ibid.

91 Marthews, A. and Tucker, C. (2020). A National Strategy on Privacy and Civil Liberties. Day One Project. <https://www.dayoneproject.org/post/a-national-strategy-on-privacy-and-civil-liberties>

92 Puente, M. (2019). Commissioners and critics question LAPD’s reports on suspected terrorist activity. Los Angeles Times, June 11. <https://www.latimes.com/local/lanow/la-me-suspicious-activity-reports-lapd-20190612-story.html>; McQuade, B. (2019). Pacifying The Homeland: Intelligence Fusion and Mass Supervision, University of California Press. August. <https://www.ucpress.edu/book/9780520299757/pacifying-the-homeland>

93 Marthews, A. and Tucker, C. (2020). A National Strategy on Privacy and Civil Liberties. Day One Project. <https://www.dayoneproject.org/post/a-national-strategy-on-privacy-and-civil-liberties>

94 An example of such a bill can be found in the USA RIGHTS Act of 2017

- o Withdraw funding from DHS' fusion centers and eliminate existing data collected;<sup>95</sup>
- o Establish a Congressional Advisory Commission to map the information sharing network between federal and municipal entities, review the efficacy of collected data, and propose efficiency and privacy improvements.

## State & Local Action

Municipal governments are the mechanism by which to test the muster of a responsible system of surveillance. With vast deployment settings across diverse state-to-state governance models, these laboratories of democracy will contribute iterative insights into further refining the model towards privacy-preserving and equity interests. Below are a set of recommendations for state & local government action:

### 9. Pass Surveillance Ordinance Legislation

- » **Action:** Municipalities seeking to acquire surveillance technologies should have surveillance ordinance structures in place to ensure democratic accountability and transparency.
- » **Description:** Surveillance ordinances have been successfully tested in at least 14 localities, and stakeholders stressed there has not been a tremendous burden involved in standing-up these structures. They authorize greater public input and city council oversight into the acquisition, use, sharing and/or borrowing of digital surveillance technologies for all entities within the jurisdiction. Ordinance legislation should be consistent with the harm-reduction approach identified above. It should also be drafted in a broad, technology-neutral manner to apply to all methods of acquisition (e.g. donations, federal grants, citizen asset forfeiture) and handle the emergence of a variety of technologies. Ordinance legislation should also contain continuous, annual reviews and assessment abilities to monitor the costs and benefits between public safety, privacy, and civil liberties, with an eye towards disparate impact and treatment. Ordinances should also contain requirements for a public-facing component responsible for justifying the type of surveillance technology used and the range of alternatives available, identifying the locations of any public surveillance, and hosting pre- and post-acquisition public commentary.
- » **Implementation: Legislative**
  - \* **Option 1 (Preferred):** City council passes a surveillance ordinance and establishes a separate administrative agency tasked with reviewing surveillance impact assessments, use policies, and annual reports. Surveillance-using agencies would draft initial documents including data and use policies and present this to the independent agency for approval and public comment. City council would be informed by the separate agency and retain final approval over acquisition. This model may appeal more to better-resourced municipalities. For an example, consider the Oakland Privacy Advisory Commission or the Santa Clara Privacy Office oversight methods.
  - \* **Option 2:** City council passes a surveillance ordinance but no separate administrative agency is created. City council establishes procedures over surveillance technology within the surveillance ordinance and periodically reviews for updates consistent with ongoing use or new acquisitions. In its administrative capacity, city council would review data and use policies and hold public comment, retaining the final approval over acquisition. This model may appeal more to less-resourced municipalities.

### 10. Secure Citizens' Digital Rights in State Amendment, Contract, and Investment

- » **Action:** Municipalities should amend state constitutions to incorporate electronic data and communications protections, and follow or supersede federal guidelines over contract standards.

