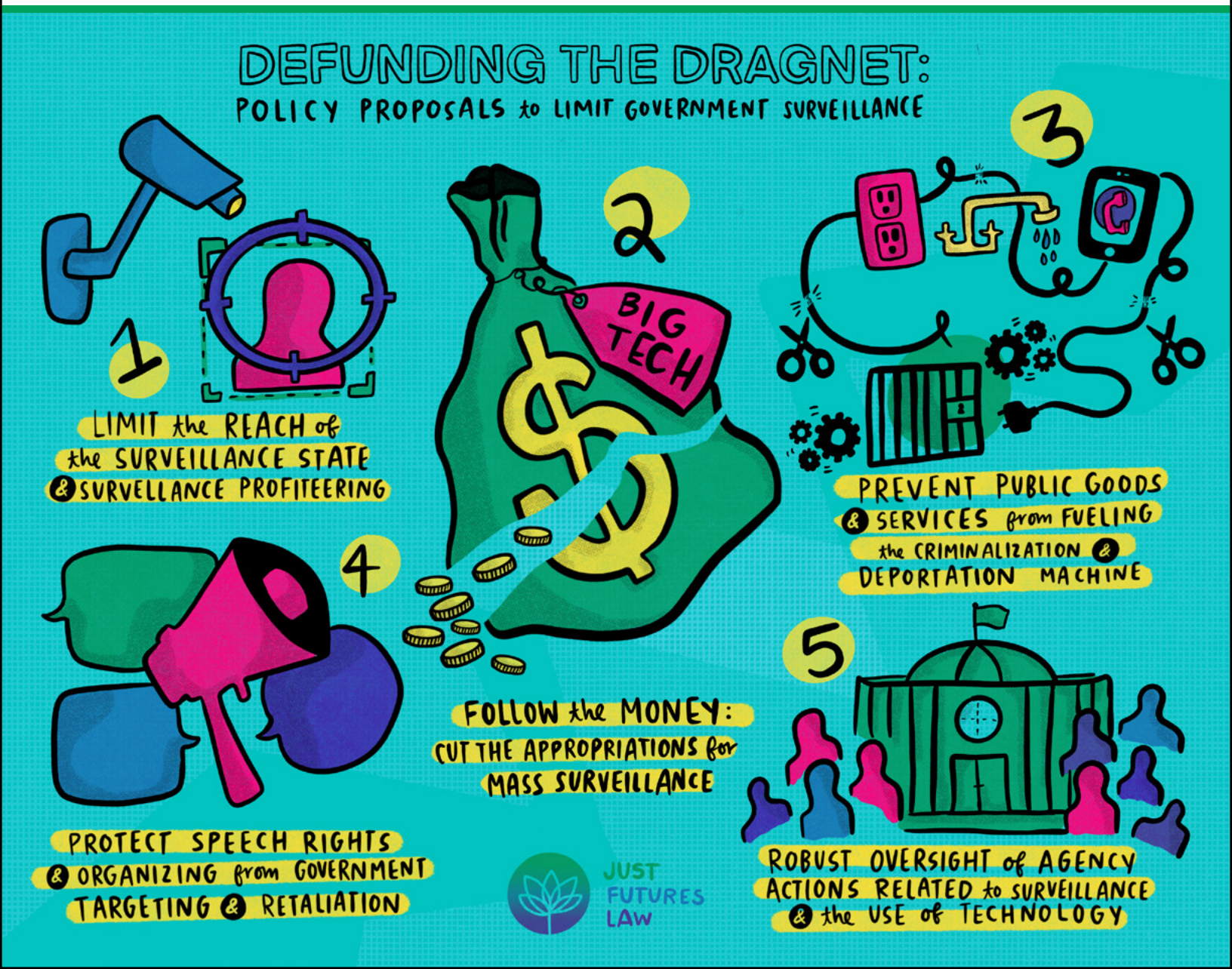
JUST FUTURES LAW

Defunding the Dragnet:

Policy Proposals to Limit Government Surveillance



Contents

Introduction

Federal, state, and local governments must intervene to fight the massive, militarized technological surveillance machine being deployed against Black and Brown communities. Local, state, and federal law enforcement, as well as private companies, are rapidly expanding the use and scope of surveillance technology, leading to abusive criminalization and reducing privacy. The range of powerful tech tools— from Clearview AI's facial recognition tool, to Thomson Reuters and RELX's person-search databases, to Border Patrol drones surveilling Black Lives Matter protesters over Minneapolis—has made clear that law enforcement entities around the country are building massive surveillance systems to track and criminalize both immigrants and native-born U.S. citizens alike. The expansion of these systems has created massive profits for companies who contract with governments at all levels to push criminalization agendas. Policymakers at all levels must end the abusive, racist use of surveillance technology, and shut down its devastating connection to criminalization, detention, and deportation.

