DAY ONE PROJECT

Mitigating and Preventing the Existing Harms of Digital Surveillance Technology

Stephen Caines

May 2021

Summary

The rapid adoption of Digital Surveillance Technology (DST) by state and local agencies is taking place in an under-regulated environment that is causing tangible harm to the communities and individuals these same agencies are tasked to protect. DST itself is plagued by fundamental flaws and vulnerabilities, issues compounded by a lack of safeguards in the environments where DST is deployed. The four biggest problems with government use of DST today are:

(1) Governments falling prey to predatory or negligently marketed DST that fails to consistently achieve stated functionalities or meet reasonable standards.
(2) Governments deploying DST in a way that does or could falsely implicate innocent individuals in criminal matters.
(3) A lack of systematic oversight that fails to ensure accountability, equity, transparency, or cybersecurity.
(4) Governments utilizing DST in a manner inconsistent with existing laws, ordinances, and regulations.

While these issues affect everyone, they disproportionately affect those who are falsely implicated in criminal matters as a result of DST, as well as the working poor (who have been historically over-surveilled). In addition to such human costs, overuse or misuse of DST exposes cash-strapped jurisdictions to multimillion-dollar lawsuits for violation of privacy and civil rights.

This proposal offers a set of actions that the Biden-Harris Administration could take to limit the harms of DST. Specifically, we recommend that the administration:

- Issue an Executive Order to create two mandatory filings for vendors and government agencies involved in active federal contracts for DST.
- Empower and fund the Federal Trade Commission (FTC) with $10 million over two years to study and produce rules regarding DST marketing and sales.
- Allocate $50 million for a Privacy Pilot Program that would allow municipalities to utilize a tailored hybrid model of government and civilian oversight for DST.
- Condition federal dollars spent on DST for law enforcement on compliance with a set of assessments.
- Instruct the Department of Justice to create a DST Task Force to study the benefits and tradeoffs of different types of DST.

These actions would together begin to rein in the unchecked power of the surveillance complex that has attached itself to our nation's law-enforcement systems. Doing so would advance racial and community equity across the United States while also helping restore public trust in law-enforcement institutions.

Challenge and Opportunity

Development, sophistication, and use of surveillance technologies have increased around the world over the last few decades. While law-enforcement agencies and vendors praise surveillance technologies for enabling a more just and secure society, community advocates, academics, and policymakers have long emphasized the threats that surveillance technologies present. Digital surveillance can be defined as the use of technology by government, law enforcement, or private individuals to detect, monitor, interpret, transmit, or retain sensitive data, information, or communications about individuals or a group.[1] Government use of Digital Surveillance Technology (DST)—such as facial recognition, predictive policing, automated license plate readers (APLR), and cell-phone trackers—for law enforcement inflicts realized and prospective harms on surveilled populations. These harms include loss of privacy, chilling of First Amendment activities, unjust implication or misidentification, and increased marginalization of at-risk communities.[2] Harms are compounded by a lack of robust and systematic record keeping: data-collection efforts for DST often focus on an individual surveillance technology, use case, or jurisdiction rather than the DST landscape as a whole.

Table 1 provides examples of the wide range of types, applications, and issues associated with government deployment of DST.

Table 1. Example DST use cases

Technology Name	*Purpose/Functionality*	*Industry Leader*	*Issues*
Gunshot Detection Technology (GDT)	Relying on acoustic algorithms, microphones, and sensors, GDT determines the occurrence and location of gunshots in an area and alerts law enforcement.[3]	ShotSpotter	**Cost; accuracy; privacy**. An analysis of data from seven cities showed police were unable to find evidence of gunshots following GDT alerts 30–70% of the time.[4] Yet cities are spending huge amounts of money on the technology: the NYPD currently has a $28 million, five-year contract with ShotSpotter.[5] GDT systems can also capture human speech, raising

