DAY ONE PROJECT

A Strategy to Blend Domestic and Foreign Policy on Responsible Digital Surveillance Reform

Ishan Sharma

February 2021

Summary

Modern data surveillance has been used to systematically silence free expression,[1] destroy political dissidents,[2] and track ethnic minorities before placement in concentration camps.[3] China's surveillance-export system is providing a model of authoritarian stability and security to the 80+ countries using its technology,[4] a number that will grow in the aftermath of COVID-19 as the technology spreads to the half of the world still to come online.[5] This technology is shifting the balance of power between democratic and autocratic governance. Meanwhile, the purported US model is un-democratic at best: a Wild West absent of accountability and full of black box, NDA-protected public-private partnerships between law enforcement and surveillance companies.[6] Our system continues to oppress marginalized communities in the US, muddying our moral claims abroad with hypocrisy. Surveillance undermines the privacy of everyone, but not equally. Most citizens remain unaware of, unaffected by, or disinterested in the daily violence propagated by the unregulated acquisition and use of surveillance. The lack of coordination between state and local agencies and the federal government around surveillance has created a deeply unregulated surveillance-tech environment and a discordant international agenda. Digital surveillance policy reform must coordinate both domestic and foreign imperatives. At home, it must be oriented toward solving a racial equity issue which produces daily harm. Abroad, it must be motivated by preserving 21st century democracy and human rights.

First, the Federal Government can realign innovation incentives towards more responsible, privacy-preserving development via a multi-stakeholder Digital Surveillance Oversight Committee certification process and a Privacy & Democracy Surveillance Accelerator, setting standards for public-private contracts and updating judiciary guidance. Second, the Federal Government can promote the more responsible use of surveillance technologies internationally by building out multilateral export controls, creating a Surveillance Oversight Group within the Inter-Parliamentary Alliance on China (IPAC), positioning the T3 partnership with Israel and India

[1]Hassine, Wafa B., The Crime of Speech: How Arab Governments Use the Law to Silence Expression Online. EFF (Nov. 2, 2016) https://www.eff.org/pages/crime-speech-how-arab-governments-use-law-silence-expression-online
[2] Parkinson, J., Bariyo, N., and Chin, J. Huawei Technicians Helped African Governments Spy on Political Opponents. WSJ. (Aug. 15, 2019) https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017
[3] Buckley C., and Mozur, P. How China Uses High-Tech Surveillance to Subdue Minorities. N.Y. Times (May 22 2019). https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html
[4] Khalil, L., Digital Authoritarianism, China and Covid. Lowy Institute (November 2 2020) https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid
[5] Greitens, S.C. 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
[6] Fidler, M. (2020) Local Police Surveillance and the Administrative Fourth Amendment. *Santa Clara Computer and High Technology Law Journal* Oct. 21. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3201113

towards surveillance issues, and engaging subnational actors on country-specific digital diplomacy.

Challenge and Opportunity

The past two centuries of recorded history have witnessed a steady oscillation between waves of democratization and reverse waves of authoritarianism.[7] In the early the 21st century, much of the foreign policy establishment assumed that the democratic model would always supersede, as technological progress consistently meant democratic progress. However, modern surveillance technologies have upended these long-held assumptions, representing a categorical shift in the potential of centralized governance. These are truly revolutionary technologies. For example, only 2% of CCTV footage is ever viewed by a human being.[8] But through advances in artificial intelligence and video analytics, it is now possible to simultaneously monitor hundreds of video streams and thousands of people with an AI that fuses the data streams and sends real-time alerts for 'anomalous' behavior.[9] Other companies offer government surveillance packages that tap into the "bidstream" -- the digital advertising ecosystem teeming with granular, geolocational and other mobile and app data -- to search vast seas of information for an individual with little else other than a phone number.[10] These are only two examples; in the Information Age, untold varieties of surveillance technologies are emerging in the complex, globalized surveillance industry. Without data, the centralized, planned economy of Soviet Russia was doomed to implode. With data, the authoritarian model has arguably become more stable, competitive, and accessible to would-be authoritarians than ever before.[11]

One-half of the world is still to come online, but over 90% of humanity is expected to be connected in the next decade.[12] This inflection period represents an opportunity for embedding digital surveillance to track citizens as they gain access to the Internet and other technologies. Indeed, a proxy battle for the future of democracy, human rights, and the rule of law is taking