<sup>95</sup> Marthews, A. and Tucker, C. (2020). A National Strategy on Privacy and Civil Liberties. Day One Project. <https://www.dayoneproject.org/post/a-national-strategy-on-privacy-and-civil-liberties>

- » **Description:** While federal privacy laws may take some time, states and localities should follow the landmark progress made by California and Michigan. States might amend their constitutions to prohibit the unreasonable search and seizure of “the person, houses, papers, possessions, *electronic data*, and *electronic communications*.” Additionally, municipalities—especially those who cannot afford data storage capabilities—might stipulate access and sharing restrictions for data in the contracts, and explicitly hold companies liable in the event of repurposed data-sharing with agencies (i.e. local law enforcement to federal immigration enforcement). Finally, the rampant digital divide that exists in urban and rural areas, which contribute mistrust in government services and hinders the possibility for a participatory democracy, must be corrected through investments promoting digital literacy.
- » **Implementation: Legislative**
  - \* State legislatures should amend their constitutions to include Fourth Amendment protections for citizens’ electronic data and communications.
  - \* State legislatures should authorize investments into digital literacy with a targeted focus on improving knowledge about the opportunities and risks of the digital world and reducing the community’s digital divide.
  - \* States should provide a verification mechanism of citizens’ non-investigative criminal records data, such as pre-conviction mugshots.
  - \* Municipalities might consider establishing a public advocate, like Seattle’s Chief Privacy Officer, to represent and guarantee citizens’ digital civil rights and liberties.
  - \* City lawyers should draft contracts with special attention to the flow of public surveillance data, ensuring that people ultimately have control over their information.

## 11. Seek and Contribute Guidance with Neighboring Localities

- » **Action:** Instead of reinventing the wheel, municipalities should consider looking at existing models to draw adaptive insights for their community.
- » **Description:** It remains difficult for municipalities without technologically literate populations to create sufficient oversight infrastructures. However, a growing number of communities have established effective oversight models that could be instructive. A model ACLU CCOPS bill also identifies a full range of portable local policy considerations. The following have created more trust in the process of acquiring and using surveillance technologies: the Oakland Privacy Advisory Commission, Santa Clara Privacy Office, Smart City PDX’s Privacy and Information Protection Principles, and the San Francisco Police Commission.
- » **Implementation: Executive**
  - \* Stakeholders were representatives of a few of these models and encouraged outreach to transfer lessons learned.

### International Action

A number of international policy levers should also be pursued in order to spotlight the surveillance reform efforts of the United States and improve the democratically-accountable use of surveillance around the world. Below are a set of key recommendations to better secure the global future of democracy and human rights:

## 12. Reform U.S. Export Control Regimes

- » **Action:** The following actions should be undertaken to modernize the export controls regime for the spread of digital surveillance technologies: (1) BIS should extend list-based export controls to certain non-dual use surveillance technologies; (2) Congress should permit BIS to execute end-use export controls in

circumstances where digital surveillance technologies are used to violate human rights by the government or by other individuals or entities of the importing country; (3) BIS should update end-user export controls to require analysis of digital freedoms and sufficient legal frameworks.

» **Description:** With increased knowledge to be gathered by the DSOC and the Democratic Surveillance Accelerator, it will become increasingly possible to inform export controls based on knowledge of human-rights violating end-users and end-uses. However, existing export control authority after the Export Control and Reform Act (ECRA) does not grant BIS the authority to utilize end-use controls for addressing human-rights related concerns—it remains limited only to WMD's. The Entity List, used to exact end-user controls, is not well-equipped to deal with the nuanced variety of end-uses that could take place, nor does it provide clarity on if listed companies are receiving exports from elsewhere. Moreover, the existing Crime Control end-user country groups list remains outdated, as is the Crime Control List (CCL).

\* **CCL-based Controls:** List-based controls can be extended to require an export license for the following sample, non-exhaustive list of surveillance technologies: (1) gunshot detection and location hardware and services; (2) x-ray vans; (3) surveillance enabled or capable light bulbs or other light fixtures.

\* **End-use Controls:** End-use controls should restrict the export of surveillance for the following, non-exhaustive list of end-uses known to violate human rights: mass surveillance, digital censorship, targeted spyware for marginalized, dissident, and other non-conforming communities, and other international privacy standards violations.

\* **End-user Controls:** The Country Commercial Guides should be updated to reflect digital freedom indices via entities listed under the State Department's Non-U.S. Government Tools, Reports, Initiatives, and Guidance,<sup>96</sup> like Freedom House's Freedom on the Net reports.<sup>97</sup> This update should also evaluate whether end-users possess the following legal frameworks: (1) authorization for use of such items or services under domestic laws that are accessible, precise, and available to the public; (2) constraints limiting the use of such items or services under principles of necessity, proportionality, and legitimacy; (3) appropriate oversight of such items and services by independent bodies; (4) the involvement of the judiciary branch in authorizing the use of such items or services; and (5) effective legal remedies in cases of abuse.<sup>98</sup>

» **Implementation:** *Legislative and Executive*

\* Congress should update ECRA §4812 to authorize the President to utilize end-use controls for addressing human-rights related concerns.

