Before the
DEPARTMENT OF JUSTICE & DEPARTMENT OF HOMELAND SECURITY
Washington, DC

In the Matter of	)	
	)	
Impact of Facial Recognition and Other Technologies on Privacy, Equity, and Civil Rights	)	REQUEST FOR COMMENT
	)	
	)	
	)	
	)	

COMMENTS OF UNITED WE DREAM AND ALLIED ORGANIZATIONS

January 19, 2024.

EXECUTIVE SUMMARY

United We Dream (UWD) is the largest immigrant youth-led community in the United States. UWD is a national non-profit, non-partisan, membership-based organization comprising more than 1.2 million immigrant youth and their allies, with more than 100 affiliate organizations located in 28 states. UWD's primary purpose is to advocate for the dignity and fair treatment of immigrant youth and their families of all immigration statuses—including the protection of immigrant civil rights from unethical law enforcement practices.

United We Dream acknowledges the administration's decision to initiate a public comment period for evaluating the impact of law enforcement technologies and practices on privacy, civil rights, and civil liberties. For far too long, public and private entities, including law enforcement agencies, tech companies, digital platforms, and data brokers with questionable ethics, have been complicit in the weaponization of personal information and systematic surveillance of underserved populations, perpetuating unjust law enforcement practices in violation of civil rights.

The use of facial recognition technology, biometric information, and predictive algorithms by law enforcement agencies, along with their practices in collecting, processing, and storing personal data from commercial databases, significantly affects the privacy and civil rights of immigrant communities. This issue falls under the scope of Executive Order 14074. While Congress continues to deliberate on privacy and consumer data, the administration must formulate a comprehensive framework for safeguarding civil rights against unethical surveillance practices by law enforcement and commercial entities, ensuring the protection of private data for all individuals, irrespective of their immigration status.

United We Dream (UWD) and its partner organizations are dedicated to empowering immigrant communities and ensuring their voices are heard in the ongoing conversation regarding privacy, civil rights, and civil liberties. We hold that law enforcement agencies should be accountable for their unrestrained use of technologies that facilitate the harassment and surveillance of immigrant communities and communities of color.

I. Digital Surveillance Practices and their Impact on Immigrant Civil Rights:

As a network of undocumented youth, United We Dream deeply works with immigrant communities by monitoring law enforcement abuses from immigration agencies like ICE; providing assistance in deportation cases; and striving to hold federal, state, and local governments accountable for any unlawful or unethical law enforcement practices. The following technologies and law enforcement methods currently in use pose significant threats to both the safety of the immigrant communities we advocate for and the protection of their civil rights and constitutional liberties:

Facial Recognition Technology:

Facial recognition technology provides law enforcement agencies with extraordinary powers to recognize, track, and surveil people, which poses major concerns for civil rights, human rights, and civil liberties. A key worry is the impact of this technology on communities of color and other over-policed groups, further drawing them into the criminal justice and immigration systems. The technology is purportedly able to match faces captured by law enforcement agencies to private and commercial databases, which includes vulnerable immigrant and undocumented communities, and raises questions about the accuracy and reliability of the data being used and the potential for wrongful arrests, detentions, and deportations.[1]

Across the country, law enforcement agencies utilize facial recognition services provided by vendors like Clearview AI, which are connected to databases containing over 3 billion biometric identifiers. These identifiers are extracted from images gathered from various social media platforms, including Facebook, Instagram, and LinkedIn without consent, an action that breaches privacy and constitutional rights.[2]

---

[1] ACLU. (2020). *Freedom of Information Act Request Regarding Use of Clearview AI Facial Recognition Software.*
https://www.immigrantdefenseproject.org/wp-content/uploads/2020/10/2020.10.19-ACLU-NC-JFL-IDP-Mijente-FOIA-re-Clearview-AI_.pdf
Hill, K. (2020). *Wrongfully Accused by an Algorithm.* New York Times.
https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.
Edmundson, C. (2019*). ICE Used Facial Recognition to Mine State Driver's License Databases.* New York Times.
https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html