[7] Huntington, S.P., Democracy's Third Wave. Journal of Democracy, 2, no. 2 (1991): 12-13, 18, https://www.ned.org/docs/Samuel-P-Huntington-Democracy-Third-Wave.pdf
[8] 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
[9] 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
[10] 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
[11] Wright, N. D., et. al. AI, China, Russia, and the Global Order. Strategic Multilayer Assessment Periodic Publication, Department of Defense and White House Chief of Staff (Dec. 2018), https://nsiteam.com/social/wp-content/uploads/2018/12/AI-China-Russia-Global-WP_FINAL.pdf
[12] 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/

place in the recently digitizing worlds of the African, Latin American, and Asian continents. Over 80 countries have imported Chinese surveillance equipment, which often comes with training and other operating procedure guidance.[13] China recognizes that the norms established now will dictate the future governance of multilateral institutions like the International Telecommunication Union (ITU). The U.S., on the other hand, has been largely absent from international leadership. With little competition, Chinese companies have unilaterally proposed every ITU standard for facial recognition technology use in the last three years, including storage of detected face features like race and ethnicity, the ubiquitous monitoring of people in public spaces, and the verification of employee attendance.[14] If China continues to set the global normative climate, the marketplace will continue to tilt in their favor, making democratically-compatible technologies even more difficult to introduce.[15]

Leadership in this competitive era must proceed by example. If we are to expect digitizing countries to responsibly deploy advanced technologies, then the US and allies must create a visible alternative to China's turnkey authoritarian technology solutions. Fortunately, in most democratic countries, targeted surveillance requires some threshold of particularized suspicion: law enforcement must obtain independent authorization and operate within limited, proportionate scope -- *in principle*.[16] However, in the U.S., the application of these principles has been weak, with judicial accountability estimated at 10-20 years behind the pace of new technology adoption.[17] The data overwhelmingly shows underrepresented communities to have been the target of discriminatory surveillance technologies.[18] Moreover, Western democracies are guilty of equipping despots throughout the world with tools and training that help them retain their grip on power.[19] Globally, COVID-19 has accelerated the intrusive use of surveillance worldwide, often without transparency, independent oversight, or avenues for redress.[20]

---

[13] 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

[14] Gross, A., Madhumita, M., Yuan, Y. (2019), Chinese tech groups shaping UN facial recognition standards. *Financial Times*, Dec. 1 https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67

[15] 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, 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

[16] 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

[17] Fidler, M. (2020) Local Police Surveillance and the Administrative Fourth Amendment. *Santa Clara Computer and High Technology Law Journal* Oct. 21. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3201113

[18] Dennis, A. (2020), Mass Surveillance and Black Legal History, American Constitution Society, Feb. 18. https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history/; 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/

[19] Woodhams, S. China, Africa, and the Private Surveillance Industry, Georgetown Journal of International Affairs Vol 21 (Fall 2020): pp. 158-165. https://muse.jhu.edu/article/766370; 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

[20] 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

Still, some laboratories of American democracy hold promise for a new model. Just over 14 municipalities have passed surveillance ordinances and reasonably succeeded at improving transparency and oversight in the acquisition and use of technology.[21] In line with a recent Day One Memo by Catherine Crump, the Federal Government should augment these efforts.[22] However, there is also a need to develop a regulatory approach to industry, one that reorients the incentives of development away from a race to invasiveness. These domestic efforts must be paired with sound international efforts to reconcile the immense demand for new age surveillance with the future of democracy and human rights in the Age of Information.

Plan of Action

(1) Commission a Digital Surveillance Oversight Committee (DSOC): To guide the competitive but accountable development of Western surveillance technology, the Biden-Harris Administration should establish a Digital Surveillance Oversight Committee. DSOC would solicit, certify, and recertify industry product proposals for current and emerging surveillance technologies, compile end-use cases and end-user data to inform nuanced export controls and strategic decisions, and develop new metrics for meaningful due-diligence assessments. While on January 11th, 2021, the Federal Trade Commission (FTC) reached a landmark settlement curbing the misuse of facial recognition by California-based photo app developer Everalbum, Inc., more attention is needed on specific surveillance technologies procured and used by the government. The FTC would be able to focus on the misuse of consumer data, while the DSOC would become a forward-looking partner on surveillance technologies themselves. DSOC would be charged with a broad scope beyond data and towards managing the rapidly developing international surveillance industry.

- **Certification:** An optional, multi-stakeholder, and objective review process. Submitted proposals would be based on the completion of a sample questionnaire , efficacy evaluations, identifying less-invasive alternatives, risk assessment frameworks,[23] technical product specifications, secure source-code and object-review testing, intended and potential use-cases, due diligence processes and safeguards against abuse, and product supply-chain security.