[1] Ishan Sharma, *A More Responsible Digital Surveillance Future: Multi-Stakeholder Perspectives and Cohesive State & Local, Federal, and International Actions* (Washington D.C., VA: Federation of American Scientists, 2021).
[2] Stephen Caines, "The Many Faces of Facial Recognition," in *Research Handbook on Big Data Law*, ed. Roland Vogel (Edward Elgar, 2021), 29–56.
[3] "Acoustic Gunshot Detection." Electronic Frontier Foundation, November 7, 2019. https://www.eff.org/pages/gunshot-detection
[4] Matt Drange, "We're Spending Millions On This High-Tech System Designed To Reduce Gun Violence. Is It Making A Difference?" *Forbes*, November 17, 2016, https://www.forbes.com/sites/mattdrange/2016/11/17/shotspotter-struggles-to-prove-impact-as-silicon-valley-answer-to-gun-violence/?sh=6b0f3b6231cb.
[5] Gabriel Sandoval and Rachel Holliday Smith, "'ShotSpotter' Tested as Shootings and Fireworks Soar, While Civil Rights Questions Linger," *THE CITY*, July 5, 2020, https://www.thecity.nyc/2020/7/5/21312671/shotspotter-nyc-shootings-fireworks-nypd-civil-rights.

			privacy concerns.[6]
Phone Cracking Tools	These devices allow law enforcement to access files on a locked cell phone by using data-extraction tools to access various data layers.[7]	Cellebrite	**Cybersecurity; output integrity.** Cellebrite was recently shown to have significant cybersecurity flaws that could allow malicious actors to plant false evidence during the data-extraction process.[8] Investigations that have utilized this technology are now having their integrity questioned, as information obtained has been used in criminal cases.[9]
Automated License Plate Readers (APLRs)	APLRs enable agencies and individuals to scan and store images of license plates, drivers and occupants, and vehicles, along with date, time, and location metadata.[10]	Vigilant Solutions	**Data overcollection; unauthorized data sharing; mission creep.** A 2019 audit of a Los Angeles APLR system revealed that 99.9% of the 320 million images stored by the technology were of innocent people.[11] The report further revealed that significant amounts of data were being shared between agencies without legally required safeguards. Moreover, while APLRs were designed to find stolen vehicles and abducted children, they have since been used by ICE to find undocumented persons.[12]
Predictive Policing System (PPS)	Predictive policing applies AI, statistics, and analytics to mass troves of data,	PredPol	**Bias in police data- and record-keeping; Over-policing and over-**

[6] Cale Guthrie Weissman, "The NYPD's Newest Technology May Be Recording Conversations," *Business Insider*, March 26, 2015, https://www.businessinsider.com/the-nypds-newest-technology-may-be-recording-conversations-2015-3.
[7] "Cellebrite - Digital Intelligence For A Safer World," EndPoint Forensics, accessed May 7, 2021, https://www.cellebrite.com/en/home/.
[8] Moxie Marlinspike, "Exploiting Vulnerabilities in Cellebrite UFED and Physical Analyzer from an App's Perspective," *Signal Messenger*, April 21, 2021, https://signal.org/blog/cellebrite-vulnerabilities/.
[9] Josh Taylor, "Signal's Hack of Surveillance Tech Used by Police Could Undermine Australian Criminal Cases," *The Guardian*, May 1, 2021, https://www.theguardian.com/australia-news/2021/may/02/how-the-hacking-of-surveillance-tech-used-by-police-could-undermine-australian-criminal-cases.
[10] "Automated License Plate Readers (ALPRs)," Electronic Frontier Foundation, May 15, 2017, https://www.eff.org/pages/automated-license-plate-readers-alpr.
[11] Auditor of the State of California, "Automated License Plate Readers To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects," Report Number 2019-118, February 2020, https://www.auditor.ca.gov/reports/2019-118/summary.html.
[12] Tracy Rosenberg, "Mission Creep – Berkeley's License Plate Readers," *Oakland Privacy*, August 8, 2019, https://oaklandprivacy.org/mission-creep-berkeleys-license-plate-readers/.

	generating police insights around individuals or locations who could be involved in criminal activity.[13]		**surveillance.**[14] In Pasco County, FL, the sheriff's office has applied its PPS to juvenile.[15] First-time juvenile offenders and their family members have been harassed by police officers based on the results of the system. One 15-year-old who was accused of stealing bikes from a garage was visited by police 21 times over five months.

The harms caused by DST can be broadly sorted into two categories: (1) efficacy and security, and (2) transparency and ethics. Considerations around each are detailed below.

