

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Katie Hobbs
Governor of Arizona
1700 W. Washington St.
Phoenix, AZ 85007

Dear Governor Hobbs:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Arizona Department of Public Safety provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

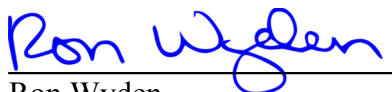
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

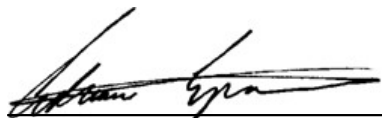
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



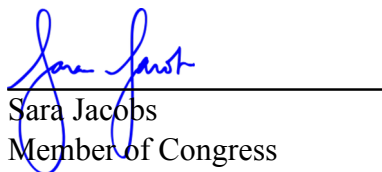
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



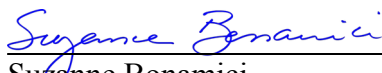
Zoe Lofgren
Member of Congress



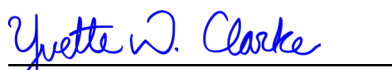
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



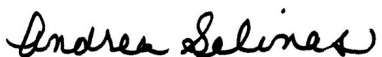
Suzanne Bonamici
Member of Congress



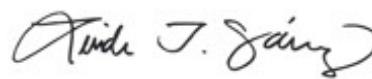
Yvette D. Clarke
Member of Congress



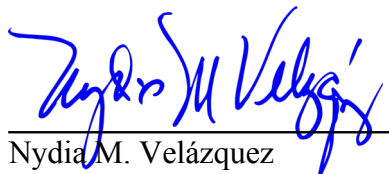
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



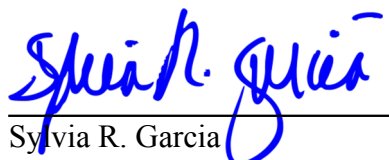
Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



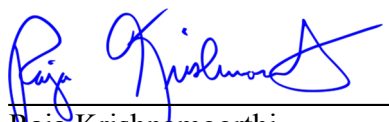
Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



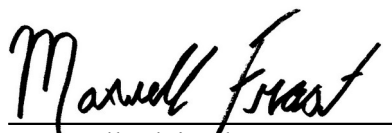
Shri Thanedar
Member of Congress



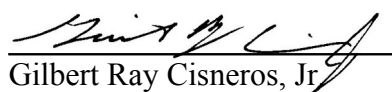
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

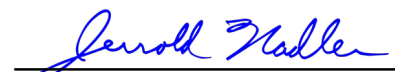

Maxwell Alejandro Frost
Member of Congress


Nanette Diaz Barragán
Member of Congress

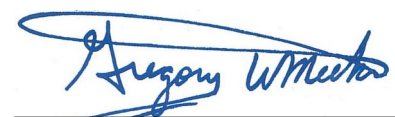

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress


Summer L. Lee
Member of Congress

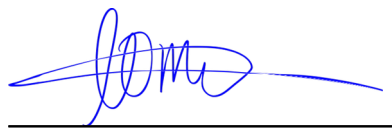

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

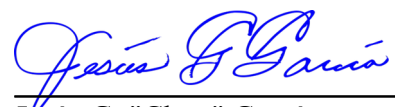

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Gavin Newsom
Governor of California
1021 O Street, Suite 9000
Sacramento, CA 95814

Dear Governor Newsom:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the California Department of Justice provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

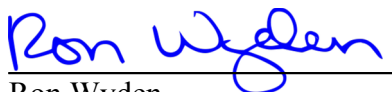
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

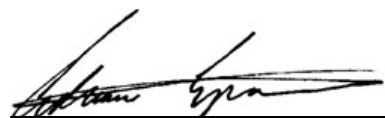
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



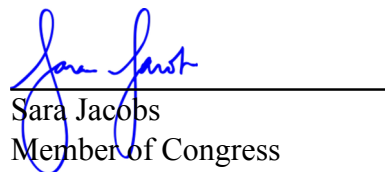
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



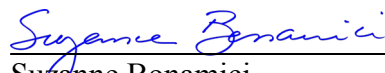
Zoe Lofgren
Member of Congress



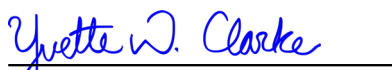
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



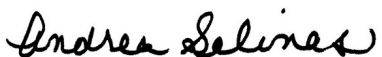
Suzanne Bonamici
Member of Congress



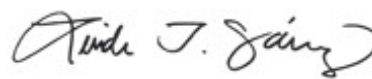
Yvette D. Clarke
Member of Congress



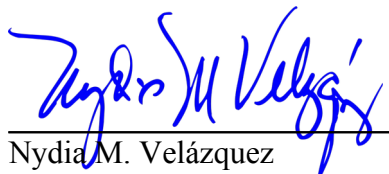
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



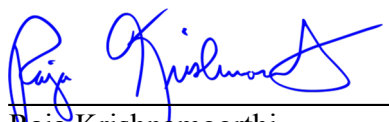
Ted W. Lieu
Member of Congress



Sylvia R. García
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



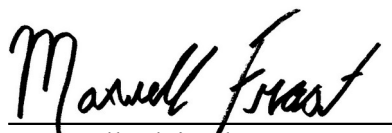
Shri Thanedar
Member of Congress



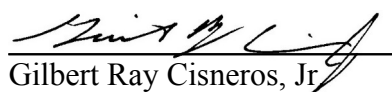
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

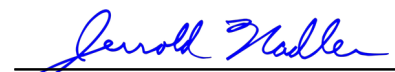

Maxwell Alejandro Frost
Member of Congress


Nanette Diaz Barragán
Member of Congress

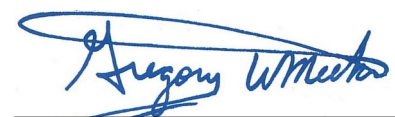

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress


Summer L. Lee
Member of Congress

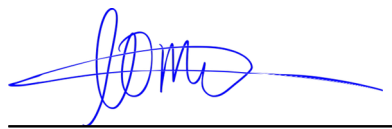

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

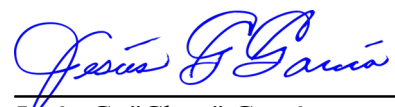

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

CC:

The Honorable Rob Bonta, Attorney General of California

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Jared Polis
Governor of Colorado
200 E. Colfax Ave., Rm. 136
Denver, CO 80203

Dear Governor Polis:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Colorado Bureau of Investigation provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

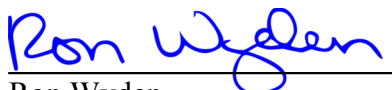
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

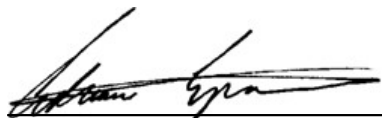
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



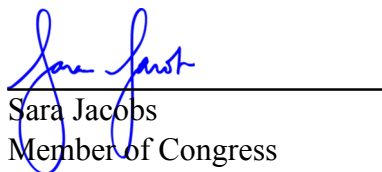
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



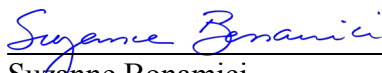
Zoe Lofgren
Member of Congress



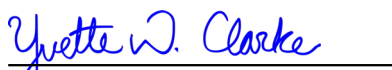
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



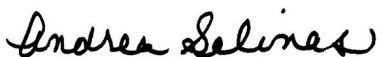
Suzanne Bonamici
Member of Congress



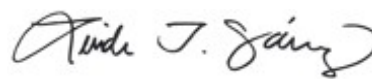
Yvette D. Clarke
Member of Congress



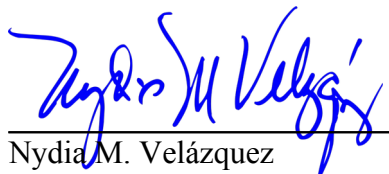
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



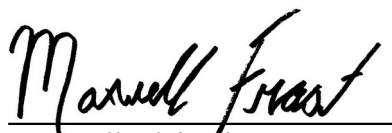
Shri Thanedar
Member of Congress



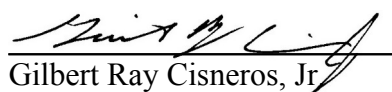
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

