SURVEILLANCE
RESISTANCE
LAB

Surveillance Resistance Lab

Submission to the Office of the High Commissioner for Human Rights

Responding to the Call for Input on the Secretary-General's Report on the Human Rights of Migrants, Addressing the 2021 General Assembly Resolution on the Protection of Migrants A/RES/76/172

May 12, 2023

This submission is on behalf of the Surveillance Resistance Lab in relation to the use of digital technologies in the context of border governance, regarding the Secretary-General's upcoming report on the Human Rights of Migrants that addresses the 2021 General Assembly Resolution on the Protection of Migrants (A/RES/76/172). Our submission focuses on the ways that digital migration control systems threaten and violate the universal "right to freedom of movement and residence" as well as the "right to leave any country." Particularly in the absence of effective remedy, we are increasingly concerned about the role that digital technologies play in enabling ongoing violations of international human rights law. Our submission focuses on the United States' government's continued and escalating deployment of these technologies, the risks and violations highlighted apply to many other States' use of technologies for migrant control, especially those sharing data and technology systems with the US.[1] This warrants urgent and enhanced scrutiny, regulation, and national and international action.

The Surveillance Resistance Lab is an non-governmental organization based in New York City. We understand state and corporate surveillance to be one of the greatest threats to migrant justice, racial equity, economic justice, and democracy. We conduct investigative research, campaign incubation, and advocacy to fight for accountability and government divestment from technologies that expand systems of control and punishment (as well as suppress dissent and difference) in public spaces, schools, workplaces, and at and across borders. The Lab was formerly the Surveillance, Tech, & Immigration Policing Project, which was housed at the Immigrant Defense Project until 2022.

We are extremely concerned about the massive investment in and use of digital technologies by US Immigration and Customs Enforcement (ICE) and other US Department of Homeland Security (DHS) agencies and the associated ongoing violations and continued threats to human rights—at US international boundaries, within the United States, as well as externally beyond US territory. Digital technologies and the corporations that create, sell, and maintain them are increasingly playing a "mission critical role"—as described by ICE[2]—in advancing the state's ability to fortify border policing regimes and expand surveillance tactics as part of the interior policing deportation apparatus. This includes significant government investment in "smart border" technologies designed to deter and police migrants, as well as ICE's use of increasingly sophisticated surveillance technology in the interior to track, monitor, and target immigrants for detention and deportation.

Technological and business "solutions" have vastly expanded the reach and presence of ICE police in cities and communities throughout the US. This presence is not only physical, with immigration

[1] This includes information and intelligence sharing agreements between the US and Mexico, the Northern Triangle countries (Guatemala, Honduras, and El Salvador), the Five Eyes intelligence-sharing alliance between the US, the United Kingdom, Canada, Australia, and New Zealand, and Israel.

[2] Spencer Woodman, "Palantir Provides the Engine for Trump's Deportation Machine," The Intercept, March 2, 2017, www.theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/.

officers conducting civil arrests at homes, workplaces, the courts, and on the streets—often based on information obtained without consent by tech companies and data brokers[3]—but also a digital presence in all domestic police stations via automatic sharing of biometric and personal information, as well as shared surveillance technologies. For example, Palantir Technologies—a $20 billion data mining firm—built and maintains an intelligence system for DHS that combines data from a range of federal agencies and private law enforcement entities, willfully enabling DHS' deportation machine.[4] The vast digital infrastructure to police immigrants also converges with "smart city" initiatives where corporations provide essential technological tools and infrastructure to urban governments, often claiming that these technologies will expand access to rights and resources.[5] While purportedly aiming to improve government services, these smart cities initiatives are frequently used as tools for policing and punishment—undermining democratic governance and struggles for justice and equality.

ICE and other DHS agencies have a well-documented history of abuse and human rights violations including medical neglect, forced family separation, use of solitary confinement, and psychological torture.[6] These abuses violate numerous international treaties to which the United States is a State Party, including the Convention Against Torture, the International Covenant on Civil and Political Rights, and the International Convention on the Elimination of all Forms of Racial Discrimination. With the emergence of new digital technologies, governments and business enterprises are increasingly enabling, contributing to, and failing to prevent abuses that their actions facilitate, contrary to the foundational principles in General Assembly Resolution 76/172.

