DRIVING PA FORWARD

SECURE OUR DATA

PROTECTING THE PRIVACY OF PENNSYLVANIA RESIDENTS AND DRIVERS

SEPTEMBER 2020

Driver's Licenses for All

DRIVING PA FORWARD

ACKNOWLEDGEMENT

Driving Pennsylvania Forward is a statewide coalition composed of advocacy, faith, businesses, farmers, labor and community organizations that work together in support of the passage of legislation regarding accessibility of a standard driver's license with strict privacy and data protections for all Pennsylvanians regardless of immigration status. The Driving Pennsylvania Forward Coalition prioritizes the leadership of the immigrant community, and welcomes everyone who believes in the importance of changing what is politically possible for the immigrant community through grassroots and legislative efforts.

The **Farmworker Legal Advocacy Clinic** is a law student clinical program at the Villanova University Charles Widger School of Law that advocates for racial and economic justice for Pennsylvania farmworker communities. This report was authored during the 2019-2020 school year by clinic students Lauren Pugh ('20), Grace Waweru ('20), Sam England ('20) and Bernadette Berger ('21) under the supervision of Professor Caitlin Barry. Additional research was provided by Ricky Schneider. We are grateful to Vanessa Stine, Muneeba Talukder and Mana Aliabadi of the ACLU of PA and Julie Mao of Just Futures Law for their invaluable feedback and editorial assistance, and to Harrison Rudolph at the Georgetown Center for Privacy and Security for sharing his expertise.

This report is largely based on documents obtained from the Pennsylvania Department of Transportation and the Office of Administration through Right-to-Know requests submitted by the ACLU of PA and the Farmworker Legal Advocacy Clinic.

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Licenses and identification cards allow Pennsylvanians to move freely, participate in the community, maintain employment, and access crucial services.[1] In recent years, Pennsylvania has taken important steps to expand access to licenses, including lifting restrictions on licenses for people with non-driving convictions[2] and adding a gender-neutral designation that allows non-binary residents to obtain identification.[3] While Pennsylvania currently restricts access to licenses for most noncitizens, 15 states across the country, including New York, New Jersey, Delaware, and Maryland, have provided access to licenses for all residents regardless of their immigration status,[4] and Pennsylvania will hopefully join their ranks soon.

There is no federal law that would prevent Pennsylvania from offering licenses to all residents. In March 2019, Pennsylvania agreed to participate in REAL ID, a federal program that sets certain standards for state-issued identification used for domestic air travel and entry to some federal facilities.[5] REAL ID has extensive requirements regarding immigration status documentation and identity verification that have raised significant privacy concerns among advocates and state officials.[6] Due to these concerns, like many states, Pennsylvania kept its standard-issue license system as the default identification available to state residents.[7] To obtain a REAL ID license or identification card, Pennsylvanians must affirmatively opt-in to REAL ID. Pennsylvania continues to process standard-issue licenses according to state laws and policies, which gives the state significant leeway to determine how and when to issue licenses and state identification cards, as the recent license expansions show.

Driving Pennsylvania Forward ("DPF") advocates for the restoration of standard-issue license eligibility for all Pennsylvania residents, which would enhance safety by ensuring all drivers have been tested and deemed eligible to drive, expand insurance coverage and increase employment by removing transportation barriers for many workers. As DPF began to research the laws and policies of other states, we learned that when driver information is not protected, federal deportation agencies have used driver information to target immigrant drivers.[8] When we reviewed Pennsylvania's current privacy practices, we discovered that Pennsylvania state officials have chosen to sell and share personal information to private companies and hundreds of government agencies, frequently without informing drivers. Pennsylvania has failed to protect the privacy of cardholder information and this failure must be addressed immediately.