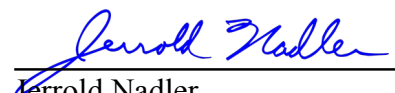

Maxwell Alejandro Frost
Member of Congress

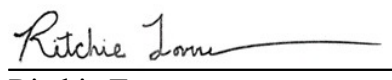

Nanette Diaz Barragán
Member of Congress

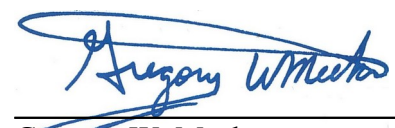

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress

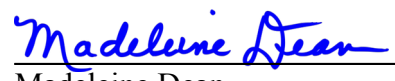

Summer L. Lee
Member of Congress

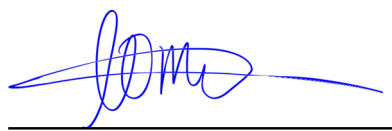

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

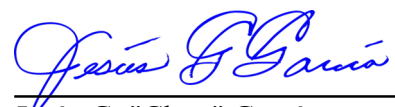

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Ned Lamont
Governor of Connecticut
210 Capitol Avenue
Hartford, CT 06106

Dear Governor Lamont:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Connecticut Department of Emergency Services and Public Protection provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

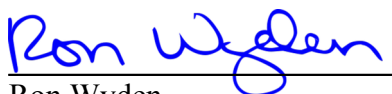
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security,

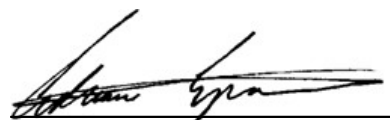
including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



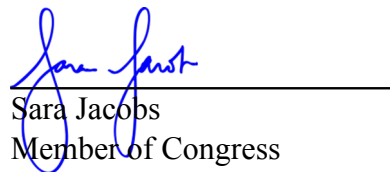
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



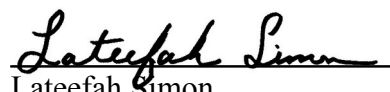
Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



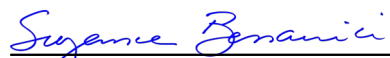
Zoe Lofgren
Member of Congress



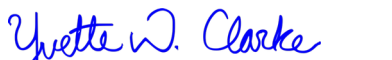
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



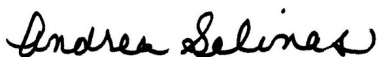
Suzanne Bonamici
Member of Congress



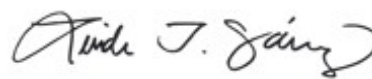
Yvette D. Clarke
Member of Congress



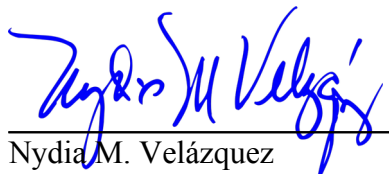
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



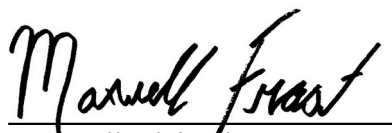
Shri Thanedar
Member of Congress



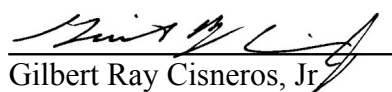
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

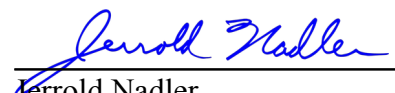

Maxwell Alejandro Frost
Member of Congress

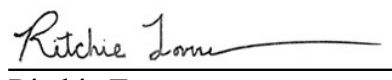

Nanette Diaz Barragán
Member of Congress

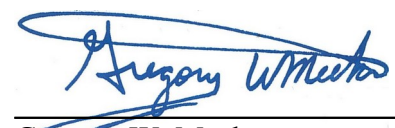

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress

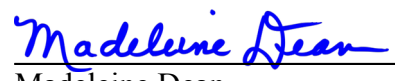

Summer L. Lee
Member of Congress

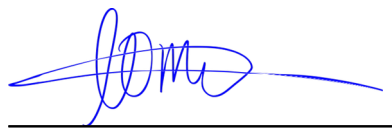

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

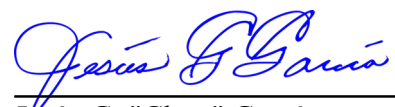

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Matt Meyer
Governor of Delaware
150 Martin Luther King Jr Blvd
South Dover, DE 19901

Dear Governor Meyer:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Delaware State Police provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

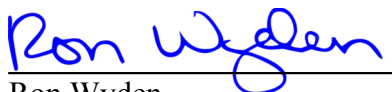
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

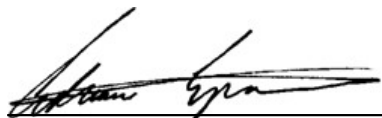
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



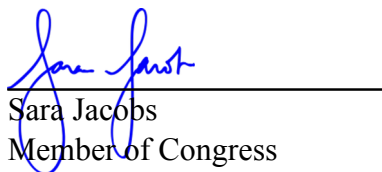
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



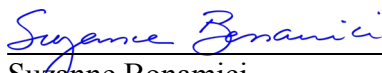
Zoe Lofgren
Member of Congress



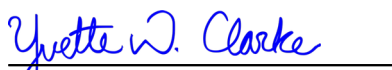
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



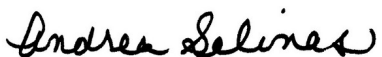
Suzanne Bonamici
Member of Congress



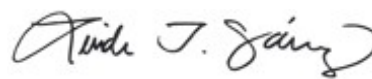
Yvette D. Clarke
Member of Congress



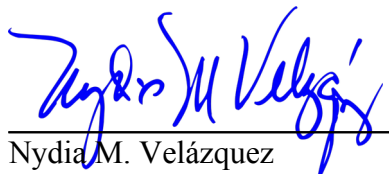
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



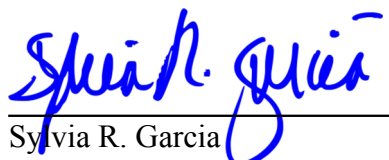
Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



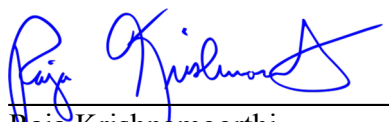
Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



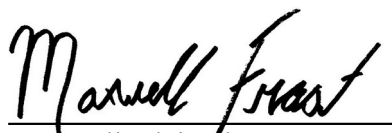
Shri Thanedar
Member of Congress



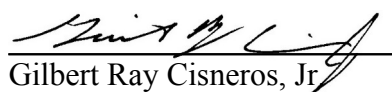
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

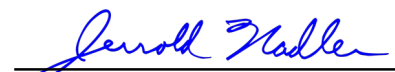

Maxwell Alejandro Frost
Member of Congress


Nanette Diaz Barragán
Member of Congress

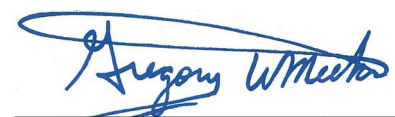

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress


Summer L. Lee
Member of Congress

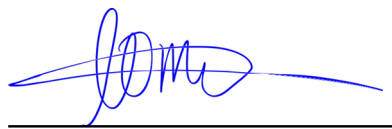

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

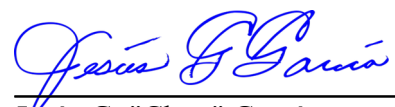

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Josh Green
Governor of Hawai'i
415 South Beretania St.
Honolulu, HI 96813

Dear Governor Green:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Hawaii Criminal Justice Data Center provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

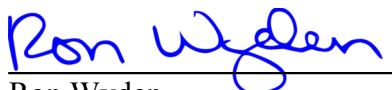
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

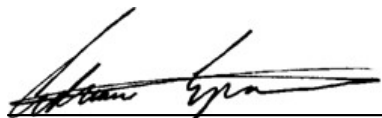
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



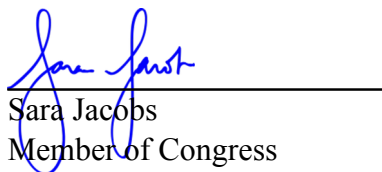
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



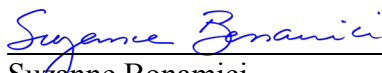
Zoe Lofgren
Member of Congress



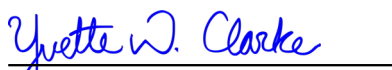
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