- **Recertification:** Every three years, companies would need to renew their certification, especially in circumstances of new updates to technology. Such recertification, however, would be based on companies' Portfolios of Operation. Domestic Portfolios might include empirical effectiveness at reaching intended use objectives, the quality of due diligence, instances of data breaches, misuse of public surveillance data, or other civil society complaints. International Portfolios

[21] Fidler, M. and Liu, L. (2020). Four Obstacles to Local Surveillance Ordinances. Lawfare. September 4. https://www.lawfareblog.com/four-obstacles-local-surveillance-ordinances
[22] Crump, C. (2021). Democratizing Police Adoption of Surveillance Technology. January 2021. https://www.dayoneproject.org/post/democratizing-police-adoption-of-surveillance-technology
[23] E.g. systems' impact on privacy, potential for errors or hacking, and susceptibility to unfair bias.

would include similar considerations but also due-diligence compliance to State Department surveillance-export guidelines and analysis of the entities in receipt of export, including systems integrators and other international distributors or end users.

- **Additional Functions:** Because certification proposals provide extensive information about intended uses, end users, due diligence metrics, and more, the DSOC would have competency to inform approaches to surveillance issues well beyond certification and recertification. It could develop and recommend new metrics and evaluation tools for measuring the effectiveness of technologies; compile end uses and create clear boundaries for international acceptable and unacceptable uses; delineate certain technologies for list-based export controls; and assist with multilateral reform efforts.

Implementation Option 1: Executive Order

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 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:

- **Privacy and Civil Liberties Oversight Board (PCLOB):** 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.
- **Department of Justice Office of Civil Rights (OCR):** This representative 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 proposed surveillance technology.
- **Department of Justice National Institute of Justice:** This representative would contribute insights from the Developing Performance Standards and Testing Equipment program towards digital surveillance technologies.
- **National Institute of Standards and Technology:** This representative would provide recommendations based on software and hardware audits, such as secure reviews of training data, source code and object review, and vulnerabilities and backdoors for data siphoning.

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

Implementation Option 2: Legislative Action

Amend 42 U.S.C. § 2000ee to expand the authorities of the Privacy and Civil Liberties Oversight Board (PCLOB) to include the regulation of digital surveillance technologies. While PCLOB represents an ideal 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 created by these limitations 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 Committee chairman vested in the Chairman of the PCLOB.

(2) Re-architect Export Control Regimes for Multilateral Controls: The existing export controls regime, codified by the Export Control and Reform Act (ECRA), grants the Bureau of Industry and Security only limited authority to address concerns related to weapons of mass destruction, not human rights violations. Partly due to the industries' many intermediaries, including systems integrators and international distributors, manufacturers claim it is often impossible to know the particular end user of a product.[24] This lack of information and coordination has resulted in U.S. technology supporting grave injustices abroad. Focused only on end-users, the Entity List is not equipped to deal with the nuanced variety of digital surveillance *end-uses* -- nor does it provide for multilateral integration into the landmark recent decision of the EU to look beyond the Wassenaar Arrangement (WA) or extend authority for end-use controls to human rights violations. Following suit, and informed by approved end use information supplied by industry and gathered by the DSOC, the U.S. export controls regime should impose end-use controls to restrict the export of surveillance in cases of mass surveillance; digital censorship; targeted spyware for marginalized communities, dissidents, and other non-conforming communities; and other international privacy standards violations.

BIS should also extend list-based export controls to certain non-dual-use surveillance technologies, including gunshot detection, location hardware and related services, x-ray vans, and surveillance-enabled or capable light bulbs. In addition, BIS should update its Crime Control end-user country groups list criteria to require analysis of digital freedoms and sufficient legal frameworks. This update should also evaluate whether end-users

[24] 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

possess the following legal frameworks: (1) authorization for use of such items or services under domestic laws that are accessible, precise, and transparent 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.[25]

Implementation: Executive and Legislative Action

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

Second, 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.
- Extend Crime Control authority to the above-identified list of technologies, per § 772.1 of the EAR.
- Revise its Country Commercial Guides to reflect digital freedom indices as reported by entities listed under the State Department's Non-U.S. Government Tools, Reports, Initiatives, and Guidance, like Freedom House's Freedom on the Net reports.