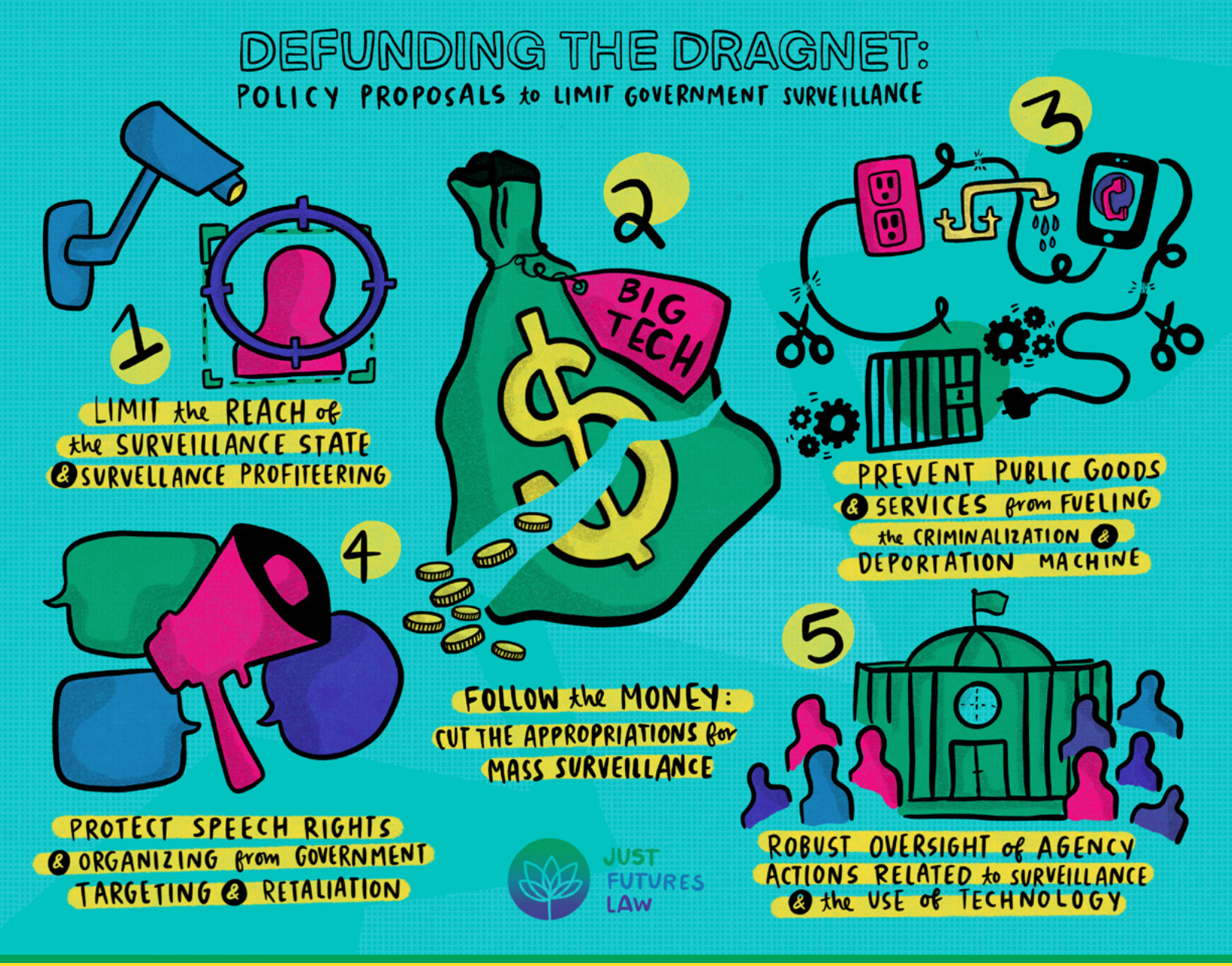
This document compiles policy proposals that advance immigrant rights, racial justice, and broader civil rights and civil liberties. Furthermore, this priorities platform maps existing efforts moving within government and incorporates long-term policy demands raised by organizers and activists around the country. While dismantling harmful and invasive surveillance programs is the goal, this forward-facing document includes concrete steps to address immediate harms and foster the partnerships necessary for more transformative work. We owe particular gratitude to abolitionist organizers, cultural workers, and scholars who have provided key frameworks for assessing advocacy efforts.[1] Our hope is that this document promotes a decarceral, anti-deportation, and surveillance free-agenda, and is used by organizers and policymakers who are actively working to reduce surveillance and criminalization.