Efficacy and security

Efficacy and security concerns center on whether DST meets advertised and discussed parameters, as well as whether a DST system is designed and operated in a way that minimizes risk of unauthorized access. In short, efficacy and security concerns revolve around **whether a given DST can be responsibly used in a given deployment environment.** DST systems are high-priority targets for bad actors and often lack sufficient cybersecurity measures to limit the amount and severity of breaches. DST hacking can lead to theft of personally identifiable information, other privacy breaches, and ransomware attacks. Given the deficit of technical expertise in most government agencies, efficacy and security concerns are usually best addressed by DST vendors and creators—though a public mandate may be required for them to do so.

Transparency and Ethics

Transparency and ethics concerns center on whether DST users (often government agencies) are being honest about what DST they are using and how they are using it. These concerns also consider whether agencies are operating DST systems in ways that recognize traditional and digital human rights, relaying accurate information of interest to the community, and are minimally invasive. In short, transparency and ethics concerns revolve around **whether a given DST application or contract should exist at all.** Several real-world cases illustrate how transparency and ethics concerns around DST are playing out in practice.

[13] Tim Lau, "Predictive Policing Explained," Brennan Center for Justice, April 1, 2020, https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.
[14] Will Douglas Heaven, "Training Data That Is Meant to Make Predictive Policing Less Biased Is Still Racist," *MIT Technology Review*, February 5, 2021, https://www.technologyreview.com/2021/02/05/1017560/predictive-policing-racist-algorithmic-bias-data-crime-predpol/
[15] Nick Sibilla, "Lawsuit: Florida County Uses 'Predictive Policing' To Arrest Residents For Petty Code Violations," *Forbes*, April 26, 2021, https://www.forbes.com/sites/nicksibilla/2021/04/26/lawsuit-florida-county-uses-predictive-policing-to-arrest-residents-for-petty-code-violations/?sh=676c22252d0f.

- Failure to disclose legal violations. The surveillance company FLIR recently signed a $300,000 contract with the City of Seattle to conduct traffic surveillance using cellphone data. Prior to securing the government contract, though, FLIR settled federal regulatory charges for illegally selling restricted military technology to prohibited nations and pled guilty to bribing Saudi Arabian officials.[16] When the City of Seattle issued a privacy impact report in 2019, they omitted mention of this track record. Strong federal laws ensuring transparency and ethics in DST use could have prohibited the City from contracting with FLIR in the first place, or at least mandated disclosure of FLIR's troubling history.

- Eroding public trust in law enforcement. Earlier in 2021, a bombshell report revealed that dozens of police departments have been lying about their use of the disruptive facial-recognition technology sold by Clearview AI.[17] Such a lack of veracity significantly undermines public trust in U.S. law-enforcement broadly—unfairly painting responsible law-enforcement agencies with the same brush as irresponsible ones. Government agencies have also used DST to generate revenue even when it fails to achieve the stated deployment purpose.[18] This issue can largely be attributed to intentional ambiguity surrounding planned use cases and a lack of standards for DST operation.

- Poor record-keeping. In 2017, the City of San Diego did not provide information directly requested by Congress about the City's use of facial-recognition technology: largely because they were not maintaining good records about their use of DST.[19] This case is particularly troubling from a national perspective as the City's use of the technology was funded by money from the Department of Homeland Security.

These multiple failures for local government agencies to responsibly manage their own use of DST highlight the need for federal involvement.

Plan of Action

Public support for regulation and legislative action around DST has been trending upward. A recent survey found that 64% of Americans are somewhat or very concerned about government data collection. At least 25 U.S. jurisdictions have surveillance ordinances on the books to help

[16] Patrick Malone, "Seattle's Surveillance Contractor Has History of Illegal Sales, Bribery, Worrying Privacy Advocates," *The Seattle Times*, March 7, 2021, https://www.seattletimes.com/seattle-news/times-watchdog/seattles-surveillance-contractor-has-history-of-illegal-sales-bribery-worrying-privacy-advocates/.
[17] Caroline Haskins, "The NYPD Has Misled The Public About Its Use Of Facial Recognition Tool Clearview AI," *BuzzFeed News,* April 7, 2021, https://www.buzzfeednews.com/article/carolinehaskins1/nypd-has-misled-public-about-clearview-ai-use.
[18] Ella Fassler, "Oklahoma Quietly Launched a Mass Surveillance Program to Track Uninsured Drivers," *OneZero*, April 6, 2021, https://onezero.medium.com/oklahoma-quietly-launched-a-mass-surveillance-program-to-track-uninsured-drivers-471bb4e5701a
[19] Jesse Marx, "San Diego Held Back Materials Sought by Congress on Facial Recognition," *Voice of San Diego,* April 30, 2021, https://www.voiceofsandiego.org/topics/government/san-diego-held-back-materials-sought-by-congress-on-facial-recognition/.