\* BIS should update the Country Chart in Supplement No. 1 to Part 738 of the Export Administration Regulations (EAR) to include: mass surveillance, censorship, persecution of dissidents and journalists, or other operations committing human rights abuses.

\* BIS should extend Crime Control authority to the above identified list of technologies over, per § 772.1 of the EAR.

<sup>96</sup> U.S. Department of State Guidance on Implementing the "UN Guiding Principles" for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities, Department of State Bureau of Democracy, Human Rights, and Labor, September 30, 2020. <https://www.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/due-diligence-guidance/>

<sup>97</sup> See Shahbaz, A. and Funk, A. (2020). Freedom on the Net 2020: The Pandemic's Digital Shadow. Freedom House. <https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow>

<sup>98</sup> Malinowski, T. (2020). Comment on FR Doc #2020-15416; Docket No. 200710-0186 [RIN 0694-XC063]. BIS Notice of Inquiry on Advanced Surveillance Systems and Other Items of Human Rights Concern. Bureau of Industry and Security BIS-2020-0021. September 15. <https://www.regulations.gov/document?D=BIS-2020-0021-0021>

### 13. Coordinate Multilateral Export Controls

- » **Action:** The Department of State's Bureau of Democracy, Human Rights, and Labor and the Bureau of International Security and Nonproliferation (ISN) should encourage the establishment of multilateral controls on digital surveillance technologies.
- » **Description:** The Wassenaar Arrangement is the existing, voluntary multilateral export control framework focused on controlling conventional and dual-use goods used for the development or enhancement of military capabilities. It is not adequately geared for addressing controls related to human rights violations. Recently, as a partial remedy, the E.U. modernized its own Cybersurveillance export control policy to apply to human-rights violating end-uses.<sup>99</sup> For the United States to coordinate multilateral controls, Congress must first grant BIS the authority to control end-uses on human rights violations. Then DRL and ISN must next decide if it can sufficiently convince WA members to extend similar end-use authorities or if a new multilateral arrangement is required. These would be applicable beyond the case of surveillance technologies and could extend towards semiconductors and other 21<sup>st</sup> century technologies.
- » **Implementation:** *Executive*

- \* **Option 1:** The scope of Wassenaar Arrangement should be amended to include consideration towards human rights violations.

DRL and ISN would need to encourage WA member states to adopt this change. However, this may be unlikely considering WA is a voluntary regime and scope changes require unanimous consent. Russia, Turkey, Hungary and others are unlikely to participate or approve scope changes.

- \* **Option 2 (Preferred):** Create an E.U.-U.S. Cybersurveillance Export Control Partnership.

DRL and ISN could lead a new multilateral arrangement in partnership with the newly created E.U. cybersurveillance export authorities. This could be coordinated in the variety of proposed multilateral arrangements among democracies (e.g. D10; T12 etc.). Both the European Union and United States would be in position to exert pressure on countries like Canada, Japan, Switzerland, and Israel to also enact similar end-use controls. Alternatively, France may make a prime, initial partner for introducing better investment screening mechanisms and export controls.

### 14. Create an E.U.-U.S. Joint Digital Development Fund

- » **Action:** Competitively promote the adoption of Western digital surveillance technologies in the digitizing world.
  - » **Description:** It is insufficient to merely build out a responsible, liberal-democratic model—it must be promoted vigorously as the alternative to authoritarian systems of surveillance. Currently, China's Export-Import Bank promotes their surveillance technology to importing Belt-and-Road countries and others with so-called 'soft loans' of easy interest rates. While 50% of Chinese loans to the developing world go unreported, as of 2016, this amount is estimated at the low end to be at \$200 billion.<sup>100</sup> These loans make the cutting-edge technology affordable. The State Department and the U.S. International Development Finance Corporation (DFC) should partner with the relevant E.U. agencies to provide a similar, competitive promotion of Western technologies.
  - » **Implementation:** *Executive*
- \* The State Department and the DFC should coordinate an international agreement with the E.U. for promoting the leapfrogged development of digitizing countries via useful and democracy-