Our submission documents four aspects of how the US government deploys digital technologies migration control, including:

- "Smart Border" Technologies Exacerbate the Harms of Migration Control
- Digital Infrastructures of Migration Control: The Everywhere Border
- Invasive and Unreliable Biometrics Collection, Databases, and Sharing
- Data Brokers Fueling Immigration Policing

[3] Mijente, Immigrant Defense Project, and the National Immigration Project of the National Lawyers Guild, *Who's Behind ICE*, 2018, https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf.
[4] Woodman, "Palantir Provides the Engine for Donald Trump's Deportation Machine."
[5] Mizue Aizeki & Rashida Richardson, eds., *Smart-City Digital ID Projects: Reinforcing Inequality and Increasing Surveillance through Corporate "Solutions,"* (New York, NY: Immigrant Defense Project, December 2021), https://surveillanceresistancelab.org/wp-content/uploads/2023/01/Smart-Cities-Digital-IDs-2021.pdf.
[6] Mizue Aizeki, Ghita Schwarz, Jane Shim, and Samah Sisay, "Cruel by Design: Voices of Resistance from Immigration Detention," Immigrant Defense Project and Center for Constitutional Rights, February 2022; Amnesty International, ICE Raids Encourage Hate and Discrimination Toward Immigrants and Communities of Color, July 11, 2019, https://www.amnestyusa.org/press-releases/ice-raids-encouragehate-and-discrimination-toward-immigrants-and-communities-of-color/; Amnesty International, USA "'You Don't Have Any Rights Here': Illegal Pushbacks, Arbitrary Detention & Ill Treatment of Asylum-Seekers in the United States," 2018, https://www.amnesty.org/download/Documents/AMR5191012018ENGLISH.PDF; Jasmine Aguilera, "Here's What to Know About the Status of Family Separation at the U.S. Border, Which Isn't Nearly Over," Time, Oct. 25, 2019, https://time.com/5678313/trump-administration-familyseparation-lawsuit; Carmen Molina Acosta, "Psychological Torture: ICE Responds to COVID-19 With Solitary Confinement," The Intercept, Aug. 24, 2020, https://theintercept.com/2020/08/24/ice-detention-coronavirus-solitary-confinement/; Rachel Treisman, "Whistleblower Alleges 'Medical Neglect,' Questionable Hysterectomies Of ICE Detainees," NPR, Sep. 16, 2020,www.npr.org/2020/09/16/913398383/whistleblower-alleges-medical-neglect-questionable-hysterectomies-of-ice-detaine.

Additional Resources: Please see Annex A for additional reports that further explain these harms, document how digital technologies directly and indirectly expand systemic inequalities in the guise of "neutral" technologies, and share a more comprehensive understanding of the relevant technologies, corporate actors, and pathways for action.

"Smart Border" Technologies Exacerbate the Harms of Migration Control

In recent years, governments including the United States have increased the call for "smart borders"—technologies that serve to manage and control migration at international borders. Yet the rhetoric of "smart borders" merely reinforces a broader regime of border policing and exclusion that greatly harms migrants and refugees who either seek or already make their homes in countries that rely heavily on such technologies such as the United States.

In our 2021 report with the Transnational Institute, *Smart Borders or a Humane World*, we illustrate that the investment in an approach centered on border and immigrant policing is incompatible with the realization of a just and humane world.[7]

As the report traces, the embrace of "smart borders" emerged in the aftermath of 9/11. Smart borders involve the expanded use of surveillance and monitoring technologies including cameras, drones, biometrics, and motion sensors to make a border more effective in stopping unwanted migration and keeping track of migrants. Championing smart borders was—and remains—one of three key pillars of US Customs and Border Protection (CBP) strategy, along with physical barriers and personnel. Smart borders are also embedded in a logic of deterrence, which seeks, by way of militarized border infrastructure, detention, and deportation, to make unwanted migration so brutal and painful that it will dissuade people from even trying to enter the United States without authorization.

The use of technology by US border agencies is not new. As early as 1919, the US government deployed armed aerial surveillance and reconnaissance of the border region. However, contemporary smart borders are unique in the sophistication of the technologies they embody, the scope of the personal data they are able to collect, analyze, and centralize, and the integration of these systems with one another. They are also more extensively used within and beyond the United States than ever before. This is reflected in the increasingly global presence of CBP and Immigration and Customs Enforcement (ICE): as of the report's publication in 2021, the former had 23 offices and the latter 48 offices outside the United States.