protect their citizens' privacy.[20] At the federal level, recent pieces of legislation like the "The Fourth Amendment is Not For Sale Act" aim to curb use of DST and have garnered bipartisan support.[21]

The time is ripe to build on this momentum. Federal action is needed to reduce the number of victims of DST, restore public trust in law enforcement, and bring order to a marketplace of DST vendors that often take advantage of unwitting government officials and lucrative government contracts. Specifically, federal action is needed to address the four biggest problems with government use of DST:

(1) Governments falling prey to predatory or negligently marketed DST that fails to consistently achieve stated functionalities or meet reasonable standards.
(2) Governments deploying DST in a way that does or could falsely implicate innocent individuals in criminal matters.
(3) A lack of systematic oversight that fails to ensure accountability, equity, transparency, or cybersecurity.
(4) Governments utilizing DST in a manner inconsistent with existing laws, ordinances, and regulations.

Effective intervention must target the supply side (technology vendors) and the demand side (government users) of the DST marketplace. Below, we present a suite of actions that the Biden-Harris administration can take to do both. The first set of proposals focuses on efficacy and security, with a goal of immediately mitigating the tangible and imminent harms of DST misuse and overuse. The second set of proposals focuses on transparency and ethics, with a goal of increasing public trust and restoring America's image as a leader of human rights and privacy over the long term.

Policy Recommendations: Efficacy and Security

Issue an Executive Order to create two mandatory filings for vendors and government agencies involved in active federal contracts for DST.

Establishing mandatory filing requirements for DST use would (1) make it harder for bad actors to continue receiving government contracts by creating a mechanism for notice of vendor vulnerabilities and issues (akin to a products liability recall), and (2) encourages accountability

[20] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," Pew Research Center, November 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/; Stevie Degroff and Albert Fox Cahn, *New CCOPS On The Beat - An Early Assessment of Community Control of Police Surveillance Laws*, February 10, 2021, https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/602430a5ef89df2ce6894ce1/1612984485653/New+CCOPS+On+The+Beat.pdf.

[21] Joseph Cox, "New Bill Would Ban Clearview and Warrantless Location Data Purchases," *VICE*, April 28, 2021, https://www.vice.com/en/article/k78qyy/fourth-amendment-is-not-for-sale-act-would-ban-clearview-and-warrantless-location-data-purchases.

and true oversight by aggregating and centralizing records of use. President Biden can implement such requirements through an Executive Order. The Executive Order should create two mandatory filing requirements:

- The first mandatory filing requirement would be a basic statement filed with the Department of Justice communicating the existence of a relationship between a vendor and agency for a specific DST tool, as well as the contract length (with "at will" or "indefinite" being acceptable responses). Such a filing could take the form of the existing General Services Administration Schedule, which is a searchable database of federal contracts.[22] The database of filings should be publicly accessible, thereby giving communities, academics, and advocates a clearer picture of the landscape of federal DST use.

- The second filing would be made with an authorized record keeper for the agency using the technology and would include the names of individuals from both parties involved in the approval and deployment process, the contract price, functionality and performance standards, stated reasons for implementation, and metrics of success. There should also be a requirement that individual uses and queries made on the technology be logged and maintained to produce an annual anonymized report. Agencies would be required to maintain records for a minimum of 15 years following the conclusion of use or the relationship. Responses to valid Freedom of Information Act (FOIA) requests for these filings should at minimum confirm the use of a technology or relationship with a vendor.