[2] Letter from Civil Rights Organizations to DHS' Secretary Alejandro Mayorkas (2021).
https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/635ff4cacc6d405fe7827911/1667232970273/Clearview-AI-sign-on-letter.pdf

The application of this technology goes beyond social media platforms, encompassing other databases such as DMV records. A report from 2022 revealed that facial recognition technology has been applied to the driver's license photos of 32% of U.S. adults. Furthermore, it was found that 74% of these individuals have their driver's license information accessible to ICE without the need for a search warrant.[3]

Facial recognition technology subjects immigrant communities to intensified scrutiny, with its inherent algorithmic biases often incorrectly identifying individuals from various immigrant backgrounds. This increases the risk of unjust arrests, detentions, and deportations. Studies have shown that individuals of color and Asian people are up to 100 times more likely to be misidentified than white men, depending on the specific facial recognition software and context.[4] The technology has even mistakenly matched legislators of color with criminal mugshots.[5]

Moreover, many facial recognition algorithms inaccurately determine the gender of transgender and gender non-conforming individuals, and some claim to ascertain a person's sexual orientation, reinforcing damaging stereotypes about the LGBTQIA+ community.[6] Misidentifications by this technology present an increased risk to young immigrants, who are more likely to have an extensive online presence from an early age, making their digital personal data readily accessible to law enforcement agencies. This data can then be utilized in facial recognition technology, amplifying the potential for errors and misidentification. These inaccuracies can lead to wrongful detentions, convictions, and deportations, disproportionately affecting members of the United We Dream network and the communities they represent - young, diverse immigrants of varying gender identities and sexual orientations.

---

[3] Georgetown Law Center on Privacy & Technology. (2022). *American Dragnet.* https://americandragnet.org/
Edmundson, C. (2019*). ICE Used Facial Recognition to Mine State Driver's License Databases.* New York Times. https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html

[4] Harwell, D. (2019). *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*. Washington Post. https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

[5] ACLU of Northern California. (2019). *Facial Recognition Technology Falsely Identifies 26 California Legislators with Mugshots*. https://www.aclunc.org/news/facial-recognition-technology-falsely-identifies-26-california-legislators-mugshots

[6] Taylor, V. (2019) *Facial recognition misclassifies transgender and non-binary people, study finds.* https://www.mic.com/impact/facial-recognition-misclassifies-transgender-non-binary-people-study-finds-19281490

The dangers posed by facial recognition technology cannot be ignored by regulators. It is imperative to establish a comprehensive framework that safeguards the privacy and rights of all individuals, regardless of their immigration status. The unrestricted use of this technology by enforcement agencies is a threat to civil rights and should be strictly prohibited.

Data Collection Practices:

It has long been understood that law enforcement agencies, such as ICE and CBP, seek personal information for surveillance purposes. Yet, what is particularly concerning is their willingness to gather this data through unethical means, showing a blatant disregard for civil liberties. The Fourth Amendment of the Constitution is intended to protect individuals from unwarranted intrusions by the government, yet federal agencies have identified and exploited legal loopholes, allowing them to covertly collect personal data without a warrant. This data, encompassing our activities, associations, and locations, is compiled, processed, and stored by data brokers, who then share this sensitive personal information with government entities.[7]

For immigrant communities, this loophole frequently turns into a mechanism for detention and deportation, allowing immigration enforcement agencies, such as ICE and CBP, to track, intimidate, and detain immigrants by using their private information and geo-location data. This is done without adhering to proper legal processes, often breaching the agencies' own policies and regulations.[8]

Over the past decade, ICE and CBP have increasingly exploited the data broker loophole to conduct systematic surveillance. A recent investigation by the Georgetown Center on Privacy & Technology revealed that ICE has accessed private databases like CLEAR, containing extensive records such as phone, water, and electricity bills, to monitor and apprehend members of immigrant communities. This report also disclosed that ICE can trace the new addresses of almost three-fourths of U.S. adults whenever they initiate a new utility or service account.[9]

However, this surveillance extends beyond utility bills. Federal court filings have shown that ICE gathers a wide array of data from sources like LexisNexis, Ventell, and Babel Street. This includes, but is not limited to, real-time geolocation data, search histories, DMV records,