In substantiating this position, the report highlights and explores five core harms of US border policing:

1) **A boom in the border and surveillance industrial complex.** Between 2008 and 2020, CBP and ICE issued 105,997 contracts worth $55.1 billion to private corporations—such as CoreCivic, Deloitte, Elbit Systems, GEO Group, General Atomics, G4S, IBM, Leidos, Lockheed Martin, Northrop Grumman and Palantir—with ever more contracts for "smart border" technologies. The spending bonanza has provided a bottomless market for growth. There can never be "total" security

[7] Mizue Aizeki, Geoffrey Boyce, Todd Miller, Joseph Nevins, and Miriam Ticktin, "Smart Borders or a Humane World?" Surveillance Resistance Lab and the Transnational Institute, October 2021, https://surveillanceresistancelab.org/resources/smart-borders-or-a-humane-world/. The Surveillance Resistance Lab was formerly known as the Surveillance, Tech & Immigration Policing Project, housed at the Immigrant Defense Project.

and, thus, there will always be an alleged need for new technology to fill perceived gaps. Failure of any kind helps create a market for the next even more expensive product or service.

2) The growing policing of immigrants and their communities, the borderlands, and society as a whole. Via surveillance technologies, the capacity of the Department of Homeland Security to police and monitor individuals has grown tremendously. On any given day, for example, GPS-enabled ankle monitors are attached to the bodies of tens of thousands of noncitizens. Such targeted forms of surveillance are complemented by passive ones that monitor a growing swath of the US population.[8] This is especially the case with the US borderlands with Mexico and Canada where CBP provides funding and equipment to local police to incentivize cooperation. CBP also uses such technologies to monitor social movements and political speech. In 2020, for example, CBP aerially surveilled Black Lives Matters protests in at least 15 cities. In addition, the capacity to arrest and detain noncitizens has grown dramatically, as ICE has vastly expanded its surveillance arsenal via, among other technologies, mobile fingerprinting devices, and data analytics developed by Palantir to facilitate tracking and targeting of individuals.

3) Separation and undermining of families and communities. Trump's zero-tolerance program made family separation a hot political issue. However, the dividing and harming of families have long been, and continue to be, outcomes of US border and immigration policy. For example, studies show that the arrest, detention, and/or deportation of family members cause symptoms associated with post-traumatic stress disorder. Such symptoms can lead to decline in school performance, negative impacts on health and nutrition, poverty, and economic insecurity—not only for those who have been forcibly deported, but also for those who remain in the United States.

4) The maiming and killing of large numbers of border crossers. The US Border Patrol reports an annual average of 355 deaths between 1998 and 2019, or about one death per day over a twenty-two-year period. Because many bodies are not recovered, however, the true figure is far higher. A strengthened border-policing apparatus has forced migrants to take even more dangerous routes. This has led to a rise in the rate of mortality, which has increased fivefold since 2000, as well as countless injuries to border crossers.

5) Exacerbation of socioeconomic inequality. The growing illegalization and criminalization of immigrant workers reduces their power vis-à-vis employers, increasing exploitability and disposability. During the pandemic, US farm laborers, most of them undocumented, were declared "essential workers" and DHS announced it would adjust its policing operations accordingly. This exposes how many nation-states and the interests they serve view workers as resources to be exploited when needed and discarded when they are not. In doing so, their practices reflect and reinforce class- and race-based distinctions and their associated inequities, contributing to an apartheid-like world. The biggest predictor of which countries construct border walls, and where, is the wealth gap between the nation-state constructing the barrier and the place and population defined as a threat. In other words, the building of walls and policing of international mobility both reflects and produces unequal—and unjust—life-and-death circumstances.

The harms outlined above manifest the extraordinary growth in the budgets for immigration and border policing, which have increased from $1.2 billion in 1990 to $25.2 billion in 2019—a more than

[8] Nina Wang, Allison McDonald, Daniel Bateyko, Emily Tucker, *American Dragnet: Data-Driven Deportation in the 21st Century*, Center on Privacy & Technology at Georgetown Law, 2022, https://americandragnet.org/.

2,000 percent jump in less than thirty years. Today's budget rivals total spending by some of the world's largest militaries: in 2019, CBP and ICE spending almost matched the military budgets of Australia, Brazil, and Italy, while exceeding those of Canada, Israel, Spain, and Turkey.

This growth reflects a political choice rather than an inevitable state of affairs. It is predicated on the purported need for massive investment in border policing in response to an ever-expanding range of manufactured threats. Yet it never seeks to address any of the root causes of unwanted migration, such as global economic inequality, intensifying climate crisis, failures of multilateral trade policy, and political violence.