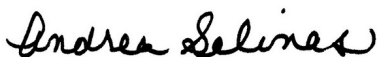
Suzanne Bonamici
Member of Congress



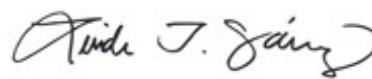
Yvette D. Clarke
Member of Congress



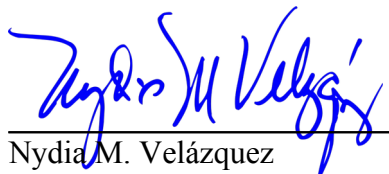
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



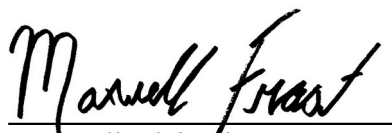
Shri Thanedar
Member of Congress



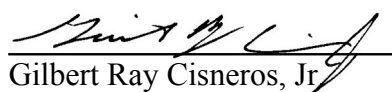
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

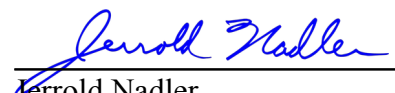

Maxwell Alejandro Frost
Member of Congress

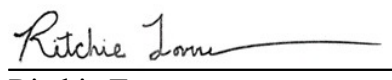

Nanette Diaz Barragán
Member of Congress

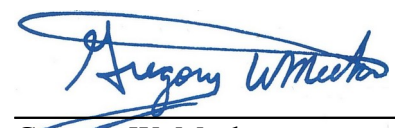

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress

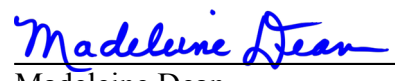

Summer L. Lee
Member of Congress

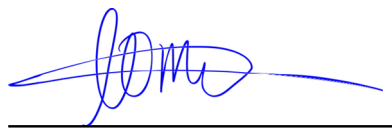

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

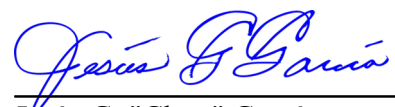

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Laura Kelly
Governor of Kansas
300 SW 10th Ave., Ste. 241S
Topeka, KS 66612-1590

Dear Governor Kelly:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Kansas Bureau of Investigation provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

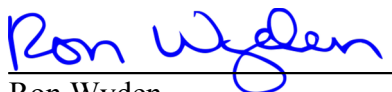
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

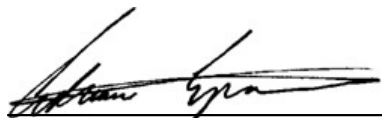
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



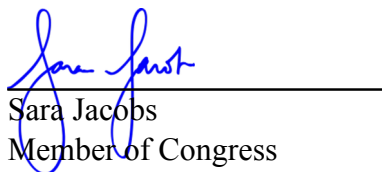
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



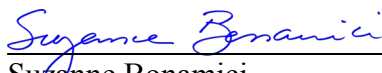
Zoe Lofgren
Member of Congress



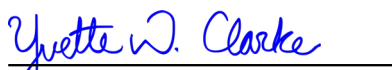
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



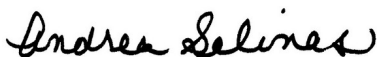
Suzanne Bonamici
Member of Congress



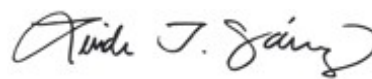
Yvette D. Clarke
Member of Congress



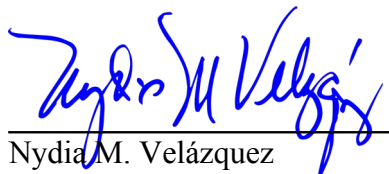
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



Ted W. Lieu
Member of Congress



Sylvia R. García
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



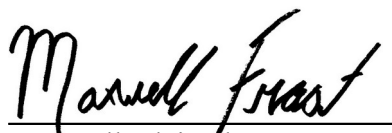
Shri Thanedar
Member of Congress



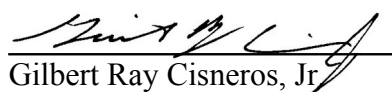
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

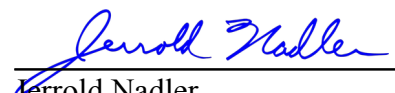

Maxwell Alejandro Frost
Member of Congress

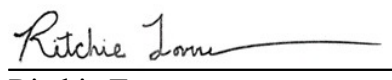

Nanette Diaz Barragán
Member of Congress

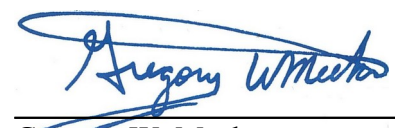

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress

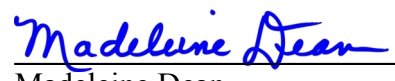

Summer L. Lee
Member of Congress

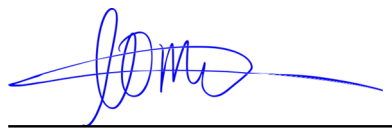

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

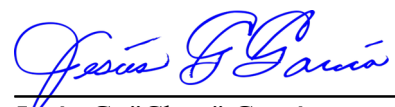

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Andy Beshear
Governor of Kentucky
501 High Street, 2nd Floor
Frankfort, Kentucky 40601

Dear Governor Beshear:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Kentucky State Police provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

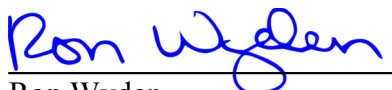
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

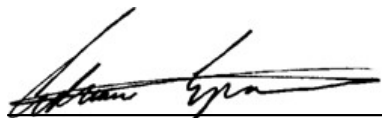
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



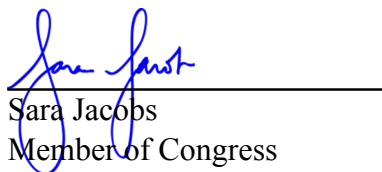
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



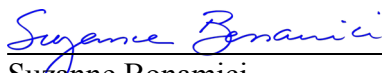
Zoe Lofgren
Member of Congress



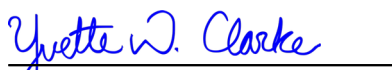
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



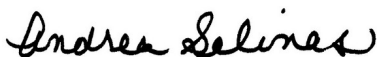
Suzanne Bonamici
Member of Congress



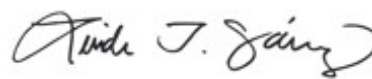
Yvette D. Clarke
Member of Congress



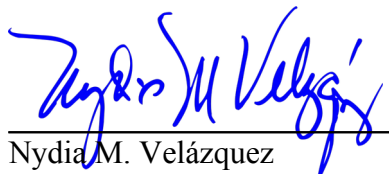
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



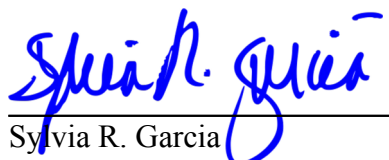
Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



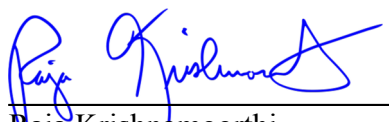
Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



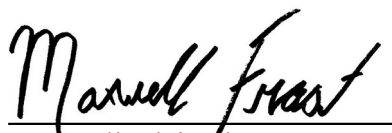
Shri Thanedar
Member of Congress



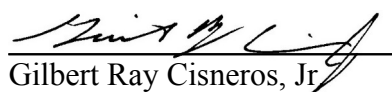
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

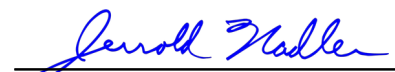

Maxwell Alejandro Frost
Member of Congress


Nanette Diaz Barragán
Member of Congress

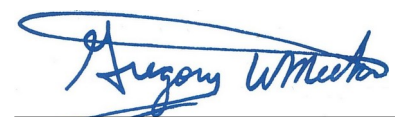

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress


Summer L. Lee
Member of Congress

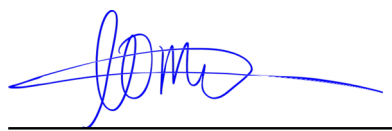

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

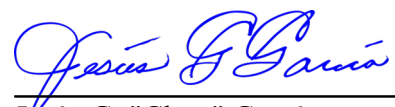

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Janet Mills
Governor of Maine
1 State House Station
Augusta, ME 04333

