Submission to the Office of the High Commissioner for Human Rights on the practical application of the United Nations Guiding Principles on Business and Human Rights to the activities of technology companies

This submission is on behalf of the Immigrant Defense Project's (IDP's) Surveillance Tech and Immigration Policing project, and the Center for Constitutional Rights (CCR), in response to the Office of High Commissioner's call for stakeholder input on Resolution 47/23, "New and emerging digital technologies and human rights." We address the growing ecosystem of public-private surveillance of migrants and immigrants in the United States, and the ways that the State and business enterprises consistently violate all three core Guiding Principles on Business and Human Rights.[1] Our submission focuses on the ways that technology companies fuel the US government's surveillance, invasive biometrics collection, policing, detention, and deportation of migrants. To draw on the risks that the resolution itself highlights, State actors including the US Department of Homeland Security (DHS) and technology companies jointly threaten and violate citizens' and noncitizens' "right to equality and non-discrimination, the right to freedom of opinion and expression, the rights to freedom of peaceful assembly and freedom of association, the right to an effective remedy and the right to privacy."[2] Particularly in the absence of effective remedy, private companies' enabling of ongoing violations of international human rights law warrants enhanced scrutiny, regulation, and national and international action.

IDP is an NGO based in New York that works to ensure fairness and justice for immigrants at the intersection of the criminal legal and immigration systems.[3] CCR, a New York-based organization, works with communities under threat to fight for justice and liberation through litigation, advocacy, and strategic communications.[4] We are extremely concerned about the massive investment in and use of digital technologies by US Immigration and Customs Enforcement (ICE) and other DHS agencies, and the ongoing violations and continued threats to human rights arising from that collaboration. 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.[5]

[1] The UN Guiding Principles (UNGPs) are grounded in the following general principles, which underpin the "protect, respect, remedy" three-pillar framework:
   a. States' existing obligations to respect, protect and fulfill human rights and fundamental freedoms;
   b. The role of business enterprises as specialized organs of society performing specialized functions, required to comply with all applicable laws and to respect human rights;
   c. The need for rights and obligations to be matched to appropriate and effective remedies when breached.

[2] General Assembly resolution 47/23, *New and emerging digital technologies and human rights*, A/HRC/RES/47/23 (13 July 2021), available at https://undocs.org/A/HRC/RES/47/23.

[3] For more information on IDP, visit https://www.immigrantdefenseproject.org/. For more info on IDP's Surveillance, Tech & Immigration Policing Project, visit https://www.immigrantdefenseproject.org/surveillance-tech-immigration-policing/.

[4] For more information on CCR, visit www.ccrjustice.org.

[5] 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.

These abuses violate numerous international treaties to which the US 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, business enterprises are increasingly enabling, contributing to, and failing to prevent abuses that their services facilitate, contrary to the foundational principles in the UNGPs Pillar II. While our submission focuses on the US, the risks and recommendations apply to other States' use of technologies for migrant control, especially those sharing data and technologies with the US.[6]

Expansion of Tech-Enabled Immigration Raids, Detention, and Deportation:

Since the 2002 establishment of DHS, civil society has been confronted by the growth of the world's largest system to arrest, detain, deport, and exclude migrants. Digital technologies and the corporations that create, sell, and maintain them are increasingly playing a "mission critical role"—as described by ICE—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. Our submission provides an overall picture of the violations of the Guiding Principles in the context of the US' migrant control efforts; we encourage OHCHR and the Working Group on Business and Human Rights to review the additional reports in Annex A for a comprehensive understanding of the relevant technologies, corporate actors, and pathways for action.

IDP has been tracking ICE's community arrests and raids in the New York City area since 2013 to monitor and analyze trends in ICE arrests and detention, and share that information with community members, advocates, and elected officials.[7] Over the years, the "mission critical" role that tech plays in ICE policing has become an increasing concern.[8] This is not a case of passive administration or misuse of technology. 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.[9] Partnerships like these present clear violations of the Guiding Principles, with both the State and business enterprise in violation of human rights.

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 officers conducting civil arrests at homes, workplaces, the courts, and on the streets—often based on

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, https://www.npr.org/2020/09/16/913398383/whistleblower-alleges-medical-neglect-questionable-hysterectomies-of-ice-detaine.

[6] 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.

[7] For information on IDP's ICEWatch work, see raidsmap.immdefense.org.

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

[9] Ibid.

information obtained without consent by tech companies and data brokers[10]—but also a digital presence in all domestic police stations via automatic sharing of biometric and personal information, as well as shared surveillance technologies. 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.[11] 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.