We must move beyond a narrow debate limited to "hard" versus "smart" borders toward a discussion of how we can move toward a world where all people have the support needed to lead healthy, secure, and vibrant lives. A just border policy would ask questions such as: How do we help create conditions that allow people to stay in the places they call home, and to thrive wherever they reside? When people do have to move, how can we ensure they are able to do so safely? When we take these questions as our starting point, we realize that it is not enough to fix a "broken" system. Rather, we need to reimagine the system entirely.

Digital Infrastructures of Migration Control: The Everywhere Border

On February 14, 2023, the Surveillance Resistance Lab, along with partners at R3D (Red en Defensa de Derechos Digitales) and the Temple University Institute for Law Innovation and Technology published an article in the Transnational Institute's *State of Power: Digital Futures*, "The Everywhere Border—Digital Infrastructures of Migration Control."[9] The article focuses on the implications of the digital border infrastructure that the US is building in neighboring countries. This digital infrastructure expands and deepens surveillance, while often concealing the state violence of migration control.

In the piece, we illustrate that we need to understand border externalization through the lens of digital infrastructure in order to capture the true scale of border practices envisaged by the US (and its competitors and allies) as well as their envisaged permanence within the future world order. Digital border infrastructure feeds on histories of domination, control, and atrocities in the name of transnational "crime-fighting" projects, setting the stage for tremendous social costs.

The first concern is scale—we are witnessing an escalation of US border imperialism and borderland violence—both in terms of geographical reach far into national territories and the further extension of "policeability" to an increasing number of individuals and groups through this digital infrastructure. This includes anyone an algorithm decides might be "dangerous," those who might migrate, as well as humanitarian actors, migrant advocacy groups, and aid organizations. Scaling and the rapid growth it engenders is a quintessential property of digital technologies, regardless of their origin or application. The shifts to new targets under digital infrastructure are frictionless compared to earlier analogue-based border policing tactics. The second concern is permanence, as advocates of digital borders in national capitals, industry and development agencies embrace the term "digital public infrastructure" as a brand, to bestow (unearned) trust, normalization, and the inevitability of contested digital tools such as biometric identification and payment systems.

[9] Mizue Aizeki, Laura Bingham, and Santiago Narváez, ""The Everywhere Border: Digital Migration Control Infrastructure in the Americas," *State of Power: Digital Futures,* The Transnational Institute, 2023, https://www.tni.org/en/article/the-everywhere-border.

We argue that ceding the privilege of defining "digital infrastructure" to actors with vested interests in current migration-control practices is reckless. Without a counter narrative that articulates their violent disposition, digital border externalization tools—including widespread biometrics collection, real-time transaction data-collection in payment systems, and the confiscation of smartphones at the border—can easily be normalized as "digital public infrastructure," rather than resisted.

Invasive and Unreliable Biometrics Collection, Databases, and Sharing

Tech is increasingly deployed to expand the state's ability to track, catalog, sort, and target people. Digital databases greatly facilitate the sharing of information across policing agencies—domestic, federal, and increasingly foreign. This data sharing is growing exponentially, often with inadequate safeguards to protect privacy and civil liberties and with few mechanisms for redress.

Our 2022 report, *HART Attack: How DHS's Massive Biometrics Database will Supercharge Surveillance and Threaten Rights*, published with Just Futures Law and Mijente, investigates how the Department of Homeland Security's Homeland Advanced Recognition Technology System (HART) will vastly expand its surveillance capabilities and supercharge the deportation system.[10] Below, we explain first the context of DHS' data infrastructure and use of biometrics collection, and then highlight the main concerns and risks of HART.

1) **DHS deployment of biometrics surveillance technologies**

DHS' data infrastructure includes the collection of invasive and unreliable biometrics, such as DNA and facial recognition, on hundreds of millions of people[11] and vast amounts of biographic, personal, and relational data.[12] For example, DHS and its agencies, including ICE and Customs and Border Protection (CBP), have been vastly expanding its collection of DNA. In 2019, CBP started to conduct Rapid DNA tests on recent border crossers—a context in which people have very few legal protections. In 2020, the federal government began collecting DNA from all people in ICE detention to be stored in the FBI DNA database, which is searchable by policing agencies across the country.[13] Similarly, DHS databases rely on facial recognition technology, which grants State and private actors the unprecedented ability to identify, locate, and track individuals.