These filing requirements would apply to all DST vendors with at least one current contract with a government agency that utilized federal funds or resources in part or in sum to procure the technology. The term "current contract" is intended to be broad enough to cover explicit and implicit agreements that permit access or the use of a vendor's systems or technology. Given the numerous methods of procurement and acquisition of DST (e.g., asset forfeiture, private benefactors, federal grants, private foundations, and kickbacks), a broad filing requirement is needed to cover all vendor whose technology is knowingly being used by a government or law enforcement agency in return for some benefit.[23] Similarly, the term "benefit" must be broadly construed as including but not limited to economic payments, access to nonpublic information, or anything else of value.

Should vendors fail to comply with these measures, they should be barred from receiving future federal contracts. Precedent for this action could come from President Biden's forthcoming Executive Order instituting a mandatory requirement for government contractors to report

[22] "GSA Schedule," U.S. General Services Administration, March 9, 2021, https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedule.
[23] Matthew Guariglia and Dave Maass, "How Police Fund Surveillance Technology Is Part of the Problem," Electronic Frontier Foundation, September 23, 2020, https://www.eff.org/deeplinks/2020/09/how-police-fund-surveillance-technology-part-problem.

cybersecurity breaches.[24] While that order would include most current federal DST vendors in the event of a cybersecurity breach, requiring multiple formal statements of general use by DST vendors is vital for curbing DST harms outlined above. These filings would also make it possible for prospective users of a given DST to compare and evaluate claims of efficacy in places where the DST is already being used. While local jurisdictions should have some authority over access, use, and admissibility of such records, they should not be able to determine whether they in fact exist. The Office of Management and Budget could provide support by flagging funds earmarked for DST, to aid compliance with the Executive Order.[25] While DST vendors will incur administrative and economic costs to comply with these filing requirements, such costs are outweighed by the benefits of improving transparency and limiting the capacity of bad actors and poorly designed and/or operated systems to cause harm.

Empower and fund the Federal Trade Commission with $10 million over two years to study and produce rules regarding DST marketing and sales. These funds would enable the FTC to study DST, catalog best practices, and conduct rulemaking governing DST use. These actions will better protect governmental consumers of DST and ensure that purchased technology lives up to stated performance. Specifically, the Office of Technology Research and Investigation within the FTC should take primary responsibility for this directive, given their combination of technical expertise and mandate for consumer protection.[26] The Office's efforts should be carried out in consultation with National Institute of Science and Technology (NIST, a non-regulatory agency that has previously studied many types of DST) and the National Artificial Intelligence Initiative (NAII).

The FTC can carry out these tasks under existing authority. Indeed, the FTC has already addressed bad actors in the data and surveillance space, with one example being the agency's rendering of a $3.7 million judgment against Everalbum for the company's use of facial recognition without user consent.[27] Additionally, in 2012 the FTC formally released "Facing Facts", a guide of best practices for vendors of facial-recognition technology about how to protect privacy and handle sensitive data.[28] Even more recently, the FTC released a public statement indicating its willingness to engage with artificial-intelligence vendors who have not adequately determined that their tools do not result in discriminatory outcomes.[29] While the

[24] Dina Temple-Raston, "Biden Order Will Require New Cybersecurity Standards In Response To SolarWinds Attack," NPR, April 29, 2021, https://www.npr.org/2021/04/29/991333036/biden-order-to-require-new-cybersecurity-standards-in-response-to-solarwinds-att.

[25] "Office of Management and Budget," The White House, The United States Government, March 26, 2021, https://www.whitehouse.gov/omb/

[26] "Office of Technology Research and Investigation," Federal Trade Commission, March 17, 2021, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation.

[27] Jonathan Mark, Kate Berry, John D Seiver and K.C. Halm, "FTC Sets Its Eye on Algorithms, Automated Tech, and AI-Enabled Applications - Breaking Ground in Facial Recognition and BOTS Act Enforcement," *Davis Wright Tremaine LLP* (blog), February 3, 2021, https://www.dwt.com/blogs/privacy--security-law-blog/2021/01/ftc-duty-to-delete-ai-algorithm.

[28] " FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies," Federal Trade Commission, October 22, 2012, https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition

[29] Elisa Jillson, "Aiming for Truth, Fairness, and Equity in Your Company's Use of AI," Federal Trade Commission, April 19, 2021, https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

statement is broad in nature, DST that is discriminatory in nature or falsely implicates individuals could undoubtedly fall within the purview of activity described and thus warrant investigation under the FTC's existing policies.