This platform implicates government agencies beyond those focused on law enforcement. At the federal level, the expansion of the surveillance state implicates agencies like the Department of Health and Human Services, the Internal Revenue Service, and the Department of Housing and Urban Development, among many others, all of which collect sensitive personal information that either is already used or could be used to facilitate incarceration, detention, and deportation. Other agencies, like the Federal Communications Commission, the Federal Trade Commission, and the Consumer Finance Protection Bureau are also implicated as entities that have the power to regulate abusive data collection practices and protect individuals' privacy rights. At the state and local level, government agency surveillance policies and practices have the potential both to enable federal initiatives and/or to support independent localized criminalization practices.

In response to the variety of government actors implicated in dismantling mass surveillance and its harms, this policy platform is broken down into the following five categories and includes potential policy actions and targets from Executive Branch, Congressional, and state actors.

Priority Areas:

- Limit the Reach of the Surveillance State & Surveillance Profiteering
- Cut Appropriations Dollars for Mass Surveillance
- Prevent Public Goods & Services from Fueling the Criminalization and Deportation Machine
- Protect Speech Rights and Organizing from Government Targeting and Retaliation
- Robust Oversight of Agency Actions Related to Surveillance and the Use of Technology



Our hope is that this document promotes a decarceral, anti-deportation, and surveillance free-agenda, and is used by organizers and policymakers who are actively working to reduce surveillance and criminalization.

PRIORITY #1: Limit the Reach of the Surveillance State & Surveillance Profiteering

Summary: Federal, state, and local governments contract and collaborate extensively with private companies to purchase and develop surveillance policing technologies and enable more efficient criminalization. The mass surveillance industry is growing and lucrative, and many companies are working to create increasingly invasive surveillance tools despite calls from advocacy groups and even tech workers themselves to stop enabling surveillance abuses. In response to the growth of these industries and widespread surveillance profiteering, it is imperative that policymakers create a default assumption against government purchase, development, or investment in invasive technologies and widespread monitoring.

While private companies enable government surveillance abuses, federal, state, and local law enforcement also collect personal information, including biometric data, using their own databases and tools. Policymakers should act to curtail law enforcement's collection of personal information and scrutinize the underlying policies used to justify collection and storage.

Executive Branch

1. Adopt a policy prohibiting the purchase and use of facial recognition technology or information derived from facial recognition technology.[2]
2. Terminate contracts with private companies engaged in the collection and sale of personally identifiable information that is used for law enforcement purposes.
3. End regulations, memoranda, and contracts and/or agreements that expand invasive technologies[3] and biometrics.
4. Initiate coordinated agency strategy to restrict or end collection of biometric data—including face prints, iris, voice prints, and behavioral characteristics for law enforcement purposes. Require agencies collecting any biometric information to implement protective barriers that prevent data sharing with law enforcement entities.
5. End the "Secure Communities" agreement that mandates local and state fingerprint sharing with ICE within the state and local criminal legal system which has further connected criminalization of Black and Brown communities with the deportation machine.

6. Reduce budget of Homeland Advanced Recognition Technology (HART) biometric identification system immediately with a plan to terminate development and use.[4]

Congressional Action

1. Pass legislation that bans agencies from purchasing and using facial recognition technology, biometric surveillance systems, and other invasive technologies.[5] In addition, this legislation should purge existing surveillance databases and end agency authorization for subcontracting with private surveillance companies. Require information collected in violation of this provision be excluded from introduction in federal court proceedings, and excluded from determinations of probable cause.[6] Provide a private right of action and monetary recovery to individuals whose rights are violated.
2. End issuance of federal grants that support local law enforcement purchase of facial recognition technologies or biometric surveillance systems.[7]
3. Repeal existing laws that empower DHS to engage in surveillance and pass laws prohibiting new surveillance.