Dear Governor Mills:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Maine State Police provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

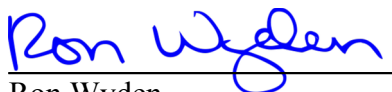
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

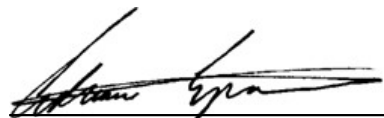
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



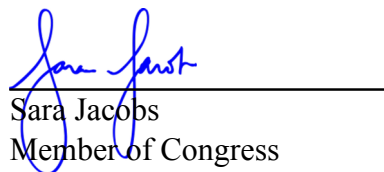
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



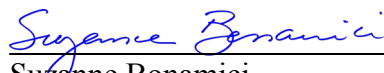
Zoe Lofgren
Member of Congress



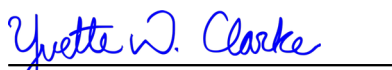
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



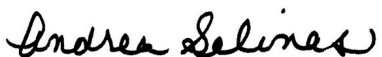
Suzanne Bonamici
Member of Congress



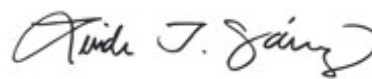
Yvette D. Clarke
Member of Congress



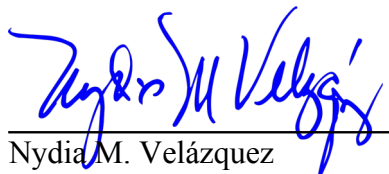
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



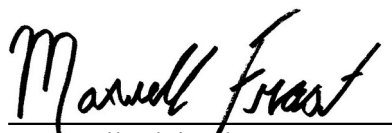
Shri Thanedar
Member of Congress



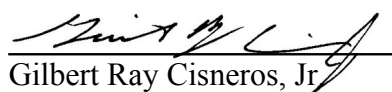
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

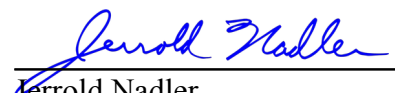

Maxwell Alejandro Frost
Member of Congress

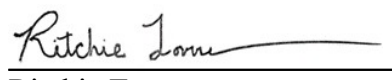

Nanette Diaz Barragán
Member of Congress

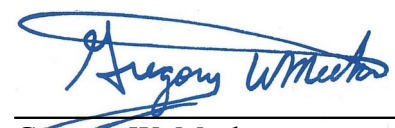

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress

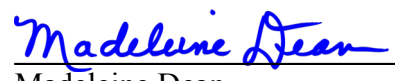

Summer L. Lee
Member of Congress

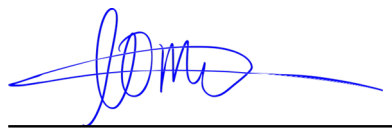

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

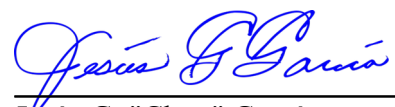

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Wes Moore
Governor of Maryland
100 State Circle
Annapolis, MD 21401

Dear Governor Moore:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Maryland State Police provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

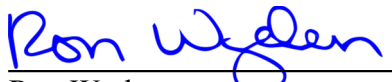
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

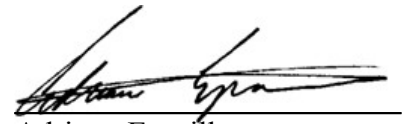
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

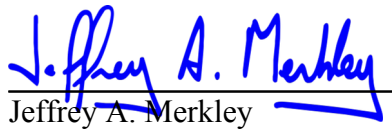
Sincerely,



Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



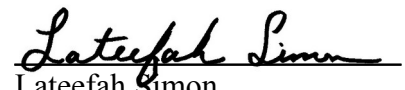
Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



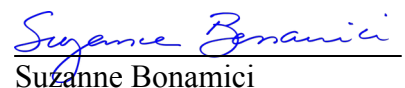
Zoe Lofgren
Member of Congress



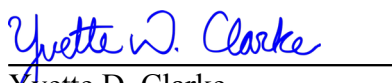
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



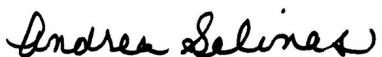
Suzanne Bonamici
Member of Congress



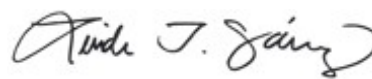
Yvette D. Clarke
Member of Congress



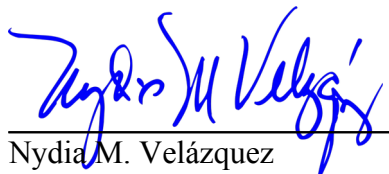
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



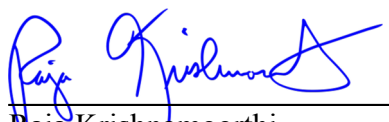
Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



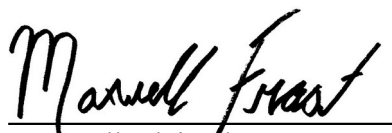
Shri Thanedar
Member of Congress



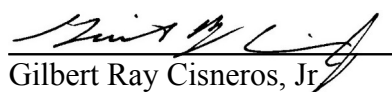
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

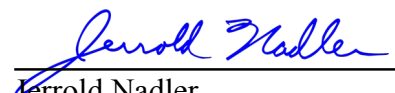

Maxwell Alejandro Frost
Member of Congress

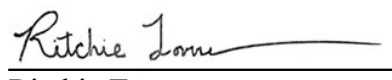

Nanette Diaz Barragán
Member of Congress

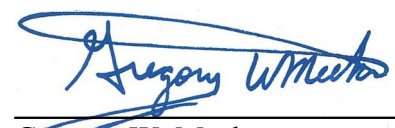

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress

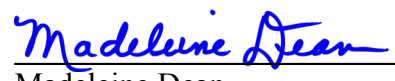

Summer L. Lee
Member of Congress

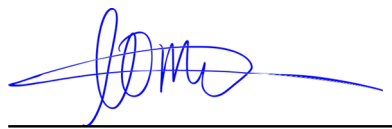

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

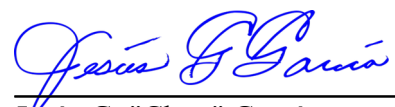

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Phil Murphy
Governor of New Jersey
P.O. Box 001
Trenton, NJ 08625

Dear Governor Murphy:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the New Jersey State Police provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

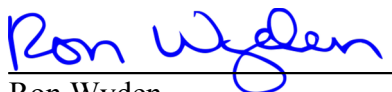
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

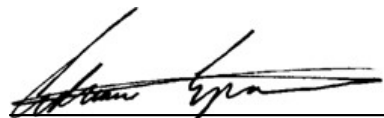
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



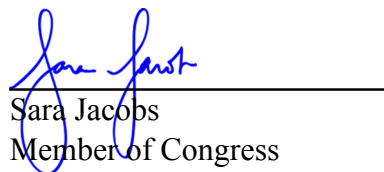
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



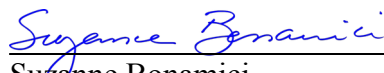
Zoe Lofgren
Member of Congress



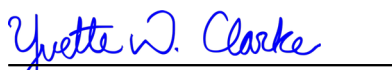
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



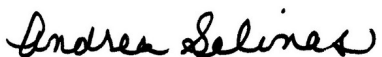
Suzanne Bonamici
Member of Congress



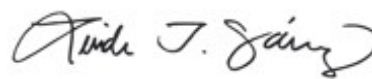
Yvette D. Clarke
Member of Congress



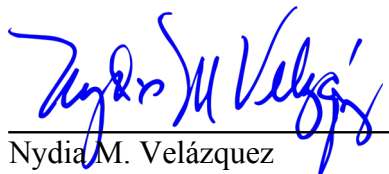
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



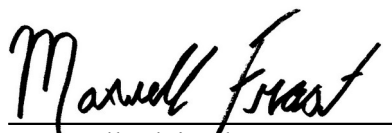
Shri Thanedar
Member of Congress



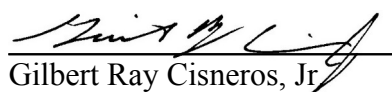
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