---

[7] Center for Democracy & Technology (2021). Legal Loopholes and Data for Dollars. https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/

[8] Cox, J. (2023). *ICE, CBP, Secret Service All Illegally Used Smartphone Location Data*. 404 Media. https://www.404media.co/ice-cbp-secret-service-all-broke-law-with-smartphone-location-data/

[9] Georgetown Law Center on Privacy & Technology. (2022). *American Dragnet.* https://americandragnet.org/

child welfare information, credit details, employment and health records, housing information, family ties, and social media activities.[10]

Moreover, contrary to claims that cellphone location data is not personally identifiable information (PII), numerous studies have shown that so-called "anonymized" mobile location data can be re-identified with up to 85% accuracy. Such capabilities allow government agencies to pinpoint and follow the movements of specific individuals or groups in targeted areas, such as border towns or immigrant neighborhoods. This enables them to extract intimate details about our private lives and associations, far exceeding the bounds of anonymity and civil liberties.[11]

The unethical and unlawful access to private data by law enforcement agencies is central to enabling systemic surveillance tools, including facial recognition technology and predictive algorithms. Personal data lies at the heart of digital surveillance and is integral to civil rights protections. It is incumbent upon regulators to develop and enforce frameworks that increase transparency regarding data practices and dealings with commercial entities that gather, process, and store this data. These agreements should adhere to strict federal guidelines, ensuring adherence to constitutional safeguards like the necessity of a search warrant and due process, while upholding individuals' rights to their personal information.

---

[10] Rivlin-Nadler, M. (2019). *How ICE Uses Social Media to Surveil and Arrest Immigrants.* The Intercept.
https://theintercept.com/2019/12/22/ice-social-media-surveillance/
Biddle, S. (202). *ICE Searched LexisNexis Database Over 1 Million Times In Just Seven Months.* The Intercept.
https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances/
ACLU. (2022). *FOIA Litigation Documents*.
https://www.aclu.org/cases/aclu-v-department-homeland-security-commercial-location-data-foia
Khabbaz, D. (2022). *DHS's Data Reservoir: ICE and CBP's Capture and Circulation of Location Information.* Epic.
https://epic.org/documents/dhss-data-reservoir-ice-and-cbps-capture-and-circulation-of-location-information/

[11] Tewari, S & Walter-Johnson, F. (2022). *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data.* ACLU.
https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data
Eshun, S & Palmieri, P. (2022). *Two De-anonymization Attacks on Real-world Location Data Based on a Hidden Markov Model.* IEEE.
https://ieeexplore.ieee.org/abstract/document/9799345/authors#authors

Predictive Algorithms and Denial of Due Process:

As previously mentioned, data collected by the ICE and CBP are a source of great concern for privacy and civil liberties advocates. The information gathered by these agencies has significant implications for the lives of immigrant communities in the U.S. One of the key ways in which this data can be used is to make decisions about who is allowed to enter the country and who may be subject to expedited removal proceedings.[12] This practice empowers Customs and Border Protection (CBP) officers to deport immigrants without any chance for review by either an immigration officer or a judge.[13] This is particularly concerning considering that immigrants, such as asylum seekers, frequently face restricted access to legal advice. This, combined with a possible lack of understanding of immigration laws and existing language hurdles, significantly diminishes their chances of appealing or challenging decisions.[14]

The use of Automated Decision-Making (ADM) Systems in immigration law enforcement, while offering efficiency gains for agencies, simultaneously triggers significant legal and ethical concerns under both domestic and international frameworks. These systems, such as ICE's Risk Classification Assessment System (RCA), have been subject to political misuse by anti-immigrant administrations, which has led to ICE's RCA showing trends of favoring indefinite detention in the past.[15] The RCA is also employed to advise ICE officers on whether a detained immigrant should be kept in custody or released on bond.[16]

In the face of increasing opposition to asylum and lawful migration channels, such as humanitarian parole, from anti-immigrant lawmakers in Congress and possible future Federal administrations, it becomes crucial to implement stringent transparency and oversight measures