State and Local Government Action

1. **Executive Action**
    a. Governors, mayors, police departments, and other authorized state and local executives should cancel their contracts with companies that currently provide them with invasive surveillance technologies, and should end the use of surveillance technologies developed through government or public-private partnerships. This should be accompanied by disclosure of any past and current purchases and deployments of surveillance technology by state and local agencies.
    b. Issue policies limiting or banning future purchase and use of invasive surveillance technologies such as facial recognition, cell site simulators or a selection or list of potential technologies as included in footnote 3.[8] As some first potential steps, policymakers should establish a moratorium on all exploration, requests for solicitation, purchases, or future uses of invasive surveillance technologies. Funding should be immediately reduced by 50% for any existing invasive surveillance technology programs.

2. **Legislation**
    a. Pass state and local laws that ban use or purchase of facial recognition, biometric surveillance technology, and biometric data collection.[9] Provide a private right of action for individuals whose information has been collected illegally in violation of these bans.[10] Ensure that state agencies and their contractors are also subject to liability for collecting biometric information in violation of local and state laws.

PRIORITY #2: Follow the Money— Cut Appropriations Dollars for Mass Surveillance[11]

Summary: Over the last 17 years, DHS has become the largest police force in the country in part because of huge budget increases.[12] The overfunding of DHS has led to the increased surveillance, incarceration, deportation and death of immigrants. A 50% reduction in the DHS surveillance budget is a first, tangible step toward limiting the harm of its growing capabilities.[13] As policymakers move toward policies that dismantle surveillance systems, they must immediately divert money away from these areas in order to support more vital priorities. At every level of government, decision makers must reject using government resources to fund mass surveillance to further terrorize communities. State and local governments should put justice ahead of dollars, and should reject federal funding that incentivizes abusive surveillance.

Executive Branch

1. Reduce the amount of funding requested from Congress for DHS biometrics and surveillance programs by at least 50%.

Congressional Action

1. Eliminate federal programs that provide grants to purchase surveillance technologies or the technologies themselves to state and local law enforcement. Relatedly, eliminate requirements in any grants that enable surveillance technology and data sharing between local and federal law enforcement such as through fusion centers or various criminal justice data platforms.[14]
2. Cut the amount allocated to DHS biometrics and surveillance budget by at least 50%.

State and Local Government Action

1. **Executive Action**
    a. Governors, mayors, police departments, and other authorized executives should reject federal funds intended for increasing surveillance collaborations between local, state, and federal law enforcement.[15]
    b. Reduce local and state police surveillance budgets by at least 50%. In addition to helping potentially reduce criminalization and incarceration, this recommendation will protect people from DHS and other federal law enforcement given the extensive information sharing and coordination that occurs between law enforcement entities.[16]
2. **Legislation**
    a. State or local legislators can pass a budget that reduces local and state police funding for surveillance technology. As mentioned above, support for reduced local surveillance budgets also often implicates DHS and federal government surveillance given extensive data sharing.

PRIORITY #3- Prevent Public Goods & Services from Fueling the Criminalization and Deportation Machine

Summary: Increasingly, government surveillance is driven by the exploitation of commercial and public data sources that people would never expect to be connected with law enforcement. As individuals, families, and communities do simple and necessary tasks like pay their water or internet bills, or buy a new cable service for their TV, the government has purchased data collected by commercial actors to access information it otherwise would not be authorized to collect.[17] DHS and ICE then use this information, which often includes people's location history,[18] to make arrests that lead to detentions and deportations. By implicating these basic public services in its mass incarceration and deportation agenda, policymakers further drive a climate of fear in Black and Brown communities, and create the potential of harsh consequences when people simply take the steps necessary to provide for themselves and their families. Government actors at all levels must protect individuals' information regarding seeking these services, and should work to ensure that this information is not repurposed to fuel detention, deportation, and criminalization.