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, in violation of the third Guiding Principle.

DHS' data infrastructure includes the collection of invasive and unreliable biometrics, such as DNA and facial recognition, on hundreds of millions of people[12] and vast amounts of biographic, personal, and relational data.[13] 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.[14] 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 aged 18-30, and women, in particular women of color.[15] The government is also increasingly reliant on algorithms to make critical determinations—such as granting

[10] 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.

[11] 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://www.immigrantdefenseproject.org/wp-content/uploads/smart-city-digital-id-products.pdf.

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

[13] 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

[14] 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.

[15] 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/

entry to the country or release from detention—even though these algorithms have been repeatedly proven to reinforce racist and other structural biases.[16]

Biometric technologies pose an unprecedented threat to individuals' privacy and security, beyond inaccuracy. 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.[17] Last year, the *New York Times* reported that ICE officials had mined state driver's license databases using facial recognition technology, analyzing millions of driver photos without people's knowledge.[18] 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.[19] 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. In 2016, DHS launched the development of the Homeland Advance Recognition Technology System (HART), likely the largest biometric and biographic database in the US, to turbocharge tracking, detention, and deportation of immigrants. 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

[16] 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.

[17] 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/.

[18] 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.

[19] For more information, please review this FOIA request submitted by IDP, 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

[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

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. Under HART, DHS will 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. The mechanisms to seek redress or obtain remedy are non-existent or wholly unrealistic.

Data Brokers Fueling Immigration Policing:

We are deeply concerned with States' use of third-party data brokers in immigration policing activities.[25] ICE relies heavily on information supplied by data brokers, 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. This raises alarms around privacy and consent, as well as civil rights violations. While people may initially provide some data freely—to apply for a driver's 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, nonconsensual data collection, and invasive surveillance that marginalize immigrants, and lead to detention under conditions that often violate human rights, including family separation, and deportation.

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.[26] In addition to facilitating detention and deportations that separate families and communities, this creates intense fear for immigrants, especially undocumented people, and creates insurmountable barriers to access of basic government services and rights.

Digital IDs and Smart City Initiatives:

The push for digital IDs has further undermined individual and collective rights. Business enterprises—including those that lobby for, administer, and profit off these technologies—have sold "smart city" interventions including digital IDs as "solutions" to streamline benefits distribution, expand access to

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] 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.

[26] https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/

legal identification, and address underbanking. However, case studies from India,[27] Kenya,[28] South Korea,[29] Uganda,[30] and across the US have repeatedly found violations of privacy, civil, and human rights. Digital IDs have also been shown to increase discrimination, expose States and individuals to massive data breaches, and increase state and corporate surveillance. Most concerningly, digital ID systems and their corporate administrators have furthered systemic exclusion of people with disabilities, the elderly, trans and non-binary individuals, noncitizens, and minority groups. In 2007, for example, the state of Indiana contracted with IBM to outsource and automate its welfare system; over the first three years of the project, more than 700,000 residents were systematically denied benefits. The ACLU brought a class action lawsuit that focused on discrimination against disabled applicants, and Indiana later sued IBM for breach of contract based on denial errors.[31]

While Digital IDs and smart city initiatives are often discussed in a different sphere than surveillance and the police-to-deportation pipeline, they are intimately linked and share a foundation of corporate disregard and violations of human rights, in exchange for profit. We encourage the Working Group and other bodies to apply the same level of scrutiny to digital IDs, to interrupt the ways that States and business enterprises use them to systemically track, monitor, exclude, and discriminate groups of people.

Additional Resources:

See Annex A for reports that further explain how business enterprises expand the power of policing and punishment, and entrench systemic inequalities in the guise of "neutral" technologies.

Recommendations:

In practice, and with the development of emerging digital technologies, the Guiding Principles do little to impact the behavior of companies or States, or to hold them to account for past and ongoing harms. We call for:

- **A holistic and rights-responsive framework that can begin to meaningfully address the problem through inclusive and innovative accountability measures.** This framework must move beyond policy commitments. For example, both Thomson Reuters and RELX Group are members of the United Nations Global Compact,[32] but continue to perpetrate and facilitate