(3) Coordinate Multilateral Export Controls: In light of BIS being extended the authority to exact nuanced, informed end-use controls, the State Department's Bureau of Democracy, Human Rights, and Labor (DRL) and the Bureau of International Security and Nonproliferation (ISN) should encourage the establishment of multilateral controls on digital surveillance technologies beyond the Wassenaar Arrangement.

Western democracies have supplied surveillance technologies towards rights-abusive ends. E.U. aid money has been used to fund the acquisition of surveillance technologies and train officials in problematic uses across the Middle East, Northern and Western Africa, and the Balkans. Currently, many Western companies are aggressively vying for market share in Gulf Cooperation States. Serious coordination is needed among democratic allies to control the proliferation of digital surveillance.

[25] 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

Implementation: Executive

Option 1: The scope of the 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 that 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 EU-US 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 E.U. and US would be in a position to exert pressure on countries like Canada, Japan, Switzerland, and Israel to enact similar end use controls. Alternatively, France may make a prime initial partner for introducing better investment-screening mechanisms and export controls.

(4) Establish a Democratic Surveillance Accelerator: Coordinated export controls on surveillance technologies will not prevent the autocratic entrenchment and misuse of this technology in countries at risk of 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 the development of a set of technical firewalls and oversight measures in the design of surveillance technologies. In addition to funding, 5-6 selected companies would benefit from enhanced domestic market access and provide an expedited export license to countries at risk of backsliding, under a set of positive conditions. For domestic markets, accelerator selection would add companies to the FBI's preferred vendors list and expedite public-private municipal requests for federal grants.

However, accelerator selection would favor companies with capacity to export internationally. For international markets, accelerator selection would grant selected companies the opportunity to compete in countries that may be at risk of backsliding with an export license with a set of positive conditions. In addition to meeting the State Department's DRL guidance to industry,[26] the conditions for the export license to such countries should also include:

- **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),

[26]E.g. like contractual and procedural safeguards that contain end-user license agreements based on human rights safeguards language, and preventative frameworks to revoke usage rights when necessary 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/

tamper-resistant tools, and artificial intelligence techniques designed to continuously learn, monitor misuse and lock operation where applicable.

- **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 compete with the free installation, servicing, and training provided by many PRC-based companies.
- **No Data Siphoning Guarantees:** Many digitizing countries already are walling off digital borders to keep data in-house. There is immense potential for U.S. companies to gain market advantage with digitizing countries by guaranteeing the security and privacy of their data.

The Democratic Surveillance Accelerator is not intended to catapult U.S. leadership to the forefront of the global surveillance industry. Rather, it provides an opportunity to signal 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.

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 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 the expedited export license with the stipulated conditions. DSOC would review, every three years, companies' Portfolios of Operation to ensure compliance with license requirements.

(5) Condition Federal Surveillance-Acquisition Grants on the Development of Local Oversight Structures: Federal grants, such as DHS' Urban Areas Security Initiative, are a primary funding mechanisms for localities acquiring surveillance technology.[27] These enable police departments to receive the technology without any appropriations oversight by City Councils. Admittedly, many smaller municipalities lack the budgetary or administrative capacities to stand up oversight infrastructures. A strong way to encourage the nationwide roll-out of surveillance oversight infrastructure would be to condition the receipt of funds on the establishment of a paid, democratically-accountable Privacy Advisory Commission, modeled after the City of Oakland.[28] Grant writing processes could provide an incentive source for localities to adopt even more protective privacy features,

[27] Guariglia, M., and Maass, D., How Police Fund Surveillance Technology is Part of the Problem. (Sept. 23, 2020). https://www.eff.org/deeplinks/2020/09/how-police-fund-surveillance-technology-part-problem.
[28] Privacy Advisory Commission, City Administration, n.d. http://www2.oaklandnet.com/government/o/CityAdministration/d/PrivacyAdvisoryCommission/index.htm#:~:text=The%20Privacy%20Advisory%20Commission%20provides,collects%20or%20stores%20our%20data.

as greater money is tied to greater oversight. Funds could also be made available for municipalities to retain access to data, either through city-owned registries or exclusive access with companies.

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). Federal grants account for a small share of police budgets,[29] and there is a germane federal interest in protecting the digital privacy and civil liberties of U.S. citizens.

(6) Establish Model Public-Private Contract Floors: A well-resourced federal government is better positioned to negotiate model contract standards with companies than frequently cash-strapped municipalities. The outcome of municipality-based contracts has been to shroud the technology in opacity and cede authority over data management to companies. Such contract floors should not preempt stronger contracts, but should rather set a minimum to include:

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

Implementation: *Executive*

The FBI can create model 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.