99 "Commission welcomes agreement on the modernisation of EU export controls," European Commission Press Release, November 9, 2020, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2045](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2045)

100 Horn, S., Reinhart, C., and Trebesch, C. (2020). China's overseas lending and the looming developing country debt crisis. VoxEU Centre for Economic Policy Research. May 4. <https://voxeu.org/article/china-s-overseas-lending-and-looming-developing-country-debt-crisis#:~:text=We%20find%20that%20about%2050,grown%20to%20around%20%24200%20billion.>

enhancing technologies. \$50 billion could be allocated from both the European Union and the United States, a fraction of the amount of Chinese loans, with potential for significant returns as companies benefit from increased sales. Promoted surveillance technologies from the United States would originate from the Democratic Surveillance Accelerator.

## 15. Engage Diplomatically

- » **Action:** Greater diplomatic action is needed to ensure that the global use of surveillance does not trend towards digital authoritarianism.
- » **Description:** Beyond investments and export controls, a range of policy action is needed to secure the future of democracy and human rights. First, basic, knowledge-gathering exercises are needed to inform digital diplomacy in the Age of Information, such as assessing international standards organizations and tracing the spread of surveillance technology abuses worldwide. Second, more small-scale partnerships and country-specific diplomacy measures are needed.
- » **Implementation:** *Executive*

- \* **Assessing and Improving International Standards:** As surveillance technologies are tested in the American laboratories of democracy, DSOC will identify a number of novel ethical considerations instructive to the international community. Informed by such considerations, the State Department should coordinate with other General Partnership on AI (GPAI) members to evaluate potential norms and standards in international standards-setting organizations designed to advantage companies based in China or authoritarian uses of technology. These efforts should culminate in a proposal of alternative, competitive standards at the International Telecommunication Union.

DRL can also host Track 1.5 dialogues designed to facilitate increased awareness about which surveillance technologies “are and are not captured by existing privacy and surveillance legislation in each country.”<sup>101</sup> Participating members should include civil society, industry, E.U. and Asian country partners with relevant technical or legal expertise.

- \* **Surveillance Oversight Group:** The Inter-Parliamentary Alliance on China (IPAC) is committed to the democratic integrity of political systems and a rules-based international order in support of human dignity. Under the banner of upholding human rights and strengthening security, The Department of State’s new Bureau of Democracy, Human Rights, and Labor and the recently established Bureau of Cyberspace Security and Emerging Technologies should facilitate an international Surveillance Oversight Group dedicated to monitoring instances of surveillance-induced repression in countries importing Chinese and Western surveillance technologies. An annual report to Congress would serve as a primary public research resource, garner media attention, stimulate public awareness and pressure, and incentivize prioritization of the issue within the State and Commerce Departments. This would also help meet industry’s oversight concerns by creating more transparent review processes over the system’s integrators and distributors who may be the intermediaries between the manufacturer and end-user. At a higher level, this would also introduce coordinated transparency and accountability to export control systems. DRL should propose the creation of the Surveillance Oversight Group at the next conference.
- \* **T3 Partnership with India and Israel:** The existing T3 multilateral arrangement among the United States, India, and Israel is focused on securing strategic, economic, and development interests around 5G telecommunications infrastructures. However, the T3 countries represent key stakeholders for the future of digital surveillance: India as the world’s largest democracy in demand of more surveillance technology; Israel as a leading surveillance technology developer; and the United States as a potential model for surveillance oversight reform. A strong partnership

<sup>101</sup> Peterson, D. (2020). Designing Alternatives to China’s Repressive Surveillance State. Georgetown Center for Security and Emerging Technology. October. <https://cset.georgetown.edu/research/designing-alternatives-to-chinas-repressive-surveillance-state/>

among the T3 could institutionalize transparency and accountability into global standards over the use and export of surveillance.

- \* **Country-specific Diplomacy:** While companies such as Huawei have country-specific marketing materials, U.S. diplomatic messaging follows a “one-size-fits-all” approach with appeals to “geostrategic rivalry, democracy and human rights, and data security” without clearly stating which is at issue.<sup>102</sup> A coordinated delegation effort between the Department of Commerce’s Digital Attaché Program<sup>103</sup> and CSET could represent a nuanced mechanism for facilitating the adoption of privacy-preserving surveillance technologies in countries like Brazil, India, South Africa, and Indonesia, as well as other digitizing countries. These efforts would recognize the role of subnational actors, who may be demanding China-based technologies to solve real-world governance problems of crime and drug-activity. Engaging subnational actors must appeal to these needs with accountable, privacy-preserving technologies. For example, explicit guarantees against data siphoning would be a persuasive contrast to China-based surveillance technology. Country-specific diplomacy would dovetail with the endeavors undertaken by the Democratic Surveillance Accelerator members to secure better democratic governance and safeguards in countries looking to apply digital surveillance.