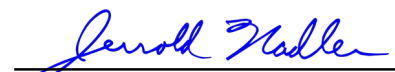

Maxwell Alejandro Frost
Member of Congress


Nanette Diaz Barragán
Member of Congress

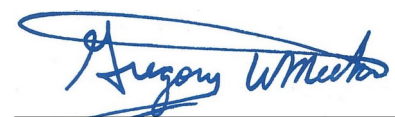

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress


Summer L. Lee
Member of Congress

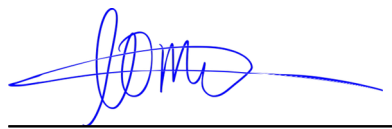

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

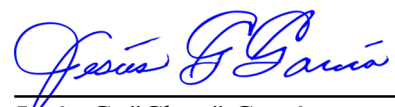

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Michelle Lujan Grisham
Governor of New Mexico
490 Old Santa Fe Trail Room 400
Santa Fe, NM 87501

Dear Governor Grisham:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the New Mexico Department of Public Safety provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

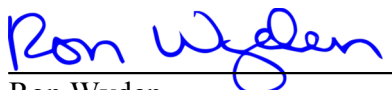
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

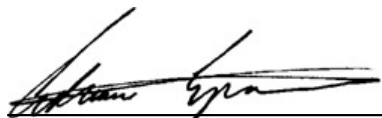
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



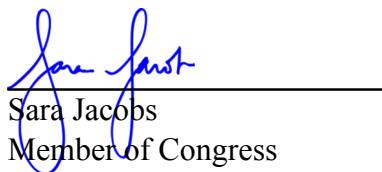
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



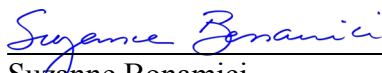
Zoe Lofgren
Member of Congress



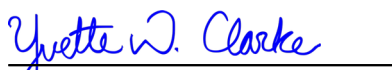
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



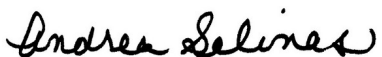
Suzanne Bonamici
Member of Congress



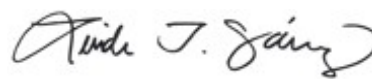
Yvette D. Clarke
Member of Congress



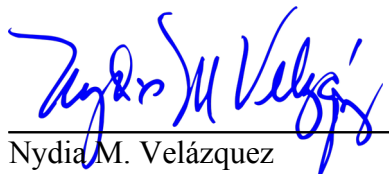
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



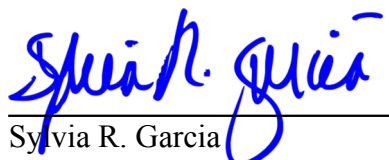
Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



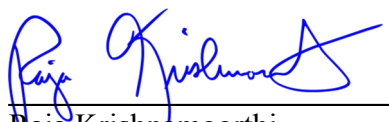
Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



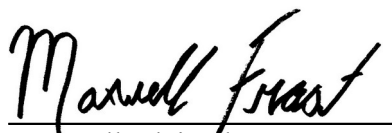
Shri Thanedar
Member of Congress



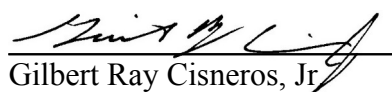
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

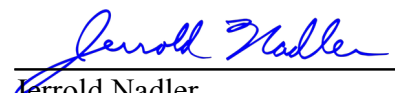

Maxwell Alejandro Frost
Member of Congress

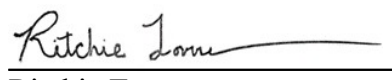

Nanette Diaz Barragán
Member of Congress

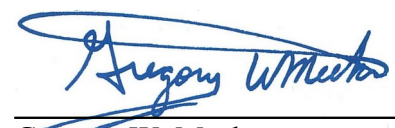

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress

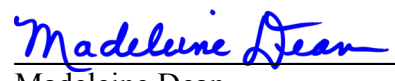

Summer L. Lee
Member of Congress

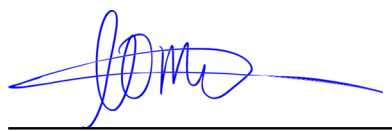

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

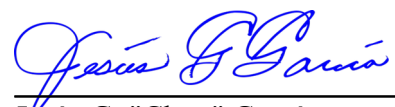

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Josh Stein
Governor of North Carolina
20301 Mail Service Center
Raleigh, NC 27699-0301

Dear Governor Stein:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the North Carolina State Bureau of Investigation provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

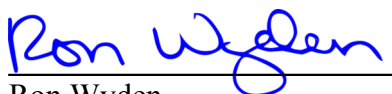
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security,

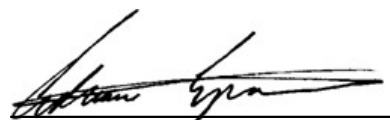
including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



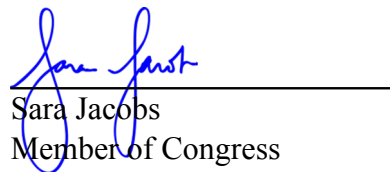
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



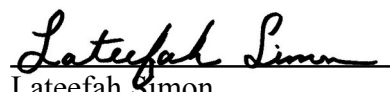
Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



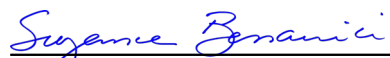
Zoe Lofgren
Member of Congress



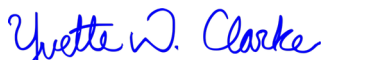
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



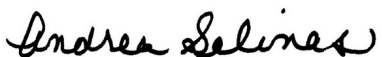
Suzanne Bonamici
Member of Congress



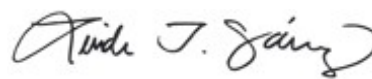
Yvette D. Clarke
Member of Congress



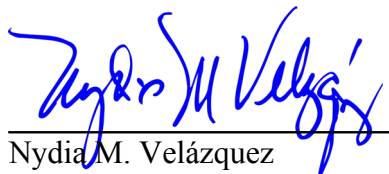
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



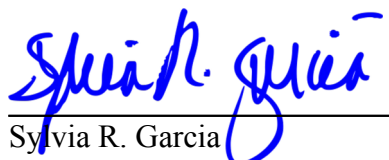
Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



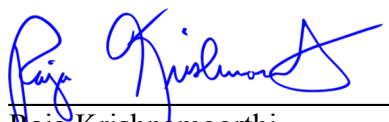
Ted W. Lieu
Member of Congress



Sylvia R. García
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



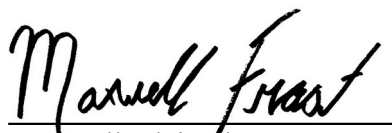
Shri Thanedar
Member of Congress



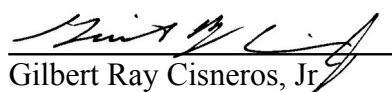
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

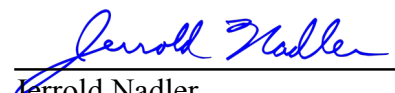

Maxwell Alejandro Frost
Member of Congress

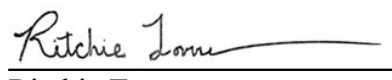

Nanette Diaz Barragán
Member of Congress

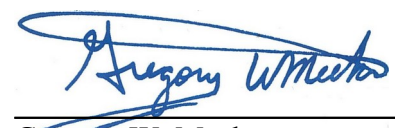

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress

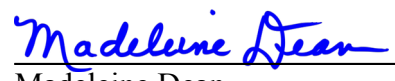

Summer L. Lee
Member of Congress

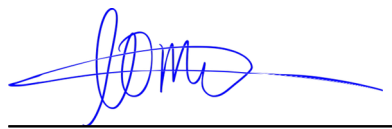

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

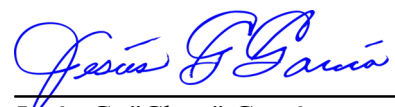

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Gretchen Whitmer
Governor of Michigan
P.O. Box 30013
Lansing, MI 48909

Dear Governor Whitmer:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Michigan State Police provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

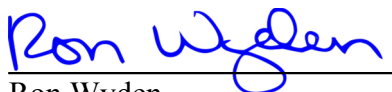
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

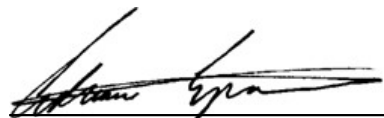
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