An individual should not have to choose between obtaining a license to drive and keeping their information private. But for many noncitizens, this choice has even graver consequences: by getting a license, they risk the possibility that U.S. Immigration and Customs Enforcement ("ICE") will use their information to track them down and deport them; if they drive without one, they risk arrest.[9] Unfortunately, Pennsylvania residents are faced with this exact dilemma. Pennsylvania gives the information of over 36 million license or identification cardholders to hundreds of agencies and private businesses, including ICE, which uses information from state motor vehicle license and registration departments ("DMVs") as one of its main sources for arresting individuals and initiating deportation proceedings.[10]

Currently, to be eligible for a driver's license in Pennsylvania, residents must submit identification documents (such as birth certificates and passports), personal information (including full name, date of birth, address, height, phone number, and eye color) and prove their state residency by providing documents (such as tax returns, utility bills, public benefit statements or medical bills).[11] Noncitizens that fall within certain legal status categories may be eligible for licenses if they can provide proof of their immigration status, along with their identification documents.[12]

All of this information is collected by PennDOT, which stores it indefinitely[13] and creates a massive data source available to outside agencies like ICE. Pennsylvania must take steps to protect driver information, particularly concerning noncitizens. This report will examine the three main avenues through which PennDOT shares driver information: (1) directly from PennDOT, (2) through state databases that have access to PennDOT information, and (3) from private data brokers that sell PennDOT license information to third parties.

2 PENNDOT SHARES AND SELLS DRIVER INFORMATION WITH FEW PROTECTIONS IN PLACE

PennDOT is responsible for operating the driver's license and state identification systems in Pennsylvania. It receives applications for licenses and identification cards and maintains copies of the application information indefinitely. It also stores driver's license information, including driving histories, vehicle information, and more. There are two main groups of information that PennDOT stores:

GROUP 1 — Application Information

- **Proof of identification:** social security card or original immigration documents indicating current lawful immigration status and either a birth certificate, certificate of naturalization, or valid passport
- **Proof of residency:** tax records, lease agreements, mortgage documents, W-2 forms, current weapons permit, or current utility bills, among other records

GROUP 2 — Driver License or Identification Card Information

- Date of birth, address, height, eye color
- Photo
- Social security number
- Driver's history
- Vehicle information related to the licenses

PennDOT keeps all driver information indefinitely in its internal database, and also places the information in Group 2 in state law enforcement databases.[14] As explained below, once that information is placed in the databases, it may be accessed by government agencies and private businesses. Finally, PennDOT also sells driver information to private data brokers, including companies that sell personal data to ICE.

A. DIRECT ACCESS TO PENNDOT INFORMATION

Any government agency, including ICE, can go directly to PennDOT to get information about drivers. PennDOT has a general "Request for Data" form that asks the requester to list what information they are seeking, explain the purpose of the request, describe how the information will be stored and kept secured, agree to not disclose or disseminate the information to other parties, and ensure that the information is kept confidential.[15]

Requestors do not have to provide any evidence in support of their request. There is no language in the form restricting what type of information may be requested. The form also does not limit the requests to criminal investigations, nor does it require the requester to confirm the information is being requested for an official purpose. This form is the only prerequisite for law enforcement to request information directly from PennDOT.

Recommendations for Restricting Direct Access to PennDOT Information

• PennDOT should establish clear privacy protections for all driver information in its possession. Access to those records should be restricted to law enforcement conducting criminal investigations who can produce judicial warrants. PennDOT should immediately enact these standards, staff should be trained accordingly, and routine audits of any requests from outside agencies should be made available to the public that document that volume, nature, and outcome of the requests.

• The Pennsylvania legislature should update the driver licensing laws to include privacy protections for license and identification card information, as the law does not currently contain any such provisions. The recent driver license expansions in New York and New Jersey contain extensive privacy provisions applicable to all licensed drivers and identification cardholders.

B. ACCESS TO DRIVER INFORMATION THROUGH PENNSYLVANIA LAW ENFORCEMENT DATABASES

PennDOT also shares driver information with outside agencies by placing that information in several databases accessed by hundreds of state and federal agencies.

What is the Pennsylvania Justice Network ("JNET")?