[27] "Initial Analysis of Indian Supreme Court Decision on Aadhaar," Privacy International, September 26, 2018, https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar; Usha Ramanathan, "The Function Creep That Is Aadhaar," Wire, April 25, 2017, https://thewire.in/government/aadhaar-function-creep-uid.
[28] Varun Baliga, "Kenya's Huduma Namba: Ambition Fraught With Risk," Mondaq, June 30, 2020, https://www.mondaq.com/ southafrica/privacy-protection/960004/kenya39s-huduma-namba-ambition-fraught-with-risk.
[29] "South Korean ID System to Be Rebuilt from Scratch," BBC News, October 14, 2014, https://www.bbc.com/news/ technology-29617196.
[30] Katelyn Cioffi et al., "Chased Away and Left to Die," Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness, June 8, 2021, https://chrgj.org/wp-content/ uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf, 8
[31] Virginia Eubanks, "Caseworkers vs. Computers," Virginia Eubanks, December 12, 2013, https://virginia-eubanks.com/2013/12/11/caseworkers-vs-computers/.
[32] The UN Global Compact is a voluntary initiative based on CEO commitments to support UN goals, including commitments to uphold human rights and make sure that they are not complicit in human rights abuses. Thomson Reuters, as a part of their approach to acknowledge social impact, states their commitment to the United Nations

ongoing violations by ICE. Voluntary commitments do little to address the degree to which powerful technology companies' actions transcend national and international law. Moreover, companies must not be permitted to claim any form of "derivative immunity" or otherwise invoke their relationship with States to evade liability when they further human rights violations.

- **Companies must carry out meaningful human rights due diligence and refuse to contract** with States when potential or actual human rights violations are identified.
- **Comprehensive regulation, prohibitions, and limitations on corporate and State data collection, sharing, and sale, and the use and sale of surveillance technologies and biometrics collection, especially when used without informed consent.** This is necessary to protect and restore basic civil and human rights. The mechanisms for this are complex and require further consultation, discussion, and cooperation.
- **Dedicated sessions held by the Working Group and other UN actors on the role of technology companies in abuses of migrant, immigrant, and refugees, as well as violations linked to surveillance technologies,** as soon as possible. People most affected by these issues must be meaningfully consulted and their needs followed in these discussions and policy decisions.
- **Deeper investigation into the specific practices of implicated business enterprises and technology companies,** including those named in this submission, past civil society submissions including,[33] and *Who's Behind ICE*, including but not limited to Amazon, LexisNexis, Thomson Reuters, and Palantir.

These steps are urgently necessary to address past and ongoing violations of the Guiding Principles and fundamental human rights.

For questions, please contact:

Alli Finn
Senior Researcher, Surveillance, Tech & Immigration Policing Project
Immigrant Defense Project
STIP-team@immdefense.org

Global Compact. More information is available at: https://www.thomsonreuters.com/en/about-us/social-impact.html; RELX Group, as a part of their corporate responsibility, states their commitment to the United Nations Global Compact. More information is available at: https://www.relx.com/corporate-responsibility/engaging-others/working-with-the-un.

[33] In particular, see the past submission from Access Now on "The Surveillance Industry and Human Rights" at https://www.ohchr.org/_layouts/15/WopiFrame.aspx?sourcedoc=/Documents/Issues/Opinion/Surveillance/ACCESS%20NOW.docx&action=default&DefaultItemOpen=1 and from Mijente on the role of private companies in immigration and border enforcement at https://www.ohchr.org/_layouts/15/WopiFrame.aspx?sourcedoc=/Documents/Issues/Mercenaries/WG/ImmigrationAndBorder/mijente-submission.pdf&action=default&DefaultItemOpen=1.

Annex A:

Additional Reports

Below are links to additional reports that further explain how business enterprises expand the power of policing and punishment, entrenching systemic inequalities in the guise of "neutral" technologies. These reports also offer possible alternatives and pathways to action, which can be applied to further OHCHR inquiry on this issue.

- *Who's Behind ICE: The Tech Companies Fueling Deportation*, published by IDP, Mijente, and NIPNLG, details the central role tech companies play in supporting ICE's mass detention and deportation regime.
- *Smart Borders or A Humane World*, co-published by IDP 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.
- *Smart-City Digital ID Projects: Reinforcing Inequality and Increasing Surveillance*, co-published by IDP and Northeastern University's Center for Law, Information & Creativity, examines the harms of digital IDs that integrate financial services, transit payment functions, and access to government services.
- Our 2020 *Freedom of Information Act Request: ICE and DHS Contracts with RELX Group and Thomson Reuters*, submitted on behalf of IDP, CCR, Mijente, and the City University of New York School of Law's Human Rights and Gender Justice Clinic, asks for crucial information on DHS and ICE contracts with commercial information technology and data service providers, and how these data broker firms' services enable immigration enforcement operations. The request raises unanswered questions that could form a blueprint for future inquiries to the US and private companies.