---

[12] MacCarroll. E. (2020).*Weapons of Mass Deportation: Big Data and Automated Decision-Making Systems in Immigration Law.* Georgetown Immigration Law Journal. https://www.law.georgetown.edu/immigration-law-journal/in-print/volume-34-number-3-spring-2020/weapons-of-mass-deportation-big-data-and-automated-decision-making-systems-in-immigration-law/

[13] See 8 C.F.R. 235.3(b) (2017); 69 Fed. Reg. 48877, 48879 (Aug. 11, 2004)

[14] Eagly, I & Shafer, S (2019). *Access to Counsel in Immigration Court*. American Immigration Council. https://www.americanimmigrationcouncil.org/sites/default/files/research/access_to_counsel_in_immigration_court.pdf

[15] Koulish, R. (2017). *Immigration Detention in the Risk Classification Assessment Era*. https://cpilj.law.uconn.edu/wp-content/uploads/sites/2515/2018/10/16.1-Immigration-Detention-in-the-Risk-Classification-Assessment-Era-by-Robert-Koulish.pdf

[16] Ferro, S. (2018) *ICE's Bond Algorithm Has One Response: Detain.* Above the Law. https://abovethelaw.com/2018/06/ices-bond-algorithm-has-one-response-detain/

for the use of predictive algorithms in enforcing immigration policies. This is necessary to ensure that these practices adhere to and respect civil, human, and constitutional rights.[17]

Many United We Dream (UWD) members are DACA recipients, eligible for DACA, or protected under other statutes like TPS or DED. With DACA's future uncertain due to ongoing legal challenges and possible termination, the lives of more than 600,000 individuals connected to UWD's network are at risk, and millions more if we account for mixed-status households.[18] The unregulated access and use of private information, including biometric data from shared databases, enables ICE to identify potential undocumented immigrants interacting with local law enforcement. This holds true even in "sanctuary cities," where such data would typically not be shared with ICE. The integration of this biometric data with automated decision-making systems intensifies worries about the fate of immigrant youth and their families.[19] The exact implications of these algorithmic applications by future administrations remain unclear.

The urgent need to safeguard the privacy and due process rights of all individuals, irrespective of immigration status, cannot be overstated. The unchecked agreements between law enforcement and private data repositories have inflicted considerable harm, infringing upon fundamental privacy and civil liberties. Furthermore, the lack of transparency and regulatory control over predictive algorithms in immigration enforcement poses a substantial risk to the human and civil rights of immigrants. Now is the time for regulatory bodies to intervene and create a comprehensive legal framework to curtail these practices and technologies. This framework should aim to restrict the gathering of commercial data by agencies like ICE and CBP, and guarantee that the use of algorithms does not compromise civil rights and due process safeguards.

II. Regulators, legislators, and other stakeholders should approach the civil rights and equity implications of digital surveillance with a focus on protecting immigrant rights and promoting fairness and equity:

In light of these pressing issues, UWD urges the Department of Justice (DOJ) and the Department of Homeland Security (DHS) to implement the following general recommendations:

---

[17] Immigrant Law Center of Minnesota. (2023). *Asylum Under Attack.* https://www.ilcm.org/latest-news/asylum-under-attack-call-congress-now/

[18] Forward.us. (2023). *DACA Court Case Updates: Summary of Litigation and Potential Supreme Court Case.* https://www.fwd.us/news/daca-court-case/

[19] Mijente, Immigrant Defense Project & the National Immigration Project of the National Lawyers Guild. (2018). *Who's Behind ICE? The Tech and Data Companies Fueling Deportations.* https://www.immigrationresearch.org/system/files/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations.pdf

Immediate Halt to Unethical Data Practices: Cease the use of facial recognition technology, biometrics, and predictive algorithms until comprehensive policies are in place to safeguard civil rights and ensure due process.

Transparency and Accountability: Institute transparent guidelines governing the acquisition, development, testing, and use of these technologies, ensuring community input and oversight.

Prohibition of Data Broker Usage: Enact regulations explicitly prohibiting immigration enforcement agencies from obtaining data from commercial data brokers without a warrant, adhering to Fourth Amendment protections.