Policy Recommendations: Transparency and Ethics

Allocate $50 million for a Privacy Pilot Program that would allow municipalities to utilize a tailored hybrid model of government and civilian oversight for DST. The progression of DST in the United States has demonstrated that municipalities and jurisdictions may be better served using proactive rather than reactive methods to address DST use. As such, the Biden-Harris administration should allocate $50 million to establish a Privacy Pilot Program within the ten most populous cities in the United States. The goal of the program would be to develop effective, tailored strategies for deploying DST in ways that respect the civil rights and privacy of city residents, and to implement frameworks that assure responsible continued use of DSt moving forward.[30] Members of the pilot program will each receive $5 million over 3 years to establish one or a combination of the following:

- Privacy Commission. A board of majority internal City employees who have veto, rulemaking, and investigative powers over the use of DST by any government office or employee in their jurisdiction. The Privacy Commission would also draft surveillance ordinances, when appropriate, for consideration by the City Council or similar body.

- Digital Privacy Task Force. A board comprising internal employees, academics, industry leaders, advocacy groups, stakeholders, and community members who would serve in an advisory capacity, helping the city craft broad privacy-policy goals as well as respond to specific use cases or applications.

- Citizen Oversight Board. A board of community members and leaders who regularly confer with law enforcement over the deployment of DST and novel surveillance tools.

- Privacy Office. A government office, overseen by a Chief Privacy Officer (CPO) and staffed by analysts, policy advisors, and program managers, tasked with reviewing city policy around privacy and the use of DST. Cities that currently have a CPO or existing privacy office could use program funds to expand its staff, purchase training tools and resources, and deploy privacy-preserving software or methods.

Should the pilot program prove successful within the initial cohort of cities, normative practices may emerge that can be extended to less populous cities. The pilot program will be directed by the U.S. Chief Technology Officer (CTO), who may grant cities permission to deviate from program strictures as necessary and appropriate. The U.S. CTO could also allow cities to apply

[30] Mailyn Fidler, "Local Police Surveillance and the Administrative Fourth Amendment," *Santa Clara High Technology Law Journal*, 36, no. 5 (2020): 481, https://digitalcommons.law.scu.edu/chtlj/vol36/iss5/2

program funds to matters outside the specific scope of DST, provided there is some clear nexus to issues of surveillance and privacy. Precedent for this program could come from cities that have already begun engaging in some of the above steps, including Oakland, San Jose, and Seattle.

Condition federal dollars spent on DST for law enforcement on compliance with a set of assessments. Prior to receiving federal funds to purchase DST, government agencies should be required to produce and submit the following documents: a (i) Privacy Impact Assessment; (ii) an Assessment of Potential for Racial and Ethnic Disparate Impact; and (iii) a Statement of Intended Purpose, Safeguards, and Evidentiary Requirements of Use. These three assessments will ensure that governments do a thorough evaluation of potential effects of DST before deployment. The Department of Justice should review all submissions and should be granted veto power over any proposed deployment.

Instruct the Department of Justice to create a DST Task Force to study the benefits and tradeoffs of different types of DST. The task force should monitor agency compliance with surveillance ordinances, review civil-rights lawsuits related to DST use, oversee the mandatory filings mentioned above, and draft clear standards of use that guide agencies through procurement, deployment, and maintenance of DST systems. The overall goal of the task force would be to set forth general guidelines for ethical deployment of DST and to investigate problematic use cases. The DOJ should work with NIST and the FTC to ensure synergy between the federal government's legislative goals and technical objectives.

Conclusion

The status quo of DST in the United States is untenable. Premature technologies coupled with limited safeguards result in tangible harm to the very communities whose interests the DST is purported to protect. It is time for the federal government to act. To reduce the number of victims of DST, restore public trust in law enforcement, and bring order to the marketplace of DST vendors, the Biden-Harris administration should establish filing requirements for DST market participants and government users, empower the FTC to have greater authority over DST rulemaking, provide resources to major U.S. cities to strengthen governance of local DST deployment, condition federal funds for DST purchasing on compliance with responsible-use assessments, and create a DST task force housed at the DST. By taking these steps, the new administration will be able to better protect the interests of all Americans in an increasingly surveilled and digital world.