The Pennsylvania Justice Network (JNET) is Pennsylvania's primary law enforcement information database.[16] According to its website, JNET "provides a common online environment for authorized users to access public safety and criminal justice information."[17] This information comes from "various contributing municipal, county, state and federal agencies."[18] PennDOT is one of these agencies and JNET has access to PennDOT's driver and identification cardholder information.[19] JNET users can search through PennDOT's photo database, license plate database, list of expired or revoked driver's licenses, current driver's licenses and photo records, certified driving records, and certified vehicle records.[20] If someone has a Pennsylvania driver's license or identification card, then JNET contains, at a minimum, that person's name, photo, address, driving record, and registration information.[21]

Not much is known about who has access to JNET, as the agency does not publish detailed information on which agencies or private businesses can access the database. As of 2018, there were over 26,000 active JNET accounts.[22] Forty-four federal agencies and eight "business" partners have access to JNET, which is granted on an individual basis.[23]

How Does PennDOT Share Its Information with JNET?

PennDOT has been contributing driver and identification cardholder information directly into the JNET database for many years, but the agency did not have any written agreements until 2018. On October 19, 2018, JNET and PennDOT entered into a Memorandum of Understanding ("MOU"), which outlines how the agencies share data and the responsibilities each agency owes one another. The MOU states that PennDOT must consent in writing to new users who can access PennDOT information.[24] According to the MOU, PennDOT provides JNET with vehicle registration information, operator license numbers, drivers' histories, title numbers, and drivers' license photos. PennDOT reviews the requests for access to PennDOT information and determines if granting access to PennDOT data is authorized. JNET also agrees not to enter into any agreements to share PennDOT data with third parties without the written permission of PennDOT. This MOU gives PennDOT the ability to control how its data is shared and who has access to its information. However, before this agreement, PennDOT was not required to review or approve new users, and ICE was granted access to the highest level of JNET access at some point prior to 2018.

Why Is It Difficult to Find Out How JNET Uses and Stores Information?

JNET's website provides only some basic information about the database: it lists the various JNET applications and the sources of available data (including PennDOT), and states that law enforcement and public safety officials use JNET. The website states that "[t]ypical users include municipal and state police, probation, corrections, courts, Office of the Attorney General, 911 and booking centers, district attorneys, children and youth and domestic relations."[25] However, JNET does not provide information on which specific government agencies nor does it mention that private businesses have access to JNET. It also does not provide any information about privacy protections JNET has in place to protect information in its database from inappropriate use.