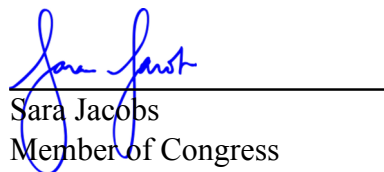
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



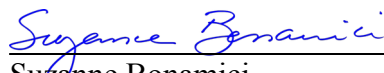
Zoe Lofgren
Member of Congress



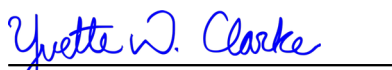
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



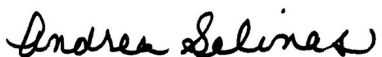
Suzanne Bonamici
Member of Congress



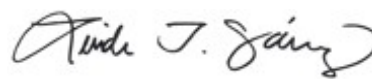
Yvette D. Clarke
Member of Congress



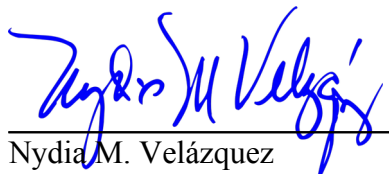
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



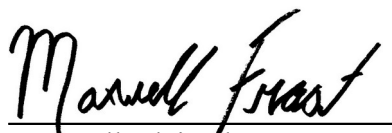
Shri Thanedar
Member of Congress



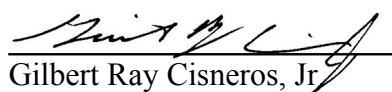
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

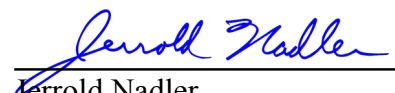

Maxwell Alejandro Frost
Member of Congress

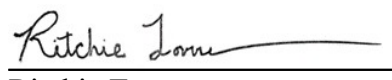

Nanette Diaz Barragán
Member of Congress

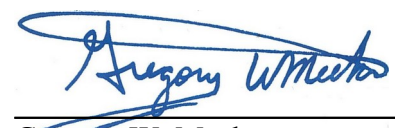

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress

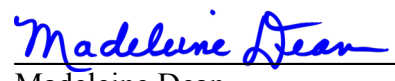

Summer L. Lee
Member of Congress

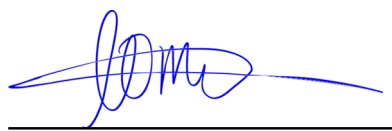

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

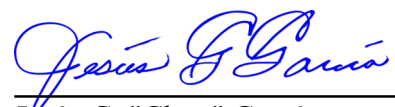

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Josh Shapiro
Governor of Pennsylvania
501 North 3rd Street
508 Main Capitol Building
Harrisburg, PA 17120

Dear Governor Shapiro:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Pennsylvania State Police provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

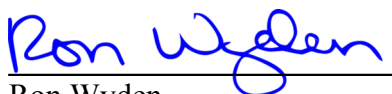
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security,

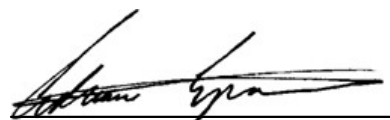
including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



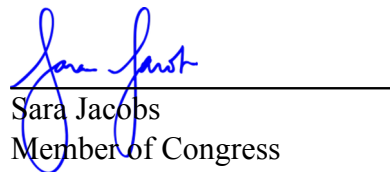
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



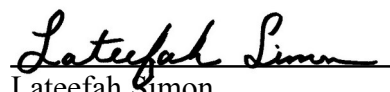
Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



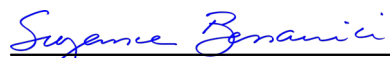
Zoe Lofgren
Member of Congress



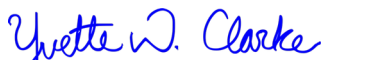
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



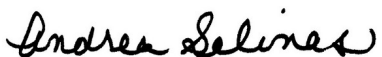
Suzanne Bonamici
Member of Congress



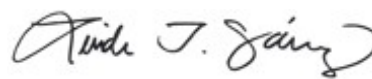
Yvette D. Clarke
Member of Congress



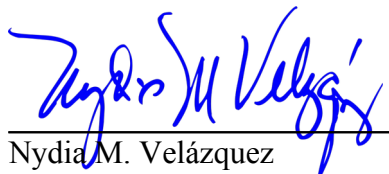
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



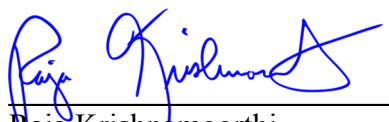
Ted W. Lieu
Member of Congress



Sylvia R. García
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



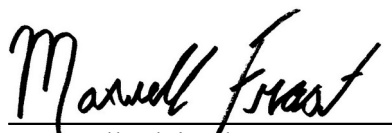
Shri Thanedar
Member of Congress



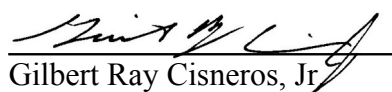
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

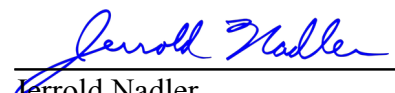

Maxwell Alejandro Frost
Member of Congress

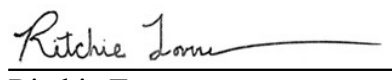

Nanette Diaz Barragán
Member of Congress

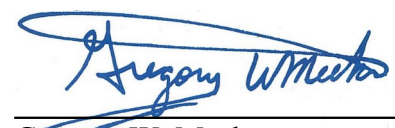

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress

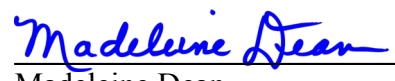

Summer L. Lee
Member of Congress

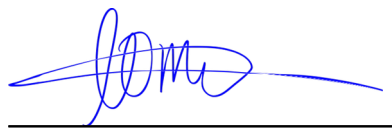

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

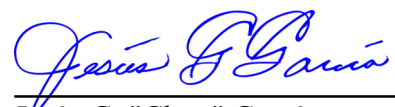

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Dan McKee
Governor of Rhode Island
82 Smith Street
Providence, RI 02903

Dear Governor McKee:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Rhode Island State Police provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

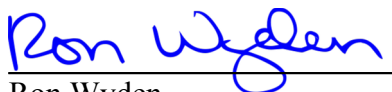
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

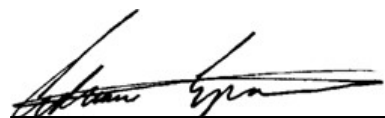
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



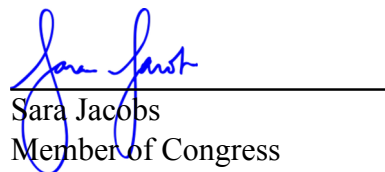
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



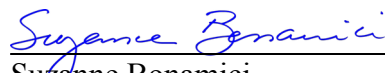
Zoe Lofgren
Member of Congress



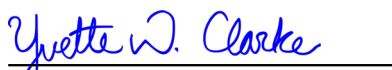
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



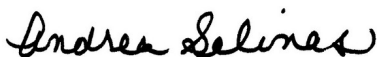
Suzanne Bonamici
Member of Congress



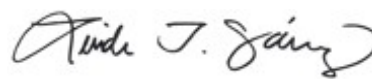
Yvette D. Clarke
Member of Congress



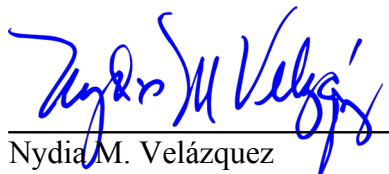
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



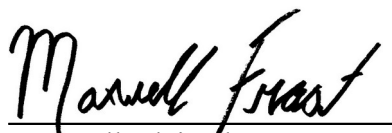
Shri Thanedar
Member of Congress



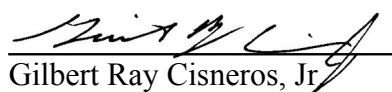
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

