United States Senate

WASHINGTON, DC 20510

September 12, 2022

The Honorable Tae D. Johnson
Acting Director
U.S. Immigration and Customs Enforcement
500 12th Street, SW
Washington, DC 20536

Dear Acting Director Johnson:

We urge U.S. Immigration and Customs Enforcement (ICE) to end its use of technologies and surveillance tactics that threaten the privacy rights of individuals all across the United States. According to a recent report, ICE has used facial recognition and other technologies, and purchased information from data brokers, to construct a "dragnet surveillance system" that helps ICE carry out deportation proceedings.[1] Much of this effort, which has enabled ICE to obtain detailed information about the vast majority of people living in the United States, has been shrouded in secrecy. This surveillance network has exploited privacy-protection gaps and has enormous civil rights implications. ICE should immediately shut down its Orwellian data-gathering efforts that indiscriminately collect far too much data on far too many individuals.

Over two years, the Georgetown Law Center on Privacy & Technology conducted an extensive investigation of ICE's contracting and procurement records and concluded that "ICE now operates as a domestic surveillance agency."[2] Among the investigation's key findings:

> ● ICE has used facial recognition technology on the driver's license photographs of almost one-third (32%) of all adults in the United States, and has access to the driver's license data of almost three-fourths (74%) of them — in most cases without obtaining a search warrant.[3]
>
> ● When almost three-fourths (74%) of adults in the United States connected the gas, electricity, phone or internet in a new home, ICE was able to automatically learn their new address.[4]
>
> ● ICE has tapped vast databases held by private data brokers, as well as state and local bureaucracies historically uninvolved with law enforcement, giving ICE access to expansive and frequently updated information streams, including Department of Motor Vehicle (DMV) records, utility customer information, call

[1] *American Dragnet: Data-Driven Deportation In The 21st Century* at 1, Georgetown Law Center on Privacy & Technology (May 10, 2022), https://americandragnet.org/.
[2] *Id.*
[3] *Id.* at 2.
[4] *Id.*

records, child welfare records, credit headers, employment records, geolocation information, health care records, housing records and social media posts.[5]

● Between 2008 and 2021, ICE spent $2.8 billion on new surveillance, data collection and data-sharing initiatives.[6]

Other reports also raise questions about ICE's surveillance activities. According to the *Intercept*, during a seven-month period in 2021, ICE searched the *LexisNexis* database 1.2 million times, accessing such information as an individual's location, work history, and family relationships.[7] Documents obtained by the American Civil Liberties Union reveal that ICE's partnership with one data broker provides the agency access to location data from approximately 250 million mobile devices, with more than 15 billion location points per day.[8] And there are concerning reports that, even when state or federal law requires a warrant to access customer records directly from utility companies or cell phone location data, ICE evades these requirements by paying data brokers for the information it seeks.[9]

However, ICE's surveillance practices remain largely covert. ICE does not, for example, regularly report how many driver's license images it accesses, what images it compares to individuals' driver's license images or their source, or how it uses the results of biometric analysis in immigration proceedings.

As the Georgetown Law Center report concluded, the manner in which ICE leverages information against its targets is especially troubling: "To locate its targets, ICE takes data that people give to state and local agencies and institutions in exchange for essential services. ICE often accesses that data without the permission or even awareness of the entity that originally collected the information."[10] These practices raise serious concerns and questions about how ICE surveils the public and avoids key accountability systems.

In light of the preceding, we request that ICE respond in writing to the following questions by October 3, 2022:

1. How does ICE access driver's license images and data? Please identify the states whose images and data ICE can access and how ICE accesses the images and data, and describe the data that is available

[5] *American Dragnet: Data-Driven Deportation In The 21st Century* at 1, Georgetown Law Center on Privacy & Technology (May 10, 2022), https://americandragnet.org/.
[6] *Id.*
[7] Sam Biddle, *ICE Searched LexisNexis Database Over 1 Million Times In Just Seven Months*, The Intercept (June 9, 2022), https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances/.
[8] Alfred Ng, *Homeland Security records show 'shocking' use of phone data, ACLU says*, Politico (Jul. 18, 2022), https://www.politico.com/news/2022/07/18/dhs-location-data-aclu-00046208.
[9] *Id.*; *American Dragnet: Data-Driven Deportation In The 21st Century*, Georgetown Law Center on Privacy & Technology (May 10, 2022), https://americandragnet.org/.
[10] *Id.*

2. Please identify any instances in which ICE obtained driver's license images or other data on the residents of a state after the state attempted to prevent ICE from obtaining those images or data; how ICE eventually accessed the images or data; and who facilitated that access.
3. When using facial recognition technologies on driver's license image databases, with what images does ICE compare the license images? Please describe how ICE obtains those images.
4. Please describe how ICE uses the results of facial recognition analysis in immigration proceedings.
5. Beyond driver's license image databases, how else does ICE employ facial recognition technologies?
6. Will ICE commit to ending the use of facial recognition technologies on driver's license images databases and otherwise? If not, why not?
7. Please identify any data brokers with whom ICE currently contracts, the terms of those agreements, the types of information ICE accesses through them and the conditions under which this data is accessed, and the number of individuals whose personal information ICE has obtained.
8. Please describe how ICE uses data it obtains from data brokers in immigration investigations and proceedings.
9. Will ICE commit to not purchasing data from data brokers and not otherwise using data that it has not obtained through a search warrant? If not, why not?
10. Please describe how ICE obtains and uses cell phone location data, including how it uses cell phone location tracking data in immigration investigations and proceedings.
11. Will ICE commit to not purchasing cell phone location data from data brokers? If not, why not?
12. Has ICE ever used data it has obtained to assist another federal or state agency or department with a non-immigrant enforcement investigation or proceeding? If yes, please describe how. If not, how would ICE handle this type of request?
13. Please describe how ICE uses data gathered about individuals in Alternatives to Detention (ATD) programs for any reason other than assuring that such individuals do not abscond.

Thank you in advance for your attention to this matter.

Sincerely,

Edward J. Markey
United States Senator

Ron Wyden
United States Senator