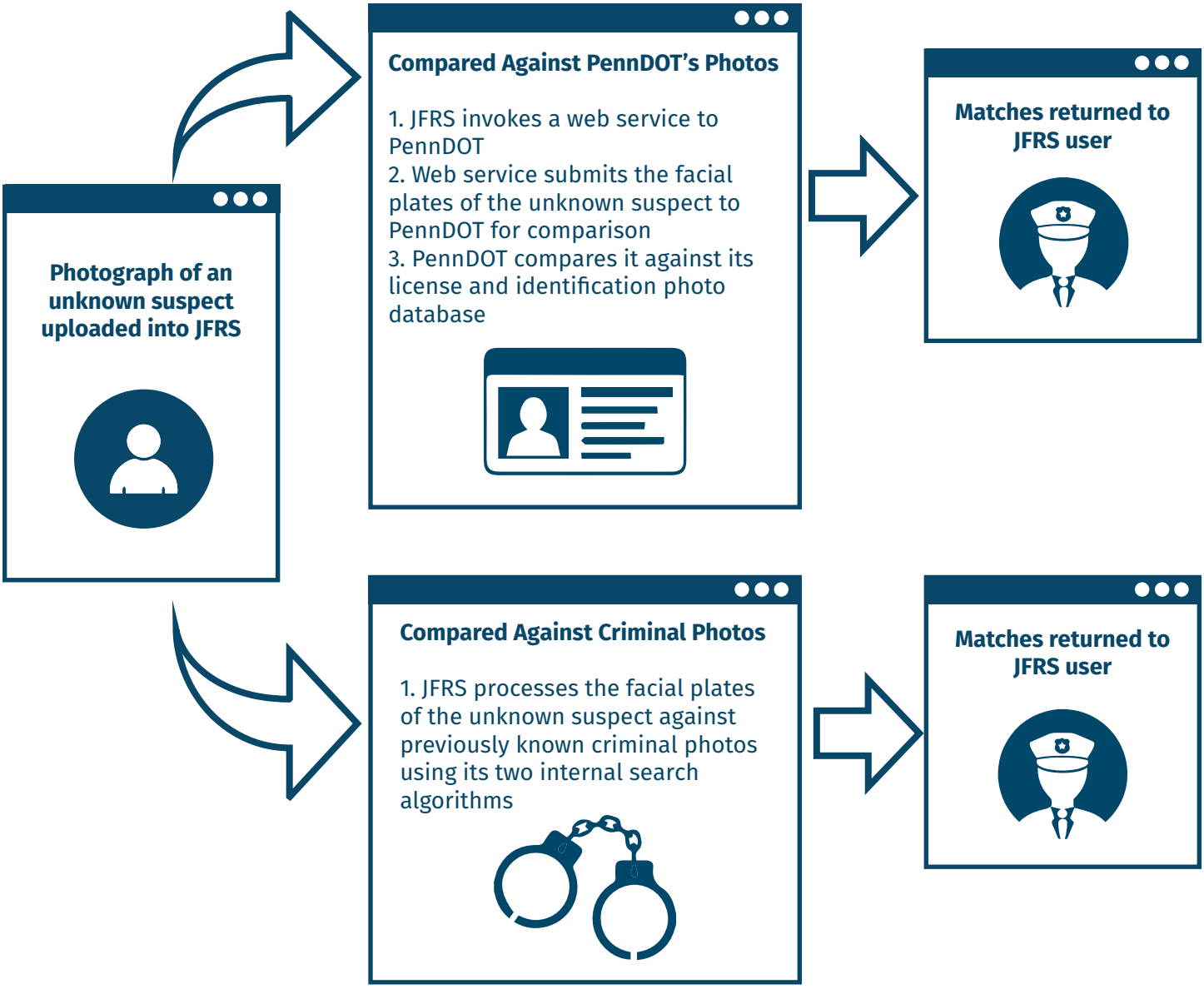
Multiple privacy advocates have filed Right-to-Know requests with the Pennsylvania Governor's Office of Administration ("OA"), the office where JNET is located, seeking the release of the list of JNET users and information on how the database is administered. The OA has resisted disclosing this information.[26] There is still no public access to the list of JNET users or the standards by which JNET grants access for individual searches.

Did You Know Certain JNET Users Can Run Facial Recognition Searches with Over 36 Million PennDOT Photos?

The JNET Facial Recognition System ("JFRS") is one JNET application that is particularly alarming because of its privacy implications. This application allows users to do more than just see photos. It allows users to compare an image, such as surveillance photos or pictures from social media sites, against PennDOT's database of over 36 million photographs.[27]

Originally, an image uploaded to JFRS could only be compared against the 3.5 million criminal booking photographs that JNET possessed. In 2013, PennDOT agreed to share the 36 million photos in its database with JNET, and the two agencies developed a set of web services to integrate the systems.