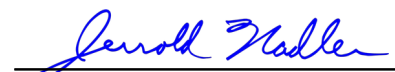

Maxwell Alejandro Frost
Member of Congress


Nanette Diaz Barragán
Member of Congress

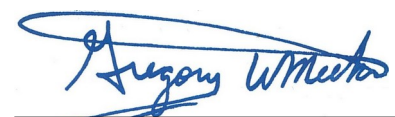

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress


Summer L. Lee
Member of Congress

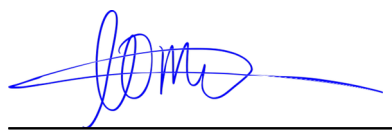

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

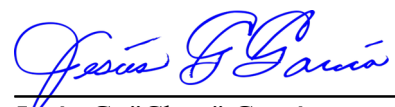

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Tony Evers
Governor of Wisconsin
P.O. Box 7863
Madison, WI 53707

Dear Governor Evers:

We write to alert you to the fact that your state is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using your state's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of your state employees. This is because the Wisconsin Department of Justice provides law enforcement agencies outside your state with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

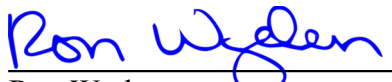
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

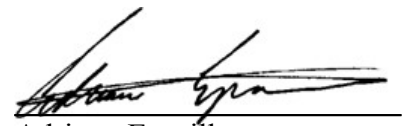
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to your state's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting your state employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

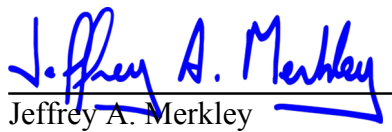
Sincerely,



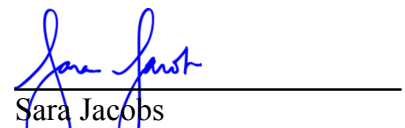
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



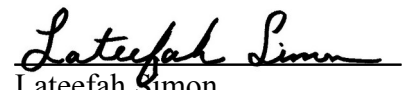
Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



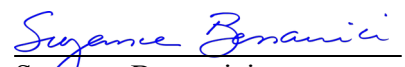
Zoe Lofgren
Member of Congress



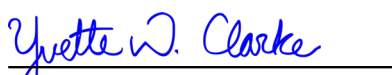
Lateefah Simon
Member of Congress



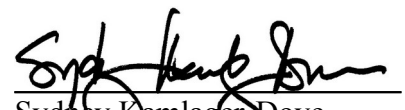
Rashida Tlaib
Member of Congress



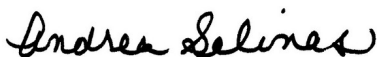
Suzanne Bonamici
Member of Congress



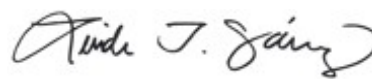
Yvette D. Clarke
Member of Congress



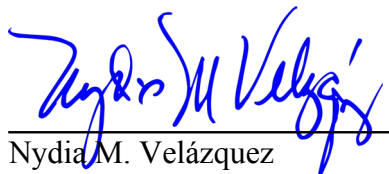
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



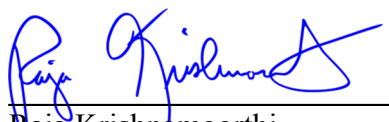
Ted W. Lieu
Member of Congress



Sylvia R. García
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



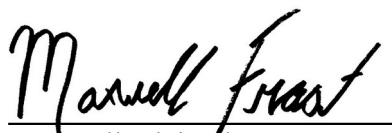
Shri Thanedar
Member of Congress



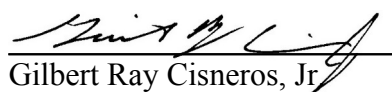
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

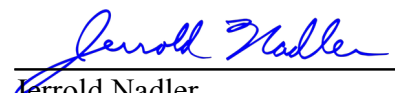

Maxwell Alejandro Frost
Member of Congress

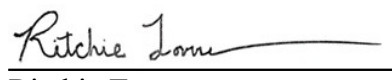

Nanette Diaz Barragán
Member of Congress

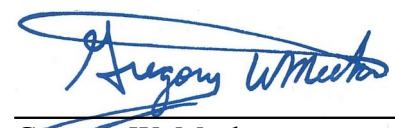

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress

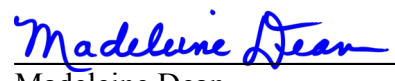

Summer L. Lee
Member of Congress

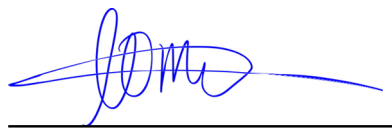

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

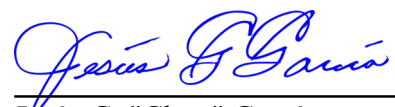

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Albert Bryan Jr.
Governor of the U.S. Virgin Islands
5047 (21-22) Kongens Gade
St. Thomas, VI 00802

Dear Governor Bryan:

We write to alert you to the fact that the US Virgin Islands (USVI) is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using the USVI's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of USVI government employees. This is because the Virgin Islands Police Department provides law enforcement agencies outside the USVI with real time access to your state Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

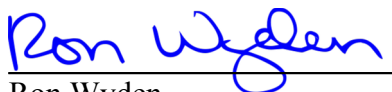
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your state Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing

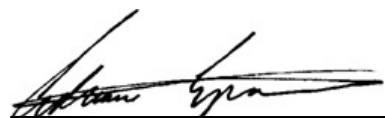
blocks for other federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to the USVI's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting USVI government employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



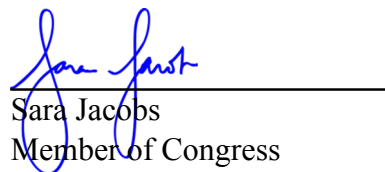
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



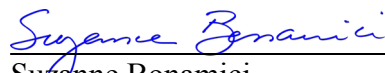
Zoe Lofgren
Member of Congress



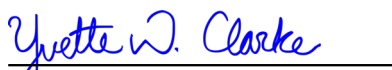
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



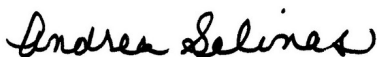
Suzanne Bonamici
Member of Congress



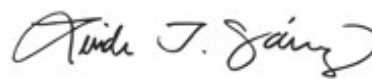
Yvette D. Clarke
Member of Congress



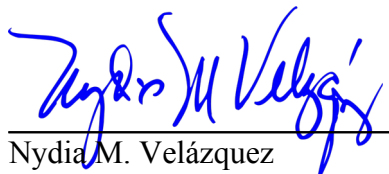
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



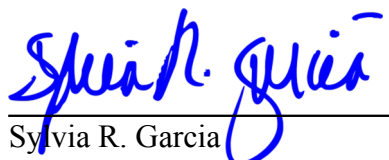
Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



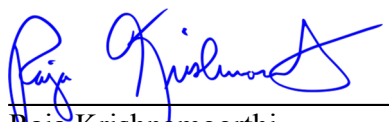
Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



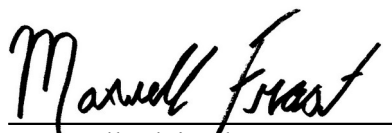
Shri Thanedar
Member of Congress



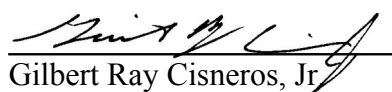
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

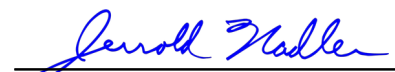

Maxwell Alejandro Frost
Member of Congress


Nanette Diaz Barragán
Member of Congress

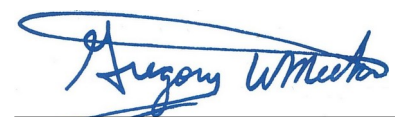

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress


Summer L. Lee
Member of Congress

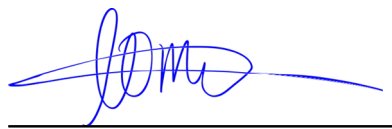

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

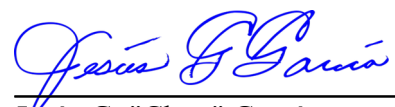

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress

Congress of the United States

Washington, DC 20515

November 12, 2025

The Honorable Lou Leon Guerrero
Governor of Guam
P.O. Box 2950
Agana, GU 96932

Dear Governor Guerrero:

We write to alert you to the fact that Guam is providing Immigration and Customs Enforcement (ICE) and other federal agencies with frictionless, self-service access to the personal data of all of your residents. We urge you to block ICE's access, as Illinois, New York, Massachusetts, Minnesota and Washington have already done and Oregon is in the process of doing, and to consider going further by blocking access to other federal agencies that are now acting as Trump's shock troops. This commonsense step will improve public safety and guard against Trump officials using Guam's data for unjustified, politicized actions, while still allowing continued collaboration on serious crimes.

