Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, DEPARTMENT OF COMMERCE
Washington, DC

In the Matter of	)	
	)	
Privacy, Equity, and Civil Rights Request for Comment	)	NTIA-2023-0001
	)	
	)	
	)	
	)	

COMMENTS OF UNITED WE DREAM AND TWENTY-TWO ALLIED ORGANIZATIONS

March 6, 2023.

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 business practices.

United We Dream applauds NTIA's initiation of a public comment period to assess the rules concerning the impact of commercial surveillance and data security on civil rights. For far too long, public and private entities, including tech companies, digital platforms, data brokers, and government agencies with questionable ethics, have controlled the personal information of underserved populations, perpetuating unjust and deceptive practices.

The way in which data is collected, processed, stored, and sold has a direct impact on the civil rights of immigrant communities and is a matter of utmost importance that falls under the scope of the NTIA, which has a proven track record in navigating complex privacy issues in the past and advising the President on this topic. Despite existing laws and ongoing conversations in Congress regarding privacy and consumer data, the NTIA must ensure the administration develops a framework to establish a federal standard for protecting civil rights against commercial surveillance and harmful business models concerning users' private data—regardless of immigration status.

United We Dream (UWD) and twenty-two partner organizations are dedicated to empowering immigrant communities and ensuring their voice is heard in the ongoing conversation regarding data privacy rights. We believe that everyone has the right to control their personal information and are working to ensure these rights are protected for immigrant communities.

I. Digital Surveillance and its Impact on Civil Rights and Immigration Practices:

Digital surveillance is increasingly widespread and puts privacy and civil rights at risk. This is particularly concerning for undocumented immigrants, who are especially susceptible to the negative consequences of data collection and processing practices by immigration enforcement agencies, such as Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP)[1].

[1] Loweree, J. (2020). *How Immigration Enforcement Is Eroding Your Privacy.* Immigration Impact. https://immigrationimpact.com/2020/03/13/data-privacy-ice/

Immigration Enforcement:

Immigration enforcement agencies such as ICE can utilize data obtained from social media and online marketplaces to locate and apprehend undocumented immigrants for deportation and family separation[2]. The ability of these agencies to collect and use data from social media and online marketplaces to locate and target undocumented immigrants for deportation undermines their privacy, due process, and equal protection rights. The use of commercial data to profile individuals based on their race, national origin, ethnicity, and other characteristics inevitably results in discriminatory practices and unequal treatment by law enforcement, which causes enormous harm to individuals and communities who are already marginalized and at a higher risk of discrimination.

Moreover, the use of unreliable data in immigration enforcement can lead to wrongful arrests, increased detention, and family separation. This can have a devastating impact on individuals and their families and can result in a lack of due process and a violation of their civil rights. It is important for regulators to examine the use of data in immigration enforcement closely and to ensure that the privacy and civil rights of individuals are protected. The implementation of strong privacy laws and oversight mechanisms can help prevent the abuse of data collection and processing practices by immigration enforcement agencies.

Facial Recognition and Border Surveillance:

The use of facial recognition technology by law enforcement has raised several concerns regarding privacy and civil rights, particularly regarding its use in immigration enforcement. The technology is purportedly able to match faces captured on surveillance cameras to private and commercial databases of known individuals, 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 and detentions.[3]

[2] Rivil-Nadler, M. (2019, December 22). *How ICE Uses Social Media to Surveil and Arrest Immigrants*. The Intercept. https://theintercept.com/2019/12/22/ice-social-media-surveillance/

[3] 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.

Customs and Border Protection (CBP) can access personal data and use facial recognition technology at entry points, airports, border communities, and immigrant neighborhoods to identify and detain individuals who are suspected of being undocumented or overstaying their visas, undermining due process protections and resulting in wrongful convictions.[4] CBP's new mobile app, CBP One, is the latest attempt by immigration enforcement agencies to access and collect personal information to target vulnerable immigrant communities, which poses significant privacy and civil rights concerns without oversight. [5]

The dangers posed by facial recognition technology cannot be ignored by regulators. It is imperative to establish a comprehensive legal 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. To ensure a just and equitable society, facial recognition technology must be kept in check and used only in carefully regulated circumstances.

Denial of Due Process:

The 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.

https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html

[4]Davis, J. *Walls Work*. U.S. Customs and Border Protection (Accessed February 24, 2022) https://www.cbp.gov/frontline/border-security

Funk, M. (2019) *How ICE Picks Its Targets in the Surveillance Age*. The New York Times. https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html

Li, E. (2021) *Mass and Intrusive Surveillance of Immigrants Is an Unacceptable Alternative to Detention*. Center for Democracy and Technology. https://cdt.org/insights/mass-and-intrusive-surveillance-of-immigrants-is-an-unacceptable-alternative-to-detention/.

Buolamwini, J & Gebru, T. (2018) *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

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-manyfacial-recognition-systems-casts-doubt-their-expanding-use/.