Frequently Asked Questions

Isn't there sufficient oversight at the municipal level to prevent harms of DST? Why does the federal government need to get involved?

Numerous real-world examples show that municipal oversight of DST is insufficient. Local government agencies often lack the technical capacity needed to tell in advance whether a DST product is worth investing in. This enables DST vendors to oversell the capabilities of their technologies in exchange for a lucrative government contract. Banjo, the recipient of a $20 million AI-surveillance system contract in Utah, failed to deliver real-time surveillance capabilities: instead it simply aided a skilled analyst through a dashboard interface.[31] In other cases, such as those referenced in the body of this memo, overuse or misuse of DST has created cybersecurity risks, compromised individual privacy, and resulted in gross overpolicing—often without public knowledge. There are multiple incentives for government actors to obscure their use of controversial DST systems (such as the potential for litigation, loss of public trust, or public attitudes toward surveillance). As such, federal involvement is important and necessary to save taxpayer dollars and protect Americans from harm.

Shouldn't determinations around local law-enforcement use of DST be left to state and local governments?

Unfortunately, there is a growing number of cases where local law-enforcement agencies have disregarded state and local privacy-preserving legislation. The San Francisco Police Department unlawfully gained access to a network of cameras operated by the Union Square Business Improvement District to monitor protestors last summer.[32] The NYPD has been using (while simultaneously denying any relationship with) technology produced by the facial-recognition technology company Clearview AI.[33] Virginia State Police have also lied about their use of the same software.[34] In an environment where "access" can be gained through the ease of a simple subscription model, DST systems can be donated or provided free of charge in return for some other incentive, and paper trails can be minimized, law enforcement has shown a willingness to exceed the scope of—or even blatantly violate—the laws they have sworn to protect. Federal intervention is needed to provide additional oversight of agencies using DST, regardless of if they are forthright about their actions or not.

Why is there a need to condition federal funding for DST on compliance with responsible use?

---

[31] Joh Dougall, Review of Banjo IT Controls, March 26, 2021, https://docs.google.com/document/d/167dlL8RJYHdHDdMFwnjgBdi5mOxv6seTYNqXmZ9pJzc/edit.

[32] Nathan Sheard, "San Francisco Supervisors Must Rein In SFPD's Abuse of Surveillance Cameras," Electronic Frontier Foundation, October 13, 2020, https://www.eff.org/deeplinks/2020/10/san-francisco-supervisors-must-reign-sfpds-abuse-surveillance-cameras.

[33] Eric Weiss, "NYPD Gets Caught Lying About Rampant Use of Clearview AI," FindBiometrics, April 14, 2021, https://findbiometrics.com/nypd-gets-caught-lying-about-rampant-use-clearview-ai-041411/.

[34] Jonathan Edwards, "Virginia State Police admit - after repeated denials - that they used controversial facial recognition app," *The Virginian-Pilot*, March 30, 2021, https://www.pilotonline.com/government/virginia/vp-nw-virginia-state-police-clearview-20210330-zqgok5644vewhjyoaozdjibi7u-story.html.

Federal use of DST can be subject to the same issues plaguing state and local use of DST. For instance, SBI-Net, the billion-dollar Secure Border Initiative, was intended to be a 53-mile long system of infrastructure, technology, and rapid-response capabilities along the U.S.-Mexico Border.[35] The project was abandoned after costs ballooned and a Homeland Security Secretary deemed the project was too expensive and ineffective. The potential for wiser allocation of resources is critical at all levels of government, especially as the nation is still reeling from the social and economic effects of the COVID-19 pandemic. Further, much surveillance technology is purchased with federal funds or through federal programs such as the 1033 Program or Equitable Sharing and Civil Asset Forfeiture.[36] Our nation owes it to taxpayers to ensure that the technology purchased with their money acts to their benefit, not their detriment.

How does the Supreme Court's recent decision regarding the Federal Trade Commission's authority to seek damages for injured parties under Section 13(b) impact this proposal?