Executive Branch

1. Adopt policy stopping federal law enforcement collection, purchase, search, and use of aggregated information from public services including water, electricity, gas, internet, phone, cell phone, license, banking, and cable services.
2. Review existing data collection sources and end/purge all law enforcement collection that aggregates information related to individuals utilizing utilities and other essential services.

Congressional Action

1. Pass legislation banning federal law enforcement from warrantless collection, search, or utilization of records from services such as water, electricity, gas, internet, phone, cell phone, license, banking, education, and cable services.[19] Purge existing records and databases where this information is aggregated. Require information collected in violation of this provision be excluded from introduction in federal court proceedings and as a basis for establishing probable cause in investigations. Provide a private right of action and monetary recovery to individuals whose rights are violated.
2. Pass legislation that bans private data brokers from collecting and providing information to ICE or other law enforcement agencies.[20]
3. Enact policies that protect personal information collected in relation to important public services and benefits from ending up in the hands of police and other law enforcement.

State Government Action

1. **Executive Action**
    a. Issue policy guidance prohibiting state and municipal run services from sharing personal data with police, private data brokers, and federal government agencies for the purpose of policing and immigration enforcement.[21] Prohibit the sale of this information to third-parties by public service agencies and provide guidance encouraging no data sharing by private actors.
    b. State attorneys general should review existing privacy laws to ensure that any private data sharing is in compliance with state law and bring enforcement actions against private actors who fail to comply with the law.

2. **Legislation**

   a. Pass legislation banning state and local government entities from collecting, searching, or utilizing records from services such as water, electricity, gas, internet, phone, cell phone, license, banking, education, and cable services for law enforcement purposes. Require information collected in violation of this provision be excluded from introduction in state court proceedings and as a basis for establishing probable cause in investigations.[22] Provide a private right of action and monetary recovery to individuals whose rights are violated.

   b. Pass legislation prohibiting private entities from sharing personal data collected as a result of consumer use of services such as water, electricity, gas, internet, phone, cell phone, license, banking, education, and cable services with other third-parties that provide data services to law enforcement, or federal, state, and local law enforcement.

PRIORITY #4- Protect Speech Rights and Organizing from Government Targeting and Retaliation

Summary: Law enforcement entities have used surveillance technologies to monitor the activities of protesters on the front lines of struggles for racial justice, immigrant rights, and environmental justice among others.[23] The targeted surveillance of protesters has chilled speech as law enforcement retaliation against protesters has come to the forefront of the national discourse.[24] Policymakers must directly address the harmful effects of surveillance in relation to grassroots advocacy, and should implement policies that protect speech and end the use of surveillance technology on individuals exercising their speech rights.

Executive Branch

1. End warrantless agency collection of social media identifiers and dragnet collection of social media information. This includes but is not limited to ending dragnet collection in relation to certain hashtags or protest locations and ending social media identifier collection and screening for people traveling to the United States, or who are applying for immigration-related benefits.

2. Adopt a policy prohibiting surveillance and policing of protest activity with drones and other militarized policing tech.
3. Adopt a policy prohibiting federal law enforcement participation in monitoring protests and supporting local law enforcement surveillance in response to protests.

Congressional Action

1. Pass laws prohibiting the use of surveillance technology in monitoring First Amendment-protected protest activities. This includes monitoring political speech on social media platforms. Require information collected in violation of this provision be excluded from introduction in federal court proceedings.[25] Provide a private right of action and monetary recovery to individuals whose rights are violated.

State Government Action

1. **Executive Action**
    a. Adopt policy prohibiting the use of surveillance technology in monitoring First Amendment-protected protest activities. This includes monitoring political speech on social media platforms.
    b. Conduct review and release findings related to all protest-related policing tactics in coordination with human rights advocates and local community members. End tactics that chill speech and limit First Amendment rights and prohibit DHS participation in monitoring protests and supporting local law enforcement in response to protests.
2. **Legislation**
    a. Pass laws prohibiting the use of surveillance technology in monitoring First Amendment-protected protest activities. This includes monitoring political speech on social media platforms. Require information collected in violation of this provision be excluded from introduction in state court proceedings. Provide a private right of action and monetary recovery to individuals whose rights are violated.
    b. Repeal laws and reject legislative efforts that criminalize protest.[26]

PRIORITY #5: Robust Oversight of Agency Actions Related to Surveillance and the Use of Technology