To use JFRS, a user simply uploads a photo. The photo is then compared against both the statewide criminal database and PennDOT's driver's license database. JFRS compares the photo against the arrest database and sends the photo to PennDOT so PennDOT can compare it against its license and identification photo database. PennDOT returns potential matches to JFRS.[28] Users can access JFRS on their mobile devices to upload images in real-time for instant comparison.[29]



JFRS users sign an agreement that states that they will abide by the restrictions set out in the JNET training materials to use the application. Despite multiple requests, those training materials have never been available to the public. In response to a Right-to-Know request filed in 2020, the OA stated that the following criteria must be met to run a search in JFRS:

- A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning a criminal activity that presents a threat to any individual, group or community
- There is an active or ongoing criminal investigation
- To assist in the identification of a person who lacks capacity or is otherwise unable to identify themselves, such as incapacitated, deceased or at-risk individual
- To assist in the identification of potential witnesses or victims of a crime[30]

These standards are not included in the JFRS user agreement, and it is not clear how they are communicated to users, how individual searches are evaluated to ensure that they meet these criteria or what the consequences are for violation of the policy.

Did You Know ICE Can Use the JNET Facial Recognition System?

Individual ICE officers and U.S. Citizenship and Immigration Services ("USCIS") personnel have access to JNET.[31] It is not clear when, how or why ICE was granted access to JFRS, as the OA states that no contracts or agreements exist with ICE.[32] But it is important to note that immigration investigations are civil, not criminal and ICE investigations should not meet the OA's purported criteria to run a search in JFRS.

With access to JFRS, an ICE officer could run a facial recognition search through PennDOT's photo database of 36 million photos and target individuals with the information they obtain from JFRS. Considering ICE's access to JFRS, if licenses are expanded to those without legal status, undocumented individuals face the significant risk of ICE officers using and abusing this facial recognition technology for immigration enforcement purposes.

Which Other Law Enforcement Databases Contain PennDOT Information?

Logging into JNET is not the only way ICE officers can access PennDOT information. ICE officers also have access to the Commonwealth Law Enforcement Assistance Network ("CLEAN"). CLEAN is a statewide computerized information system administered by the Pennsylvania State Police.[33] CLEAN users can access certain PennDOT information through searches that provide a driver's license number, validation date, name, address, expiration date, social security number, date of birth, sex, eye, height, restrictions, suspensions, and operator class.[34] CLEAN is also Pennsylvania's conduit to the National Law Enforcement Telecommunications System ("Nlets"). Nlets is a private non-profit interstate public safety database that was created by the fifty states' law enforcement agencies.[35] Its Driver History Query contains information such as a driver's name, address, date of birth, social security number, license status, license number, and photo.[36] It is not clear when or how ICE was granted access to CLEAN.

Driving is an essential and basic need for most of us in order to access employment, healthcare, childcare, food, and education. In light of its key role in connecting us to basic necessities, we must also protect our personal information from disclosure in the application process. DMV should not be able to share our information without our knowledge, notice, input, or consent. DMV's disclosure of such personal information has clear and potentially devastating consequences for us -- particularly immigrant families.

We already protect such personal information in schools. For example, we protect personally identifiable school information from disclosure under federal law. This protection enables all children and families to access school without fear and upholds the critical right of a child to receive an education. We need to permit immigrants to secure a driver's license without fear that their information will be shared with ICE. Pennsylvania needs to follow the path of other states who have ensured the confidentiality of this information.

--Maura McInerney, Legal Director, Education Law Center

Summary of Databases ICE Can Access with PennDOT Information

	JNET	CLEAN	Nlets
What is It?	Pennsylvania's primary information database located within the Governor's Office of Administration	Statewide computerized information system administered by the Pennsylvania State Police	Statewide computerized information system administered by the Pennsylvania State Police
What Type of PennDOT Information can ICE Officers Access?	PennDOT's driver's photos, driving history records, vehicle registration information, vehicle inspection information, and JNET's Facial Recognition System which compares an unknown suspect's photo against PennDOT's database of over 36 million photos	Driver's license number, validation date, name, address, expiration date, social security number, date of birth, sex, eye, height, restrictions, suspensions, and operator class	Driver's name, address, date of birth, social security number, license status, license number, and photo

Recommendations for Protecting Information in Pennsylvania Databases

• PennDOT should immediately instruct JNET and CLEAN to rescind ICE's access to PennDOT information in those databases.

• PennDOT should require any outside law enforcement agency to provide a judicial warrant before accessing PennDOT information in the future.