102 Greitens, S.C. (2020). China’s Surveillance State at Home & Abroad: Challenges for U.S. Policy, Working Paper for the Penn Project on the Future of U.S.-China Relations, October 2020, [https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b/732/files/2020/10/Sheena-Greitens\\_Chinas-Surveillance-State-at-Home-Abroad\\_Final.pdf](https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b/732/files/2020/10/Sheena-Greitens_Chinas-Surveillance-State-at-Home-Abroad_Final.pdf)

103 Ratner, Ely., et. al. (2020). Rising to the China Challenge. Center for New American Security. January 28. <https://www.cnas.org/publications/reports/rising-to-the-china-challenge>

## Appendix A: List of Stakeholders

### **Albert Fox Cahn**

*Surveillance Technology Oversight Project*

### **Andrew Guthrie Ferguson**

*Professor of Law, American University  
Washington College of Law*

### **Bisa French**

*Chief, Richmond Police Department*

### **Brian Hofer**

*Chair, City of Oakland Privacy Advisory Commission  
(OPAC), and Executive Director, Secure Justice*

### **Catherine Crump**

*Clinical Professor of Law, UC Berkeley School of Law,  
Director, Samuelson Law, Technology and Public Policy  
Clinic, and Co-Director Berkeley Center for Law &  
Technology*

### **Chad Marlow**

*American Civil Liberties Union (ACLU)*

### **Charles Rollet**

*IPVM*

### **Clare Garvie**

*Georgetown Center on Privacy and Technology*

### **Courtney Bowman**

*Palantir Technologies*

### **Dahlia Peterson**

*Georgetown Center for Security  
and Emerging Technology*

### **David Ray**

*Rank One Computing*

### **District of Columbia Metropolitan Police Department**

### **Elizabeth Goiten**

*Brennan Center for Justice*

### **Elizabeth O'Sullivan**

*Surveillance Technology Oversight Project*

### **Esha Bhandari**

*ACLU*

### **Farhang Heydari**

*New York University Law School's The Policing Project*

### **Hector Dominguez Aguirre**

*Open Data Coordinator, City of Portland*

### **Ivan Quinn**

*Secure Planet Inc.*

### **Jacklyn A. Kerr**

*The Brookings Institution, National Defense University,  
and Former AAAS Fellow, Office of Science & Technology  
Advisor to the Secretary of State*

### **Jason Lando**

*Commander, Pittsburgh Police Department*

### **Jeremy Slavish**

*Amazon Web Services*

**James Dempsey**

*Executive Director, Berkeley Center for Law and Technology*

**Sarah Brayne**

*Assistant Professor of Sociology,  
The University of Texas at Austin*

**Judith Mowry**

*Office of Equity and Human Rights, City of Portland*

**Sarah Lageson**

*Assistant Professor of Sociology,  
Rutgers School of Criminal Justice*

**Kelsey Finch**

*Future of Privacy Forum*

**Sharon Bradford Franklin**

*Open Technology Institute, New America and Former  
Executive Director, Privacy and Civil Liberties Oversight Board*

**Kevin Wolf**

*Akin and Gump LLC and Former Assistant Secretary of  
Commerce of Export Administration, Bureau of Industry  
and Security*

**Sheena Chestnut Greitens**

*Associate Professor at Lyndon B. Johnson School of Public  
Affairs, University of Texas at Austin*

**Marilyn Fidler**

*Berkman Klein Center Fellow, Harvard University*

**Tom Wheeler**

*The Brookings Institution and Former Chairman  
of the Federal Communications Commission*

**Matthew Guariglia**

*Electronic Frontier Foundation*

**Michael German**

*Brennan Center for Justice and  
Former FBI Special Agent*

**Michael Shapiro**

*Santa Clara Privacy Office*

**Rachel Levinson-Waldman**

*Brennan Center for Justice*

**Rashall Brackney**

*Chief, Charlottesville Police Department*

## **Appendix B: Interview Questions**

### **More Responsible Model (General):**

- \* If you can imagine it, what does a responsible system of surveillance look like? And what are the major obstacles towards reaching it?
- \* In broad strokes, how can we overcome these barriers/expand protections?
- \* Is there greater coordination needed at the federal and state/local?
- \* How important is building public trust for a responsible system of surveillance?