For more than 20 years, every state and the District of Columbia (DC) have made their residents' data available to approximately 18,000 federal, state, local, tribal and territorial law enforcement agencies across the United States and Canada. These law enforcement agencies have direct access to your residents' data and can search and retrieve that data without the knowledge or assistance of Guam government employees. This is because the Judiciary of Guam provides law enforcement agencies outside Guam with real time access to your Department of Motor Vehicles (DMV) database, which includes drivers licenses and other state-issued ID cards. This data sharing is done through a non-profit organization managed by state police agencies known as Nlets — the International Justice & Public Safety Network ("Nlets").

In the year prior to October 1, 2025, Nlets facilitated over 290 million queries for DMV data, 292,114 of which were from ICE and 605,116 were from Homeland Security Investigations (HSI), according to data Nlets recently provided to Congress. These statistics represent federal and out-of-state requests for data, because law enforcement agencies do not generally access DMV data about residents of their own states through Nlets.

Each state can decide for itself the data it makes available through Nlets, the queries it permits federal and out-of-state law enforcement agencies to make of its data, and the specific agencies that can (or cannot) access its data. According to public data published by Nlets, 20 states and DC allow law enforcement agencies to search drivers' license records using any individual's name and date of birth. In contrast, all 50 states and DC allow agencies to search driver data using a driver's license number. In theory, drivers' license number searches are less likely to be used for dragnet surveillance; however, drivers' license numbers are readily available for purchase from commercial data brokers.

In addition, 41 states share drivers' license photos through Nlets, which can be accessed by federal agencies and analyzed using facial recognition software. According to recent press reports, ICE agents in the field are now using a facial recognition app, called Mobile Fortify, which can instantly identify individuals using over 200 million photos. ICE's Mobile Fortify is reportedly able to access data from Nlets. It remains unclear if ICE is using drivers' license photos for facial recognition.

In early November, Nlets told Congress that it is aware of only four states — Illinois, New York, Massachusetts, Minnesota — that have blocked access to DMV data by ICE. In addition, after engaging with Congressional Democrats, Washington indicated that it too has now blocked ICE's access to DMV data, and Oregon is working on a process for blocking ICE's access to DMV data.

While a number of states have enacted laws, executive orders or policies that are intended to prevent DMV data from being shared with or accessed by immigration authorities, these laws and policies are often ineffective, due to major flaws: First, these policies often only apply to the department of motor vehicles, which does not connect to Nlets, and do not apply to the state police, who act as a conduit for out-of-state and federal agency access to the state DMV database through Nlets. Second, these policies often restrict the activities of state employees, but with respect to Nlets, state employees do not facilitate individual requests for data. Computer systems automatically route Nlets requests and state policies often do not apply to automated computer systems. Third, these policies often restrict data sharing only when data is sought for immigration enforcement. However, because Nlets requests from ICE and other federal agencies do not indicate the purpose of a request, states do not have affirmative knowledge of the purpose, which could then trigger a requirement to block the request. Moreover, even if requesters were required to provide a purpose for a given request, the Trump administration cannot be trusted to tell the truth, and there are no meaningful legal consequences for federal officers who provide a false reason.

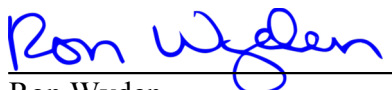
It is now abundantly clear that a major reason that so few states have locked down the data they share through Nlets is because of an information gap. Because of the technical complexity of Nlets' system, few state government officials understand how their state is sharing their residents' data with federal and out-of-state agencies. Critically, it seems apparent that elected officials accountable to voters, including governors, attorneys general, and legislators have not been fully briefed on the current scale of state information sharing with ICE and other federal agencies, nor the availability of technical controls to restrict data sharing with these federal agencies.

To that end, we urge you to promptly request a detailed briefing from your Nlets coordinator; request and make public aggregate statistics on the number of data requests and disclosures to ICE and Homeland Security Investigations (HSI) in 2024 and 2025; and implement technical blocks to prevent data sharing with the Department of Homeland Security, including ICE, HSI and U.S. Border Patrol. We also urge you to seriously consider implementing blocks for other

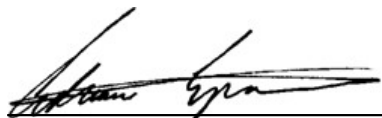
federal agencies whose agents now work on immigration enforcement. To be clear, blocking agencies' unfettered access to Guam's data through Nlets will not prevent federal law enforcement from obtaining information needed to investigate serious crimes, but taking these measures will significantly increase accountability and reduce abuse by permitting Guam government employees to review data requests from blocked agencies first.

Thank you for your attention to this important matter.

Sincerely,



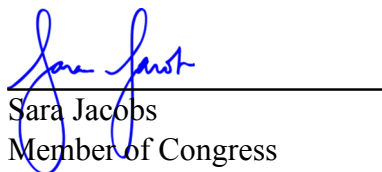
Ron Wyden
United States Senator



Adriano Espaillat
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



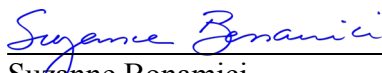
Zoe Lofgren
Member of Congress



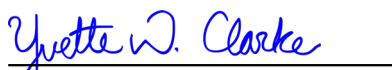
Lateefah Simon
Member of Congress



Rashida Tlaib
Member of Congress



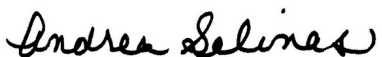
Suzanne Bonamici
Member of Congress



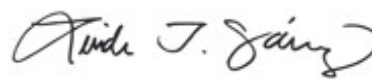
Yvette D. Clarke
Member of Congress



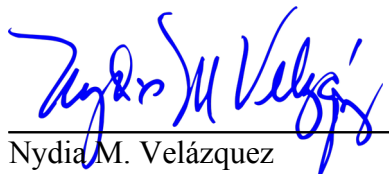
Sydney Kamlager-Dove
Member of Congress



Andrea Salinas
Member of Congress



Linda T. Sánchez
Member of Congress



Nydia M. Velázquez
Member of Congress



Maxine Dexter, M.D.
Member of Congress



Jared Huffman
Member of Congress



Ted W. Lieu
Member of Congress



Sylvia R. Garcia
Member of Congress



Dan Goldman
Member of Congress



Raja Krishnamoorthi
Member of Congress



Eleanor Holmes Norton
Member of Congress



Darren Soto
Member of Congress



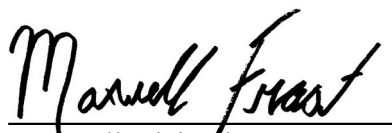
Shri Thanedar
Member of Congress



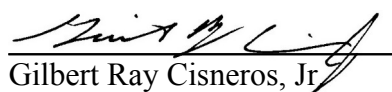
Greg Casar
Member of Congress



Raul Ruiz, M.D.
Member of Congress

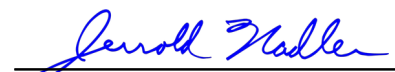

Maxwell Alejandro Frost
Member of Congress


Nanette Diaz Barragán
Member of Congress

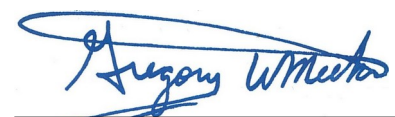

Gilbert Ray Cisneros, Jr.
Member of Congress


James P. McGovern
Member of Congress


Summer L. Lee
Member of Congress

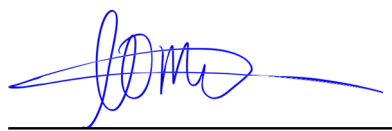

Terrold Nadler
Member of Congress


Ritchie Torres
Member of Congress


Gregory W. Meeks
Member of Congress

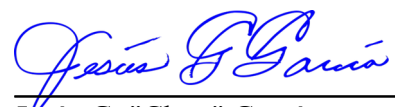

Veronica Escobar
Member of Congress


Madeleine Dean
Member of Congress


Ilhan Omar
Member of Congress


Paul D. Tonko
Member of Congress


Luz M. Rivas
Member of Congress


Jesús G. "Chuy" García
Member of Congress



Mark DeSaulnier
Member of Congress



Pablo José Hernández
Member of Congress