(7) Develop Federal Judiciary Guidance on Surveillance: Federal judiciaries should create advisory resources, best practices, and other guidance for state and local judges seeking to improve regulation over emerging surveillance technologies. Many judges lack the tools and resources needed to make informed decisions about the reasonable and proportionate use of surveillance -- in both warrant processes and civil and criminal

[29] "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

procedures. With more resources at their disposal, 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 as a problem by many stakeholders.

Implementation: Judicial

A Judicial Conference Committee should be commissioned to create an official Federal list of amicus curiae on topics related to surveillance, evaluate and develop advisory materials on the Davis Good Faith exemptions' 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.

(8) Surveillance Oversight Group at 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 State Department's Bureau of Democracy, Human Rights, and Labor should facilitate an international Surveillance Oversight Group dedicated to monitoring instances of surveillance-induced repression in countries importing Chinese and Western surveillance technologies. This would also help meet industry's oversight concerns by creating more transparent review processes over the system's integrators and distributors who are often the intermediaries between the manufacturer and end user.[30] At a higher level, this would also introduce coordinated transparency and accountability to export control systems.

Implementation: Executive

The U.S. delegation to IPAC should propose a new campaign that establishes an ongoing Surveillance Oversight Group.

(9) Consolidate Standards-Setting Efforts: As surveillance technologies are tested in 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 norms and standards in international standards-setting organizations potentially designed to advantage PRC-based companies or authoritarian

[30] 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

uses of technology. These efforts should culminate in a proposal of alternative, competitive standards at the ITU.

Implementation: Executive

DSOC should inform the State Department on novel standards and use-considerations to propel better standards-setting efforts internationally. DRL and the recently approved Bureau of Cyberspace and Emerging Technologies (CSET) should review and actively contribute to international standards setting efforts via multilateral coordination with GPAI partners and alternative recommendations at the ITU.

(10) T3 Partnership with India and Israel: The existing T3 multilateral arrangement among the U.S., 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 U.S. as a potential model for surveillance oversight reform. A strong partnership among the T3 could institutionalize transparency and accountability into the global standards for the use and export of surveillance.

Implementation: Executive

The State Department should initiate the conversation on promoting more responsible export and adoption of surveillance technologies within the multilateral arrangement.

(11) 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. A coordinated U.S.-led effort could represent a more nuanced mechanism for facilitating greater adoption of privacy-preserving surveillance technologies in countries like Brazil, India, South Africa, Indonesia and other digitizing countries. These efforts would recognize the role of subnational actors, who are demanding Chinese technologies because they are attempting 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 Chinese 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.

Implementation: Executive

Coordination between the Department of Commerce's Digital Attaché Program and the State Department's CSET could be focused on the design of country-specific policies and messaging and identify mechanisms to promote more responsible technology adoption.

Taken together, these recommendations offer a comprehensive strategy to blend domestic and foreign policy to counter digital authoritarianism. Reforming domestic processes to reduce the daily harms suffered by marginalized communities from invasive digital means is essential to solving the digital authoritarianism question. Ensuring that neither our country, nor any other democratic country, exports cutting-edge surveillance tools would limit the supply and abuse of modern surveillance worldwide. By themselves, however, expo controls would not preserve the future of democracy and human rights. Too many alternative supply sources exist for the half of the world still to come online. Promoting American surveillance technologies is not about American leadership in the industry -- it is about normalizing the baseline of expectations that should follow from the export of these technologies: technical safeguards against misuse, democratically-consistent training, and more. Rather than shying away from engaging countries who may be at risk of democratic backsliding, the U.S. must engage in savvy multilateral and country-specific diplomacy to encourage the responsible use of technology. The alternatives of banning surveillance or continuing the status quo will only continue to worsen the global resurgence of authoritarianism.

Conclusion

In this digital era, the persistence of democracy is far from guaranteed. Surveillance technologies represent a fundamental shift in the capacities of governments to perfect information flows and control populations. With hi-tech surveillance, no longer is a costly, unstable reliance on military repression needed. If we are to avoid a future of normalized, effective authoritarianism, it is paramount that the US and allies present an alternative, responsible model of surveillance. Our surveillance system is broken, but through Federal Government action there is hope of introducing meaningful democratic accountability at home and abroad.

Frequently Asked Questions

What is your definition of "digital surveillance"?