### **Transparent Acquisition:**

- \* How best can we increase transparency in the acquisition process?
- \* What standards should guide public-private contracts?
- \* What role should citizens/city council/federal government play, if any, in the acquisition process?

### **Accountable Use:**

- \* Who and what areas would likely come first under surveillance and why?
- \* What role should judges, city council, citizens, companies, and the Federal Government play in the accountability of surveillance?
- \* Which body should be responsible for ensuring public knowledge about surveillance protocols?
- \* Which actor(s) should be responsible for data storage, security, and privacy?
- \* What is your evaluation of the current due diligence measures, such as disparate impact assessments, privacy impact assessments, annual surveillance impact reports etc.
- \* How should liability be assigned in the event of harmful effects of surveillance (on privacy, discriminatory impact etc.)?

### **Innovation & Global Competition Challenges**

- \* How might we realign innovation incentives to encourage the competitive adoption of privacy-preserving surveillance?
- \* How can we ensure U.S. companies do not cede crucial market share to autocratic actors, especially with respect to recently digitizing countries?
- \* Can export controls work in this domain? Which countries are leaders in surveillance technology and would be willing to partner on ethical safeguards?
- \* Should we let autocratic actors be responsible for the installation of likely-to-be-misused surveillance technology in rapidly digitizing countries? Does any installation from the US/West end up becoming an unethical policy option?
- \* Are there portable governance methods beyond privacy-preserving techniques in the equipment that might make US/West leadership in the global surveillance industry more advantageous for democracy?
- \* Would you recommend a move away from the Wassenaar Arrangement through a partnership with new E.U. cybersurveillance control regimes? Are there multilateral fora you're particularly excited about for 2021 that could coordinate such controls (i.e. Biden's Summit of Democracies etc.)?
- \* Are there strategic levers that the US/West can use to engage subnational officials driving the important demand and promote more responsible surveillance use?

## **Appendix C: Sample Certification Questionnaire**

### **Bias and Discrimination:**

- \* Describe the metrics your company uses to evaluate the proposed technology for unfair bias.
- \* Describe the risks of unfair bias in training and intended use contexts for the proposed technology.
- \* How are these risks prioritized against other competing interests of the company?
- \* What independent third-parties approved of your designs or assessments?

### **Proportionate Use:**

- \* How did you assess the appropriateness of your system for public use?
- \* What are the competing alternatives to your method of surveillance?
- \* How do you avoid the overcollection of data? What is your company's plan for extraneous data?

### **Privacy by Design:**

- \* What processes in the development, testing, and deployment support privacy?
- \* What company resources are devoted to privacy by design?
- \* What is your data retention policy? Why is this appropriate for the intended use cases?

### **Performance Security:**

- \* Describe how any metrics used in the marketing or sale of the technology were developed.
- \* How have you assessed the total risks of your system's operation, including privacy, errors, unfair bias, hacking and cyberattacks, decision-making transparency, and infringements on civil and human rights?
- \* What standards are followed to evaluate the accuracy and performance of systems?
- \* What are the measured rates of false positive and false negatives?

### **Right to Information:**

- \* How are end-users kept informed about software management for your system?
- \* What portals are available for citizens to access their stored personal data? Does this require paying any fees?
- \* What portals are available for contracting agencies to access data? Does this require paying additional fees?
- \* Other than citizens and contracting agencies, what other entities have access to the public surveillance data?
- \* Will a description of intended purposes, data retention, data-sharing policy be publicly available?

### **Exports:**

- \* What countries do you anticipate becoming your primary customers?
- \* What types of technical firewalls have you installed in your product to ensure greater oversight?
- \* What company resources will be devoted towards monitoring inappropriate end-uses?
- \* Under what circumstances will you revoke software operation from the end-user?