This raises serious civil and human rights and civil liberties concerns; one of the most alarming is how the technology can fuel and justify systemic racism against Black people and other over-policed communities. Police use of facial recognition continues to grow even though it has been repeatedly demonstrated to be less accurate when used to identify Black people, people of Asian descent, people

[10] Mijente, Just Futures Law, and Surveillance Resistance Lab, "HART Attack: How DHS's Massive Biometrics Database will Supercharge Surveillance and Threaten Rights," 2022, https://surveillanceresistancelab.org/resources/smart-borders-or-a-humane-world/. The Surveillance Resistance Lab was formerly known as the Surveillance, Tech & Immigration Policing Project, housed at the Immigrant Defense Project.

[11] U.S. Department of Homeland Security, DHS/OBIM/PIA-004, "Homeland Advanced Recognition Technology System (HART) Increment 1 PIA," February 24, 2020.

[12] Immigrant Defense Project, Just Futures Law, and Mijente, "Freeze Expansion of the HART Database," April 2021, https://justfutureslaw.org/wp-content/uploads/2021/04/HART-Appropriations-2022.pdf

[13] Saira Hussain, "DOJ Moves Forward with Dangerous Plan to Collect DNA from Immigrant Detainees," Electronic Frontier Foundation, June 10, 2020, https://www.eff.org/deeplinks/2020/03/doj-moves-forward-dangerous-plan-collect-dna-immigrant-detainees.

aged 18-30, and women, in particular women of color.[14] The government is also increasingly reliant on algorithms to make critical determinations—such as granting entry to the country or release from detention—even though these algorithms have been repeatedly proven to reinforce racist and other structural biases.[15]

Biometric technologies pose an unprecedented threat to individuals' privacy and security, beyond inaccuracy—which increased accuracy rates will not address. Over the past several years, face recognition systems in the US have been used to criminalize poverty, facilitate mass arrests and incarceration of ethnic and racial groups, surveil demonstrators exercising their First Amendment rights at protests, and target immigrants for deportation.[16] The *New York Times* has reported that ICE officials had mined state license databases using facial recognition technology, analyzing millions of driver photos without people's knowledge.[17] Clearview AI, a software company that significantly expands the reach of facial recognition, has built a massive facial recognition database by scraping and scanning billions of personal photos from the Internet, including social media sites—without consent.[18] The company claims that, through this enormous database, it can instantaneously identify the subject of a photograph with unprecedented accuracy. Clearview AI sells access to this trove of personal, private information to law enforcement agencies, private businesses, and international entities and police departments, including those in countries with anti-LGBTQ laws.

This business is incredibly lucrative, and corporations have little motivation—or, when it comes to securing government contracts, incentive—to follow international standards around transparency, due diligence, and redress.

2) The development and dangers of the Homeland Advance Recognition Technology (HART) system:

In 2016, DHS launched the development of the Homeland Advance Recognition Technology System (HART), likely the largest biometric and biographic database in the US, which will turbocharge tracking, detention, and deportation of immigrants. This $6.158 billion-dollar, next-wave biometric

[14] Alex Najibi, "Racial Discrimination in Face Recognition Technology," Harvard University: Science in the News, October 26, 2020, https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

[15] Adi Robertson, "ICE rigged its algorithms to keep immigrants in jail, claims lawsuit," *The Verge,* March 3, 2020, https://www.theverge.com/2020/3/3/21163013/ice-new-york-risk-assessment-algorithm-rigged-lawsuit-nyclu-jose-velesaca.

[16] Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." *The New York Times*, The New York Times, 18 Jan. 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; "Ban Facial Recognition Technology." *Amnesty International*, 7 Jan. 2022, https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/. See also Amnesty's Ban the Scan campaign at https://banthescan.amnesty.org/.

[17] Catie Edmondson,"ICE Used Facial Recognition to Mine State Driver's License Databases." The New York Times, The New York Times, 8 July 2019, https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.

[18] For more information, please review this FOIA request submitted by the Immigrant Defense Project, Mijente, Just Futures Law, and the American Civil Liberties Union of Northern California in 2020: https://www.immigrantdefenseproject.org/wp-content/uploads/2020/10/2020.10.19-ACLU-NC-JFL-IDP-Mijente-FOIA-re-Clearview-AI_.pdf

database will collect, organize, and share invasive data on over 270 million people (including juveniles), with that number projected to grow significantly.[19] This data will come from federal agencies including DHS and the FBI, as well as local and state police, and foreign governments.