Summary: Given the long history of abuses and continuing harms caused by law enforcement surveillance, robust oversight by empowered independent governmental and non-governmental actors, as well as broad transparency measures, are crucial to ensuring that the most harmful surveillance policies and practices are eliminated. Too often, surveillance and its harms happen in the shadows as a result of policy and practice. This disempowers accountability efforts and allows select groups of law enforcement and security state professionals to dominate narratives about surveillance. While transparency alone does not eliminate the real harms of the surveillance state and its connections to policing and violence against Black and Brown communities, without more tools to investigate, predict, and reveal the extent of government surveillance, efforts toward abolition and immediate harm reduction will be several steps behind on-the-ground realities.

Executive Branch

1. Establish a White House Task Force composed of experts in human rights, immigrants' rights, digital rights, and racial justice to investigate the privacy, civil rights, civil liberties, and human rights implications of government surveillance technologies—in consultation with people from affected communities—and to publish a report on its findings. Include a publicly released audit on DHS and its contractors that collect, analyze, share, store, or purchase personally identifiable information.
2. Ensure that any new technologies used for data collection are contingent on notice and a public comment and findings period.
3. Create a data collection review board housed in the White House Office of Science and Technology Policy that specifically addresses the human rights impacts of existing and future surveillance data collection policies. This board should be staffed by practitioners focused on the human rights and civil rights implications of data collection, and should involve substantial collaboration and coordination with communities most impacted by government surveillance.

Congressional Action

1. Utilize DHS oversight powers to gather information about surveillance technology use by federal officers, including requiring DHS to provide a list of all contracts, contractors, use, and monies deployed for surveillance and technologies.
2. Hold hearings with groups that have been targeted by federal agencies for surveillance to discuss the impact on immigrants and communities of color.

State Government Action

1. **Executive Action**
    a. Require a bi-annual public transparency report about the use of invasive technologies by state law enforcement agencies. Include information about all contracts with private entities, and all data sharing cooperation agreements with state and local government agencies.
    b. Adopt a policy requiring disclosure of any potential law enforcement or non-law enforcement data-sharing agreements and make adoption of any sharing agreement contingent on notice and a period for public comments and findings.
2. **Legislative Action**
    a. Enact laws requiring that any new technologies used for data collection are contingent on notice and a public comment and findings period.[27]
    b. Require state and local agencies to publish quarterly reports detailing existing surveillance technology contracts and uses.[28]

Conclusion

Bold policy actions are necessary at all levels of government to push back against the consistent expansion of already enormous surveillance systems that implicate nearly every aspect of daily life in our communities. We hope groups will strategize on the ideas presented here with other partners, collaborate with us in strengthening this platform, and will use it to spark generative conversations about surveillance and police-free futures.

15 Acknowledgments

WRITER
Dinesh McCoy

EDITORS & PROOFREADERS
Just Futures Law

ILLUSTRATION
Laura Chow Reeve, Radical Road Maps

REPORT LAYOUT DESIGN
Stay Curious Studio

We express our gratitude to Data for Black Lives, Mijente, The Georgetown Center on Privacy and Technology, and The Brennan Center for Justice for providing feedback on this platform.

16 Endnotes

1 *See* Critical Resistance, *Reformist reforms vs. abolitionist steps to end IMPRISONMENT* (2021), http://criticalresistance.org/wp-content/uploads/2021/02/CR_abolitioniststeps_antiexpansion_2021_eng.pdf.

2 Special thanks to the Immigrant Surveillance Working Group— Many demands included here reflect similar demands that members of ISWG developed to share with the incoming-Biden Administration during the transition period.

3 Definition: Invasive surveillance technologies include, but are not limited to surveillance towers such as autonomous sentry towers and fixed surveillance towers

- Remote Video Surveillance Systems (RVSS)
- Thermal imaging, underground sensor, motion sensor, and camera technology
- Aerial surveillance: drones, tethered Aerostat Radar System (blimps)
- Biometric surveillance such as facial recognition, iris, fingerprint, and DNA collection technologies
- Automated License Plate Readers technology including data provided by third-party companies
- Mobile and vehicle forensic software to hack vehicle systems and track mobile location data.
- Data broker tools that aggregate consumer and other types of personal information, including machine learning or AI tools.