## **Appendix D: Draft Executive Order**

### **Draft Executive Order Digital Surveillance Oversight Committee Prepared by Ishan Sharma, Federation of American Scientists**

\*\*\*\*\*

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

#### **Section 1. Creation of a Digital Surveillance Oversight Committee.**

A. There is hereby established the Digital Surveillance Oversight Committee (hereinafter referred to as the Committee). The Committee shall be composed of representatives designated by each of the following:

1. The Chair of the Privacy and Civil Liberties Oversight Board
2. The Attorney General
3. The Secretary of Commerce
4. The Secretary of State

The first-appointed representative of the Secretary of Commerce, which shall be the Under Secretary of Commerce for Standards and Technology, will be appointed the chairman of the Committee. The chairman, as he deems appropriate, may invite representatives of other departments and agencies to participate from time to time in the activities of the Committee.

B. The Committee shall have primary continuing responsibility within the Executive Branch for monitoring, certifying, and recertifying current and emerging surveillance technologies in the United States. In fulfillment of this responsibility, the Committee shall:

1. Solicit, review, and certify surveillance technology proposals based on the proposal authors' answers to an objective questionnaire, comparison of existing, less-invasive alternatives, software and hardware audits, the intended and potential use-cases of the technology and safeguards against misuse, and the technology's design environment, including but not limited to supply-chain security and internal due diligence (e.g. risk assessment frameworks of the impact on privacy and potential for errors, hacking, and bias).
2. Oversee, every three years, the renewal of technology's certification, based on the proposal authors' Domestic and Foreign Portfolios of Operation. Portfolios shall include empirical use-cases, measures of efficacy (e.g. number of false positives and false negatives, measured crime reductions, disparate impact, cases of misuse, and third-party evaluations), recorded instances of data mismanagement (e.g. public surveillance data breaches, resale or repurposing of data gathered from the technology), civil society complaints, any foreign entities including systems integrators, international distributors, or end users in receipt of the technology, contractual language of authorized end-uses and recorded violations of such stipulations, and newly installed safeguards against abuse.
3. Make every effort to meaningfully involve diverse public stakeholder input, including members of historically surveilled communities, human rights, privacy, and tech-ethicist scholars, retired law enforcement and industry professionals, and leading civil society organizations.
4. Compile data on the range of oversight measures and intended use-cases submitted by proposal authors and other stakeholders with the aim of creating a database equipped for nuanced due diligence in each type of surveillance technology.

5. Inform the Bureau of Industry and Security nuanced digital surveillance export controls efforts, based on data gathered through the certification and recertification process.

## **Section 2. Duties**

The duties of the the Chair of the Privacy and Civil Liberties Oversight Board, the Attorney General, the Secretary of Commerce, and the Secretary of State and their appointees are as follows:

1. In addition to appointing the chair, who is also specially tasked with performing technical software and hardware audits, the Secretary of Commerce shall also appoint a representative of the Bureau of Industry and Security to review the integrity of proposed technologies' supply chains for security or sustainability threats.
2. The Attorney General shall appoint a representative from the Department of Justice's Office of Civil Rights, which is responsible for conducting diverse public stakeholder engagement and examine the range of civil rights and civil liberties concerns originating from the surveillance technology. The Attorney General shall also appoint a representative from the National Institute of Justice to contribute insights from its Developing Performance Standards and Testing Equipment program.
3. The Chair of the Privacy and Civil Liberties Oversight Board must extend appointment to other members, and must limit participation in certification and recertification decisions to cases concerned with the surveillance of terrorism.
4. The Secretary of State shall appoint a representative from the Bureau of Democracy, Human rights, and Labor to review proposals seeking to export the technology and evaluate end-use violations in recertification cases.

## **Section 3. Plan of Action**

- A. Within 6 months of the date of this memorandum, the Committee shall be formed and empowered to execute the authorities outlined above.

## **Section 4: General Provisions**

- A. All departments and agencies are directed to provide, to the extent permitted by law, such information and assistance as may be requested by the Committee or the Secretary of Commerce in carrying out their functions and activities under this order.
- B. Nothing in this order shall affect the data-gathering, regulatory, or enforcement authority of any existing department or agency over surveillance standards and technology, and the certifications, recertification, or other recommendations of surveillance technologies provided by this order shall not in any way supersede or prejudice any other process provided by law.

\*\*\*\*\*

**Cover image:** Atypeek Dgn. "Modern equipment for video surveillance on wall".  
<https://www.pexels.com/photo/modern-equipment-for-video-surveillance-on-wall-5966513/>



Federation  
*of* American  
Scientists