Built with military-level technology, HART was initially developed by military defense contractor Northrop Grumman,[20] whose federal IT department was then acquired by a private equity firm, Veritas Capital, for $3.4 billion.[21] DHS has contracted with Amazon to store HART's data on Amazon Web Services GovCloud.[22] Despite Congressional concerns about the project's development and ever-expanding budget,[23] DHS does not hold these companies accountable for accuracy, quality, or due diligence, and they face little to no public oversight. According to the required Privacy Impact Statement on HART's first phase, DHS does not vouch for the data's accuracy since the data is owned by third party providers, does not hold itself responsible to obtain consent for data collection or use,[24] and has directly acknowledged third party sharing as a particular risk. Despite these concerns and admissions, DHS will retain and use this data for at least 75 years.[25]

HART will aggregate and compare biometrics data including facial recognition, DNA, iris scans, fingerprints, and voice prints—most often gathered without obtaining consent or a warrant. Under HART, DHS will also allow officers to enter subjective personal and "encounter" data—including people's supposed relationships, political beliefs,and religious affiliations—without verification and with little oversight. This will allow DHS to target immigrants for surveillance, raids, arrests, detention, and deportation. HART could be used to identify people in public spaces, creating chilling consequences for people's rights to protest, assemble, associate, and to live their daily lives. HART threatens to violate human and privacy rights at an exponential rate, particularly in Black, brown, and immigrant communities already facing discriminatory policing and surveillance.

Despite the terrifying risks, HART remains a black box—shrouded in secrecy with virtually no oversight and accountability mechanisms. The mechanisms to seek redress or obtain remedy are non-existent or wholly unrealistic. While troubling questions over its privacy and human rights

[19] Mijente, Just Futures Law, and Surveillance Resistance Lab, "HART Attack."

[20] "Northrop Grumman Wins $95 Million Award from Department of Homeland Security to Develop Next-Generation Biometric Identification Services System," Northrop Grumman Newsroom, February 26, 2018, https://news.northropgrumman.com/news/releases/northrop-grumman-wins-95-million-award-from-department-of-homeland-security-to-develop-next-generation-biometric-identification-services-system.

[21] Valerie Insinna, "Northrop sells IT business to Veritas Capital for $3.4B," Defense News, December 8, 2020, retrieved Jan 19, 2022.

[22] Jack Corrigan, "DHS to Move Biometric Data on Hundreds of Millions of People to Amazon Cloud." *Nextgov.com*, Nextgov, 13 Apr. 2021, https://www.nextgov.com/it-modernization/2019/06/dhs-move-biometric-data-hundreds-millions-people-amazon-cloud/157837/.

[23] "Department of Homeland Security Appropriations Bill, 2022, Report 117-87,"Committee on Appropriations, 117th Congress," p. 21-24. https://www.congress.gov/117/crpt/hrpt87/CRPT-117hrpt87.pdf; Explanatory Statement for the Homeland Security Appropriations Bill, 2022." https://www.appropriations.senate.gov/imo/media/doc/DHSRept_FINAL.PDF

[24] U.S. Department of Homeland Security, DHS/OBIM/PIA-004, "Homeland Advanced Recognition Technology System (HART) Increment 1 PIA," February 24, 2020, 18. https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf.

[25] Currently, international records are retained for 75 years, and law enforcement records are retained for 75 years after the end of the calendar year in which it was collected. DHS, DHS/OBIM/PIA-004, 28.

violations remain, Congress continues to fund HART, even though it has failed to meet every milestone in its government contract.

Data Brokers Fueling Immigration Policing

We are also deeply concerned with States' use of third-party data brokers in immigration policing activities.[26] ICE relies heavily on information supplied by data broker firms, such as Thomson Reuters (Westlaw) and LexisNexis (RELX), which supply troves of personal data to police. Data brokers facilitate use of data that far surpasses its intended reason for collection; this "mission creep" can result in arbitrary, and sometimes unlawful, invasive surveillance programs that target immigrants.