4 *See* Jennifer Lynch, *HART: Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' "Non-Obvious Relationships,"* Electronic Frontier Foundation (June 7, 2018), https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and. DHS' Homeland Advanced Recognition Technology (HART) database is intended to replace its current database, Automated Biometric Identification (IDENT). HART will expand IDENT's surveillance potential by storing a huge amount of information about individuals, ranging from their biometric information like facial recognition data, digital fingerprints, and DNA, to their political affiliations, religious activities, and relationship patterns. HART data will make it possible to identify and track people in real time- which chills people's ability to exercise their First Amendment rights to protest, assemble, or associate. It will also greatly expand DHS' ability to locate individuals for deportation enforcement purposes.

The rollout of the HART system has been characterized by delays and consistent re-writing of the contractual agreements with private companies helping to build HART's surveillance infrastructure. It's time the government ends the program altogether rather than invest more in this flawed effort. See GAO DHS Annual Assessment, Jan. 2021, https://www.gao.gov/assets/gao-21-175.pdf.

5 *See* Facial Recognition and Biometric Technology Moratorium Act of 2020, https://www.congress.gov/bill/116th-congress/house-bill/7356/text.

6 *See* e.g., Fourth Amendment Not for Sale Act, 117th Cong. (2021). https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-. This act specifically forbids the introduction of information gathered in violation of the Act as evidence in any state or federal government proceeding.

7 For example, the Facial Recognition and Biometric Technology Moratorium Act of 2020 limits distribution of JAG Byrne grants to localities that similarly ban the use of biometric surveillance systems. However, we do not endorse the use of JAG Byrne grants in any context, and recommend ending all grants that enable police surveillance.

8 *See* note 3 for definitions. For example, after public outcry about Clearview AI's invasive facial recognition technology, Chicago Police Department cancelled its contract with Clearview in May 2020. *Chicago police drop Clearview facial recognition technology*, Associated Press (May 29, 2020), https://apnews.com/article/c354e15c592548eba0e84a7b0702f72e; Los Angeles Police Department banned the use of commercial facial recognition technology like Clearview after more than 25 LAPD employees had performed nearly 475 searches using Clearview AI. Brianna Sacks, et al, *Los Angeles Police Just Banned The Use Of Commercial Facial Recognition*, Buzzfeed (Nov. 17, 2020), https://www.buzzfeednews.com/article/briannasacks/lapd-banned-commercial-facial-recognition-clearview

9 *See* https://epic.org/banfacesurveillance/index.php?c=United%2BStates#country; https://www.banfacialrecognition.com/map/. Jurisdictions around the country have passed facial recognition bans. Portland, Oregon was the first city to ban both private and public-sector use of facial recognition technology. Boston, Cambridge, Northampton, and Brookline, Massachusetts have all banned the use of facial recognition technology, along with Oakland and San Francisco, California. Jackson, Mississippi has banned police from using facial recognition technology. On the state level, California and Oregon have issued prohibitions and moratoriums on facial recognition technology being used on police body cameras.

10 Illinois' Biometric Information Privacy Act (BIPA) provides a private right of action for any person aggrieved by a violation thereof, and permits recovery of statutory damages of $1,000 per negligent violation or $5,000 if the violation is deemed intentional or reckless. Washington and Texas also expressly regulate the collection and storage of individuals' biometric data; however Illinois' BIPA legislation is the most robust by allowing for a private right of action. BIPA specifically allows for recovery of damages even where individualized harm has not been sustained. *See Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 (Ill. 2019) (holding that plaintiffs can pursue BIPA claims even if they have not suffered any actual harm.); *see also Patel v. Facebook Inc.*, No. 18-15982 (9th Cir. Aug. 8, 2019), pet. for rehearing en banc denied, (Oct. 18, 2019) (holding that plaintiffs can pursue BIPA claims even when they have suffered no harm when a BIPA violation amounts to a violation of a substantive privacy right). However, we support even stronger legislation because of BIPA's significant carve-outs allowing biometric data collection by law enforcement.

11 This section accompanies the Just Futures Law fact sheet *In 2021, It's Time for Congress to Defund DHS Surveillance*. While this section focuses on DHS's role in surveillance, as noted previously, many agencies are implicated in the government's proliferation of invasive and abusive use of surveillance technologies.