Protecting Marginalized Communities: Regulators, legislators, and other stakeholders should take into account the unique risks and challenges faced by marginalized communities, including immigrant communities, people of color, and low-income populations. These groups are often more vulnerable to the negative consequences of commercial data collection and processing and should be given special protections.

Community Impact Assessments: Conduct thorough impact assessments on immigrant communities, considering the potential harm and disparate impact of these technologies on various demographic groups.

Strengthen Privacy Safeguards: Implement robust privacy controls and safeguards, particularly for vulnerable communities like undocumented immigrants, ensuring the protection of personally identifiable information (PII) and biometric data.

Promoting Fairness and Accountability: Regulators should work to ensure that their vendors are held accountable for any negative impacts their data collection and processing practices have on individuals and communities. This could include imposing fines, strengthening requirements for federal contracts between agencies and third-party vendors, requiring companies to take corrective actions, or even revoking companies' licenses to operate as federal vendors.

Supporting Research and Education: Regulators, legislators, and other stakeholders should support research and education initiatives that help individuals understand the implications of commercial data collection and digital surveillance as well as how they can protect their rights and privacy. This could include public education campaigns, research projects, and legal support for individuals who have been affected by these practices.

United We Dream emphasizes the urgent need for the DOJ and DHS to prioritize the protection of civil rights, ensuring fair treatment, due process, and dignity for all, irrespective of immigration status. We stand united in advocating for a just and equitable approach to technology use in law enforcement, free from violations of constitutional rights.

III. The following principles should guide the administration in addressing disproportionate harms experienced by immigrant communities due to unethical business practices related to commercial data collection, processing, and sharing:

1. *Transparency:* Companies should be transparent about their data collection, processing, and sharing practices and provide individuals with clear and accessible information about what data they collect and how it is used. Transparency must include straightforward options for individuals to reduce, customize, and opt-in to data collection and use by companies. Companies must provide full transparency with regard to the data collection processes, including the sources of the collected data, the parties with whom the data is shared, the methodology employed for data analysis to create consumer profiles, the scope of usage for the collected data, the criteria used for determining the provision of goods, services, and content, and the measures implemented to ensure the security of collected data.
2. *Accountability:* Companies should be accountable for their data practices, including ensuring that they comply with privacy laws and regulations and that individuals have the right to access, rectify, and delete their personal data. The administration should advance regulations that ban the collection and utilization of harmful and unnecessary data. Consumers should not be forced to sacrifice their privacy, service quality, or other rights by providing information to use a service, especially when such data is not necessary for delivering the promised service.
3. *Privacy by Design:* Data collection, processing, and sharing practices should be designed with privacy in mind, and companies should take proactive measures to protect privacy, including that of immigrant and undocumented individuals. This includes government-owned platforms and contracts with commercial data brokers.
4. *Data Minimization:* Companies should only collect, process, and share the minimum amount of personal data necessary for their business purposes, including data about an individual's immigration status. The administration should promote policies that reduce the scope of data collection, storage, and sale of individual information while setting limits on the kind of data that can be collected and the surveillance of users by businesses.
5. *Respect for Human Rights:* Data collection, processing, and sharing practices should respect human rights, including rights to privacy and due process, and not violate the dignity of immigrant and undocumented individuals.
6. *Access to Remedies:* Individuals, including immigrant and undocumented communities, should have access to remedies in the event of privacy violations, including the ability to seek compensation for harm suffered, without fear of immigration retaliation.

7. *Non-Discrimination:* Companies should not discriminate against individuals based on immigration status, race, ethnicity, or other protected characteristics, and should not assist in the profiling or targeting of immigrant and undocumented communities. The DOJ should advance regulations to guard against digital discrimination towards groups that are protected under civil rights laws and enforce penalties for companies that do not comply with existing civil rights frameworks.

***

This comment was prepared by United We Dream (UWD) and partner organizations from the digital civil rights and tech accountability sector, and immigrant rights movement. Member signatories include:

Fight for the Future

Free Press

Kairos Action

Media Alliance

Muslim Advocates

Tierra Común

UCLA Center for Critical Internet Inquiry

United We Dream

Xīn Shēng | 心声 Project