Our 2022 submission with Just Futures Law, Media Justice, Mijente, and the UCLA Center on Race and Digital Justice to the US Federal Trade Commission raises alarm about the pervasive use of commercial data products in government dragnet surveillance programs and calls for prohibition of their use. [27]

Data brokers collaboration with DHS and ICE raises alarms around privacy and consent, as well as civil rights violations. While people may initially provide some data freely—to apply for a drivers license or to pay a utilities bill—there is no way for an individual to know their data will be shared with third parties and subsequently police and immigration enforcement, or for them to retract consent. This data is fed into case management systems, databases, and intelligence sharing systems, some managed by third party companies, and fuels biased predictive policing programs, nonconsentful data collection, and invasive surveillance that marginalize immigrants, and lead to detention under conditions that often violate human rights, including family separation, and deportation. The scale of this data collection by commercial enterprises is unprecedented: for example, LexisNexis states that its consumer databases include 10,000 different data points on hundreds of millions of people, with its products often marketed to law enforcement.[28]

Alarmingly, data brokers undermine local and state laws, including "sanctuary" policies that prohibit data sharing between local law enforcement and federal immigration agencies. Data brokers' systems allow DHS to buy data that they would otherwise have to acquire from local agencies, through massive privatized databases.[29] This represents a mass violation of immigrants' rights to privacy and is then used to facilitate DHS and ICE's abuses of human rights. In addition to facilitating detention and deportations that separate families and communities, this creates intense fear for immigrants,

[26] Sarah Lamdan, "When Westlaw Fuels Ice Surveillance: Legal Ethics in the Era of Big Data Policing," New York University Review of Law & Social Change 255 (2019), Available at SSRN: https://ssrn.com/abstract=3231431; "Immigrant Rights Groups, Law School and Legal Organization FOIA for Info on Thomson Reuters, RELX Group Contracts with ICE," Sept. 2020, https://ccrjustice.org/home/press-center/press-releases/immigrant-rights-groups-law-school-and-legal-organization-foia-info.

[27] Just Futures Law, Media Justice, Mijente, Surveillance Resistance Lab, and the UCLA Center on Race and Digital Justice, "Comments to the Federal Trade Commission, Trade Regulation Rule on Commercial Surveillance and Data Security," 2022, https://surveillanceresistancelab.org/wp-content/uploads/FTC-Comment-Commercial-Surveillance.pdf. The Surveillance Resistance Lab was formerly known as the Surveillance, Tech & Immigration Policing Project, housed at the Immigrant Defense Project.

[28] Sam Biddle, "LexisNexis to Provide Giant Database of Personal Information to ICE," The Intercept (Apr. 2, 2021), https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/.

[29] Biddle, "LexisNexis to Provide Giant Database of Personal Information to ICE."

especially undocumented people, and creates insurmountable barriers to access of basic government services and rights.

The US government's pervasive and increasing use of digital technologies for migration control requires urgent action to address ongoing harms, human rights abuses, and violations of UN principles and international law.

For questions, please contact:

Alli Finn
Senior Researcher and Organizer
Surveillance Resistance Lab
info@surveillanceresistancelab.org

Annex A: Additional Reports

Please see additional reports below that further explain how digital technologies directly and indirectly expand the harms of migration control, and entrench systemic inequalities in the guise of "neutral" technologies.

- "The Everywhere Border—Digital Infrastructures of Migration Control," co-published by the Surveillance Resistance Lab, R3D (Red en Defensa de Derechos Digitales), and the Temple University Institute for Law Innovation and Technology in the Transnational Institute's *State of Power: Digital Futures*" article focuses on the implications of the digital border infrastructure that the US is building in neighboring countries. This digital infrastructure expands and deepens surveillance, while often concealing the state violence of migration control.
- *Smart Borders or A Humane World*, co-published by the Surveillance Resistance Lab and the Transnational Institute, explores the role of tech in a broad regime of border policing and exclusion that greatly harms migrants and refugees who either seek or already make their home in the US.
- *HART Attack: How DHS's Massive Biometrics Database will Supercharge Surveillance and Threaten Rights* co-published by the Surveillance Resistance Lab, Just Futures Law, and Mijente, investigates how the Department of Homeland Security's Homeland Advanced Recognition Technology System (HART) will vastly expand its surveillance capabilities and supercharge the deportation system.
- *Who's Behind ICE: The Tech Companies Fueling Deportation*, published by the Immigrant Defense Project, Mijente, and NIPNLG, details the central role tech companies play in supporting ICE's mass detention and deportation regime.

Please note that some of the Surveillance Resistance Lab's reports were previously published under our former name as the Surveillance, Tech, and Immigration Policing Project, housed at the Immigrant Defense Project.