[5] Pinto, R. (2021). *The New CBP One App May Put Immigrants and Travelers' Privacy at Risk.* Immigration Impact. https://immigrationimpact.com/2021/08/05/cbp-one-app-privacy-risks/

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 without due process protections.[6] This is a concerning development, as it puts the lives and freedoms of immigrant communities at risk and results in increased harassment of immigrants by law enforcement and systemic violations of civil rights and the right to seek asylum at the border.

It is imperative that we act immediately to protect the privacy and rights of every individual, regardless of their immigration status. The unrestricted contracts between law enforcement agencies and data brokers have caused significant harm and violated basic privacy and civil liberties. It is time for regulators to step in and establish a robust legal framework to rein in these practices. The framework must be designed to limit the collection of commercial data by enforcement agencies such as ICE and CBP, and ensure that the privacy and rights of all individuals are inviolable.

II. Targeted Violence Against Immigrant Communities as a Result of Discriminatory Algorithms and Harmful Business Models:

The impact of harmful algorithms and adverse business models on immigrant communities constitutes a pressing issue that requires scrutiny by the NTIA. These practices, inherently driven by biased data and motivated by profit, can perpetuate harmful stereotypes and discrimination against immigrants and other minority groups. This has resulted in a marked increase in incidents of hate crimes and violence against immigrant, and Black and brown communities. The deployment of these algorithms and models puts at risk the life and integrity of immigrant and Black and brown communities, raising questions regarding the influence of these models on targeted violence based on race, ethnicity, nationality, and more. Addressing these issues requires the NTIA to scrutinize the implications of these practices and promote the ethical and responsible use of technology in order to ensure the protection of immigrant populations.[7]

Political targeting:

Political campaigns and advocacy organizations can leverage data from commercial data brokers and platforms to design and deliver their messages to a specific audience. This approach

[6] 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/

[7] Crawford, K. (2016). The Hidden Biases in Big Data. Harvard Business Review. https://hbr.org/2013/04/the-hidden-biases-in-big-data

allows these organizations to carefully select and target voters based on their specific interests, beliefs, and behaviors. In the case of anti-immigrant sentiments, these organizations can use the data to identify individuals who hold such views, and then deliver messages that appeal to their emotions and mobilize them to take action.[8]

However, this approach can also result in negative consequences for immigrant communities. For example, the spread of xenophobic propaganda and radicalization can take place when individuals are repeatedly exposed to messages that demonize immigrant communities and portray them as a threat to society. This can further fuel hatred and discrimination towards these communities, leading to the incitement of violence against them.

In addition, the use of data to target political messages can also lead to the creation of echo chambers, where individuals are only exposed to messages that align with their beliefs and views. This can limit their exposure to diverse perspectives, leading to a reinforcement of their existing biases and further entrenchment of their anti-immigrant sentiments.

It's crucial for organizations involved in political targeting to exercise caution and responsibility in the use of data and to ensure that their messages do not incite hate and violence against any particular community.

Promotion of xenophobic content:

Private tech companies implement business models that promote content that maximizes engagement and profit from amplifying white nationalism and dangerous conspiracy theories like the Great Replacement Theory which has inspired violence in places like El Paso, Texas, and Buffalo, New York.[9]

The Great Replacement Theory is a white supremacist conspiracy theory that falsely claims that white populations are being deliberately replaced by non-white immigrants and that this is being carried out through a deliberate plot by political and economic elites, among other false anti-semitic claims. This theory has been widely discredited by experts, yet it continues to

[8] Lewis, B & Marwick, A (2017). *Media Manipulation and Disinformation Online.* Data & Society.
https://datasociety.net/library/media-manipulation-and-disinfo-online/

[9] Merrill, J & Oremus, W. (2021). *Five points for anger, one for a 'like': How Facebook's formula fostered rage and misinformation*. The Washington Post.
https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/
Ranking Digital Rights. (2022) *It's the Business Model: How Big Tech's Profit Machine is Distorting the Public Sphere and Threatening Democracy.*
https://rankingdigitalrights.org/its-the-business-model/.

be promoted by some tech companies through their content recommendation algorithms and advertising practices.

These companies implement business models that prioritize engagement and profits over the responsible dissemination of information. It is imperative that private tech companies take responsibility for the content that they promote and implement measures to prevent the spread of xenophobic content and dangerous conspiracy theories. This may involve implementing more stringent content moderation policies, better monitoring of content recommendations, and partnering with experts and organizations that are dedicated to promoting responsible and accurate information.

III. Commercial Data Collection and Service Discrimination:

Commercial data collection and processing practices can prevent immigrant communities from getting access to equal economic opportunities and financial services. Some of the adverse effects of these practices include but are not limited to:

> *Job discrimination*: Employers can use data from commercial data brokers and background check companies to make decisions about who to hire, which can result in discrimination against immigrant workers[10].
>
> *Housing discrimination*: Landlords can use data from commercial data brokers to screen tenants and make biased decisions about who to rent to, which can disproportionally affect immigrant families subjected to prejudice and xenophobia.[11]
>
> *Banking*: Banks and other financial institutions can use data from commercial data brokers to make decisions about who to approve for loans, credit cards, and other financial products, which can result in financial discrimination against immigrants[12].