Digital Surveillance: a product or service marketed for or that can be used (with or without the authorization of the seller) 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, products designed to clandestinely intercept live communications)
- **Biometric identification** (e.g., facial recognition software, automated biometric systems, rapid DNA testing, gait analysis software)
- **Data analytics** (e.g., social media analytics software, predictive policing systems, data fusion technology, 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)
- **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)

What are the primary obstacles to achieving this strategy?

The largest obstacles will come from ensuring meaningful public stakeholder engagement and representation in the certification and recertification process of digital surveillance technologies. This should be a formalized, required process. Admittedly, this will run counter to the aspiration to create an effective, timely process that does not militate against innovation. While many companies may be initially opposed to this process, there is some evidence that industry could favor more clarity in strategic signaling of innovation criteria. The certification and recertification process would prevent a race to the bottom, wherein certain startup companies might be less-inclined to consider due diligence and provide technology to bad actors.

Another potential issue will be the constitutionality of an Executive Order that conditions federal grants on the installment of local surveillance oversight structures. The recent analog was President Trump's Executive Order 13768, which withheld federal funding from sanctuary cities that did not abide by immigration enforcement restrictions. However, such funding represented

13% of the budget for municipalities, which made conditionality overly coercive. Current federal grant funding for the overall municipal police budget is estimated to be much lower.

What is a sample case the Committee could resolve? How might the Committee work together?

A domestic or foreign company is seeking to sell an emotion recognition surveillance technology software in the United States. They would be required to submit a list of intended use cases and competing alternatives, answers to a questionnaire, supply chain information, and due diligence operations, including risk assessment frameworks, and evaluation of the technology's efficacy. Representatives from the Department of Justice's Office of Civil Rights would seek public stakeholder comment for a set period of time, ideally no more than three weeks, in which representatives from the National Institute of Justice and the National Institute of Standards and Technology would conduct technical, software and hardware audits testing submitted claims of efficacy. Representatives from the Bureau of Industry and Security would approve or disapprove the submitted supply chain documents on the basis of security or sustainability threats. For domestic companies seeking to export or international companies seeking to import in the U.S., the Bureau of Democracy, Human Rights, and Labor would review evidence on the companies' past customers, human-rights conducive contractual language, and end-use violations of those agreements. In circumstances when intended use cases are aimed at Federal Government use of surveillance for terrorism, the Privacy and Civil Liberties Oversight Board would be able to offer comment. However, without legislative amendment, their participation would be limited. Once the public comment period has concluded, the chairman of the DSOC would convene the parties to present the information gathered and render a decision to certify or not certify the technology.

What level of bipartisanship is to be expected with this strategy?

High. While the Democratic party would likely strongly support the policies outlined in this strategy, considering it addresses in part the racially-charged, daily harms of surveillance against marginalized U.S. citizens, there is also strong reason for Republican party support. The strategy envisions the strengthening of democracy at home and abroad, as well as guarantees of U.S. citizens' privacy in the digital age. Strong technology regulation appears to have consistent bipartisan support. Moreover, this strategy is architected to counter digital authoritarianism, a hallmark of U.S. efforts for dealing with a technologically empowered China and an issue of strong bipartisan support.

What domestic and foreign progress has been made on addressing these issues?

Very little. Fourteen localities have passed surveillance ordinances aiming to improve democratic oversight in the acquisition and use of surveillance at the municipal and state levels. Internationally, the EU has initiated a landmark decision to extend human rights concerns for end-use export controls restrictions, a novel breakaway from the Wassenaar Arrangement.

About the Author

Ishan Sharma is a Herbert Scoville Jr. Peace Fellow of Emerging Technologies at the Federation of American Scientists and a Project Advisor at the Day One Project. He holds a B.S. from Cornell University and has studied jurisprudence and international human rights law at the University of Oxford. At FAS, Ishan leads a project on Emerging Technologies and International Security, which is currently focused on countering digital authoritarianism. Part of this effort has involved interviews with representatives from the NYU Policing Project, Palantir Technologies, the Oakland Privacy Advisory Commission, the DC Metropolitan Police Department, and 40 other stakeholders for his forthcoming multi-stakeholder report on a more responsible, liberal-democratic alternative to surveillance. He has been published on China's strategic exports in the political economy of AI surveillance and co-authored a prize-winning piece for the 2020 Security Models "Era of Covid" policy competition at New America among other publications.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of the next presidential term. For more about the Day One Project, visit **dayoneproject.org**.