While the recent decision in *AMG Capital Management, LLC v. FTC (2021)* curtails the FTC's ability to directly secure financial restitution or disgorgement for those harmed by deceptive trade practices, the case still permits Section 13(b) to be used to secure injunctive relief.[37] While equitable relief is not financial compensation, it can still prevent future agencies from falling prey to the same practices by restraining vendor activity. Ideally, this will prevent negligent and malicious vendors from continuing to take advantage of government agencies. Further, the FTC can still issue a cease-and-desist order to violators. In the event of noncompliance, district courts are empowered through Sections 5(1) and 19 to secure equitable relief as well as monetary damages. While the FTC may be required to take a few more steps to secure remedies in a given case, there still exists a way to ensure integrity in the DST vendor space. Therefore, the FTC has the authorities and compliance mechanisms needed to carry out the duties outlined in this memo.

Where does the authority or precedent for the two proposed mandatory filings established via Executive Order come from?

Executive Orders have been the vehicle for some of America's most radical shifts and transformations. Under Article II of the U.S. Constitution, the President is instructed to oversee and direct the various activities of the Executive Branch.[38] DST, often purchased with Federal dollars and operated by agencies under the supervision of the Executive Agencies, is currently

[35] Julia Preston, "Homeland Security Cancels 'Virtual Fence' After $1 Billion Is Spent," *The New York Times*, January 15, 2011, https://www.nytimes.com/2011/01/15/us/politics/15fence.html.
[36] Matthew Guariglia, "End Two Federal Programs That Fund Police Surveillance Tech," Electronic Frontier Foundation, January 26, 2021, https://www.eff.org/deeplinks/2021/01/end-two-federal-programs-fund-police-surveillance-tech.
[37] Christopher Willis, "SCOTUS Rules FTC Act Section 13(b) Does Not Authorize FTC to Seek Restitution or Disgorgement," *JD Supra*, April 23, 2021, https://www.jdsupra.com/legalnews/scotus-rules-ftc-act-section-13-b-does-3340698/.
[38] "The Power of the President: The Roles of Executive Orders in American Government," *LawShelf Educational Media*, accessed May 1, 2021, https://lawshelf.com/shortvideoscontentview/the-power-of-the-president-the-roles-of-executive-orders-in-american-government/.

causing and contributing to civil-rights violations such as the false arrests and detentions of Nijer Parks, Robert Williams, and Michael Oliver.[39] The President can justify implementing mandatory-filing requirements by Executive Order due to his responsibility to protect American citizens and limit wasteful spending. Moreover, the working group created by Executive Order 13688 (issued by President Obama) recommended a number of safeguards to the procurement of equipment by local law-enforcement agencies, such as prohibited lists and some forms of mandatory filings.[40] This proposal goes one step further by placing an obligation on equipment vendors as well.

What issues of DST are not addressed by this proposal?

The role of the data-brokerage industry in fueling many DST systems is not addressed. This industry is particularly adept at providing highly specalized data streams about individuals, such as the Department of Defense receiving user-location data from a Muslim prayer app with 98 million users.[41] This proposal does not address vendors that are globally marketing and training technologies used for human-rights abuses such as facial-recognition technologies used by China to target Uighur Muslims. This proposal does not address development of countersurveillance tools such as Fawkes, nor does it address an outright ban of specifically dangerous use cases. This proposal does not address the trade secret and competition arguments often raised by vendors. Finally, the scope of this proposal does not extend to hybrid private surveillance networks that are accessed by law enforcement (e.g., Ring Doorbell). Due to space constraints herein and the complexity of issues involved, these vital matters must be discussed in another forum.

[39] Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *The New York Times*, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.
[40] *Recommendations Pursuant to EXECUTIVE ORDER 13688 Federal Support for Local Law Enforcement Equipment Acquisition*, May 2015, https://bja.ojp.gov/sites/g/files/xyckuh186/files/publications/LEEWG_Report_Final.pdf
[41] Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," *VICE*, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

About the Author

Stephen Caines is a second-year Residential Fellow at CodeX - The Stanford Center for Legal Informatics and a Technology, and Innovation Policy Advisor for the City of San Jose. He is a legal technologist with a passion for privacy and access to justice. Stephen's work primarily focuses on use of facial-recognition technology by governments and law enforcement, as well as on examining the impacts of other emerging technologies. Stephen is a co-founder of the CoronAtlas dashboard, a free pandemic resource open to the general public. He currently serves on the San Jose Digital Privacy Advisory Task Force.

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 to develop actionable policies that can improve the lives of all Americans. For more about the Day One Project, visit dayoneproject.org