[10] Milner, Y &Traub, A. (2021). *Data Capitalism and Algorithmic Racism*. Data for Black Lives & Demos.
https://www.demos.org/research/data-capitalism-and-algorithmic-racism.

[11] Hershberger, S. (2022). *What Big Data Reveals About Modern-day Housing Segregation*. Washington University in Saint Louis Magazine.
https://artsci.wustl.edu/NeighborhoodBranding

[12] *Banking on Your Data: the Role of Big Data in Financial Services*: Hearing before Task Force on Fin. Tech. of the House Comm. on Fin. Serv., 116th Cong., at 9 (Nov. 21, 2019) (statement of Dr. Christopher Gilliard),
https://financialservices.house.gov/uploadedfiles/chrg-116hhrg42477.pdf.

IV. Regulators, legislators, and other stakeholders should approach the civil rights and equity implications of commercial data collection and processing with a focus on protecting immigrant rights and promoting fairness and equity:

Establishing clear regulations: There should be clear and enforceable regulations that set standards for how data can be collected, processed, and used by tech companies. These regulations should be designed to protect individual privacy and prevent the misuse of personal information.

Ensuring transparency: Tech companies should be required to be transparent about the data they collect, how it is processed, and who it is shared with. This will help individuals understand what information is being collected about them and how it is being used.

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.

Promoting fairness and accountability: Regulators, legislators, and other stakeholders should work to ensure that tech companies are held accountable for any negative impacts their data collection and processing practices have on individuals and communities. This could include imposing fines, requiring companies to take corrective actions, or even revoking their licenses to operate.

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 processing and 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.

V. Existing US laws and regulations provide limited privacy protections for immigrant communities.

Despite the importance of privacy in a democratic society, existing U.S. laws and regulations provide limited protections for these communities. This raises serious questions about the ability of these communities to enjoy their basic rights and freedoms, and about the extent to which their personal information is accessible to government entities and other organizations. It is critical that steps are taken to address this issue and to ensure that immigrants and undocumented communities have the privacy protections they deserve.

The Privacy Act of 1974[13] only applies to federal agencies and not to private companies. The Electronic Communications Privacy Act of 1986[14] provides some protection for electronic communications but it is outdated and in need of revision. The Fourth Amendment of the US Constitution[15] protects against unreasonable searches and seizures, but the extent of this protection can vary depending on an individual's immigration status.

Laws and regulations addressing the privacy harm experienced by immigrant communities should provide comprehensive privacy protections, regardless of immigration status, and ensure that these communities have access to legal remedies in the event of violations. Additionally, these laws should specifically address the use of technology by immigration enforcement agencies, as the use of databases, facial recognition, and other surveillance technologies can exacerbate the privacy harms experienced by immigrants, especially those who are undocumented. Furthermore, laws and regulations should consider the unique privacy challenges faced by these communities, such as the risk of exploitation and discrimination, and provide protections accordingly.

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

a. *Transparency:* Companies should be transparent about their data collection, processing, and sharing practices and provide individuals with clear and accessible information about their data and how it is used. The NTIA should focus on advancing regulations that require private entities to offer individuals straightforward options to reduce, customize, and opt out of data collection and usage 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.
b. *Fairness:* Data collection, processing, and sharing practices should be fair and not perpetuate discrimination or perpetuate existing inequalities. This includes not using data to target immigrant and undocumented communities for discriminatory purposes. The

[13] Privacy Act of 1974, Pub. L. No. 93-579, as codified at 5 U.S.C. 552a

[14] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508
[15] US. Const. Amend. IV

NTIA must promote the enforcement of policies that regularly and continuously examine the effect of algorithms on underserved groups to prevent discriminatory behavior.

c. *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 NTIA should advance regulations that ban the collection and utilization of harmful and pointless data. Consumers should not be forced to sacrifice their privacy, service quality, or other rights by providing unnecessary information just to use a service, especially when such data is not necessary for delivering the promised service.
d. *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-own platforms and contracts with commercial data brokers.
e. *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 NTIA 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.
f. *Respect for Human Rights:* Data collection, processing, and sharing practices should respect human rights, including the right to privacy and due process, and not violate the dignity of immigrant and undocumented individuals.
g. *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.
h. *Non-Discrimination:* Companies should not discriminate against individuals on the basis of immigration status, race, ethnicity, or other protected characteristics, and should not assist in the profiling or targeting of immigrant and undocumented communities. The NTIA should advance regulations to guard against discrimination in the digital space 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 disinformation defense and tech accountability sector, and immigrant rights movement. Member signatories include:

Asian American Arts Alliance

Bend the Arc: Jewish Action

Define American

Envision Freedom Fund

Global Project Against Hate and Extremism

Hispanic Federation

Hispanics in Philanthropy

Human Rights Initiative Of North Texas

Human Rights Watch

Immigrant Law Center of Minnesota

Indivisible

Jolt Action

Kairos

La Mesa Boricua de Florida

Latin America Working Group (LAWG)

Muslim Advocates

National Council of Asian Pacific Americans (NCAPA)

National Hispanic Media Coalition

Project On Government Oversight

UCLA Center on Race and Digital Justice

UndocuBlack Network