12 *See* Muzaffar Chishti & Jessica Bolter, *As #DefundThePolice Movement Gains Steam, Immigration Enforcement Spending and Practices Attract Scrutiny*, Migration Policy Institute (June 25, 2020), https://www.migrationpolicy.org/article/defundthepolice-movement-gains-steam-immigration-enforcement-spending-and-practices-attract.

13 *See* Mariame Kaba, *Yes, We Literally Mean Abolish the Police, N.Y.* Times (June 12, 2020), https://www.nytimes.com/2020/06/12/opinion/sunday/floyd-abolish-defund-police.html. Kaba describes the tangible goals of the police and prison abolitionist movement, and argues a 50% reduction in the NYPD budget is an important first step away from investment in mass incarceration and toward a reinvestment in communities toward priorities like health care, housing, education, and good jobs.

14 *See The Silicon Hills Have Eyes*, Just Futures Law, Grassroots Leadership, and BU School of Law, July 2021, *available at* https://www.flipsnack.com/JustFutures/the-silicon-hills-have-eyes/full-view.html.

15 *See* Jasmine Demers, *Pima County supervisors reject Operation Stonegarden grant funding* 3-2, Arizona Daily Star (Feb. 4, 2020), https://tucson.com/news/local/pima-county-supervisors-reject-federal-operation-stonegarden-grant-3-2/article_45e117a6-2344-58ae-b95c-170dd6f4dfa1.html.

16 *See* National Immigration Law Center, *How ICE Uses Local Criminal Justice Systems to Funnel People Into the Detention and Deportation System* (Mar. 2014), https://www.nilc.org/issues/immigration-enforcement/localjusticeandice/.

17 *See* Drew Harrell, *ICE Investigators Used a Private Utility Database Covering Millions to Pursue Immigration Violations*, Wash. Post (Feb. 26, 2021), https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/.

18 *See* Sam Biddle, *Thomson Reuters Defends Its Work for ICE, Providing "Identification and Location of Aliens"*, The Intercept (June 27, 2018), https://theintercept.com/2018/06/27/thomson-reuters-defends-its-work-for-ice/.

19 Legislation could be based on California law that prohibits warrantless data sharing between some public utility companies and ICE. See Public utilities: cooperation with immigation authorities, AB-2788, Assembly Session 2019-2020, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?-bill_id=201920200AB2788. However, our proposal here pushes further than existing legislation.

20 *See* Cora Currier, *Lawyers and Scholars to LexisNexis, Thomson Reuters: Stop Helping ICE Deport People*, The Intercept (Nov. 14, 2019), https://theintercept.com/2019/11/14/ice-lexisnexis-thomson-reuters-database/; see also McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, New York Times Magazine (June 7, 2021), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html. Major data brokers such as Thomson Reuters and RELX have multimillion dollar contracts with ICE, and provide the agency with data ranging from individuals' cellphone registries and social media posts, to information on jail bookings. This data assists ICE in locating and surveilling individuals, and in carrying out enforcement operations and deportations.

21 *See* California public utilities legislation, *supra* note 18. As previously noted, we recommend more robust and protective legislation.

22 *See* note 6 regarding provisions that create exclusionary rule for information gathered in violation of statute.

23 *See* Connie Fossi & Phil Prazan, *Miami Police Used Facial Recognition Technology in Protester's Arrest*, NBC Miami (Aug. 17, 2020), https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/.

24 *See* Zolan Kanno-Youngs, *U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance*, N.Y. Times (June 19, 2020), https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html/.

25 See note 6 regarding provisions that create exclusionary rule for information gathered in violation of statute.

26 *See* Peter O'Dowd & Samantha Raphelson, *More States Propose Legislation To Criminalize Protests*, WBUR (Nov. 20, 2020), https://www.wbur.org/hereandnow/2020/11/20/criminalize-protests-civil-rights; *see also* U.S. Protest Law Tracker, International Center for Non-Profit Law, https://www.icnl.org/usprotestlawtracker/(last updated Sept. 7, 2021).

27 This does not include technologies used exclusively for law enforcement data collection and surveillance purposes, which should be banned.

28 This should include, at a minimum, any technology has been used, how often data was shared with external entities and who those entities are, a breakdown of where technology was deployed and how often, and any violations of the scope of the granted usage of technology.