• Regular audits should be conducted to ensure that no other JNET or CLEAN users are providing driver information to ICE or other outside agencies and those audits should be available to the public.

• Both agencies should inform drivers of how their information is being used by publishing regular reports available to the public specifying which agencies and private businesses have access to their databases, and the standards by which users can search driver information.

• Given the heightened privacy concerns with facial recognition technology, PennDOT should institute a moratorium on facial recognition searches.

• The Pennsylvania legislature should enact laws that protect how PennDOT information is shared within these databases. By limiting the sharing of driver data to criminal investigations supported by a judicial warrant, a privacy provision in the driver licensing laws could ensure that driver information in law enforcement databases would not be shared with immigration agencies or other inappropriate users.

C. PRIVATE SALE OF DRIVER'S LICENSE INFORMATION

Did You Know PennDOT Sells Driver's License Information to Private Companies?

In addition to direct access to state databases, ICE can learn a lot about a person by purchasing data from private companies. These private companies, known as data brokers, collect information from a variety of sources, such as credit agencies and utility records and compile it to form individual profiles. The most common data brokers include LexisNexis, Thomson Reuters, Transunion, and Acxiom.[37] Multiple reports have confirmed that at least LexisNexis and Thomson Reuters sell data to ICE for use in immigration enforcement.[38]

According to a 2016 audit, PennDOT sells information to LexisNexis.[39] The audit indicates that LexisNexis failed to follow certain safety protocols to safeguard PennDOT information. Specifically, LexisNexis disclosed PennDOT driver information to a third party without obtaining PennDOT's consent and LexisNexis had inadequate customer safeguards to ensure the security of PennDOT information.[40]

One private company, CLEAR, which is owned by Thomson Reuters, collects information from credit agencies, cell phone registries, social media posts, property records, and utility records, among others, to create comprehensive profiles about each United States resident.[41] Multiple news outlets have reported that ICE uses CLEAR for deportation purposes.[42]

PennDOT makes millions of dollars each year selling driver's names, date of births, addresses, and driving records to private entities and data brokers.[43] While it is not clear whether PennDOT information is sold to ICE by data brokers, there do not appear to be any current protections in place to prevent them from doing so.

Recommendations for Restricting Private Data Sales

• PennDOT's contract with private data brokers should expressly prohibit sales to third parties, including ICE, of any PennDOT information.

• PennDOT should publish reports on its sales to private companies, including the terms of the sales and restrictions on further sales to third parties. It should ensure, which it failed to do with LexisNexis, that the information it sells is safeguarded and only accessible to those users who obtain PennDOT's consent. Any contract with a data broker should require the broker to certify that they will not release information to immigration agencies or other third parties conducting civil investigations.

I have been living in Pittsburgh for about 13 years. I am a single mother of 2 children. A driver's license is important to me since as a single mother I am afraid that the police will stop me and deport me, and then my children would be left completely alone. That is the greatest fear and fear for my 12-year-old son.

Having a driver's license would mean that the state of Pennsylvania recognizes us as human beings. Not having access to a driver's license or identification has always been a barrier to communities of color and low-income communities, when we try to obtain a better life, work, access to health insurance or a good home.

As workers we have been called essential for the country, for the economy, but the treatment we receive does not feel that of someone who is called essential. We are asking legislators to recognize us as human beings and to also remove one of the many obstacles that communities of color and low-income encounter every day of our lives.

--Olga, Member of Casa San Jose

3 PENNSYLVANIA CAN AND SHOULD PROTECT DRIVER INFORMATION

Pennsylvania has a long history of protecting the privacy of driver information. In 2007, Pennsylvania's legislature debated whether to comply with the requirements of the Real ID Act, which required states to alter their driver's license policies to fit new federal requirements. Many states, including Pennsylvania, were opposed to the new law and viewed it as "neither the business nor the responsibility of the [federal] government" to create and mandate a law that intruded upon states' management of their own DMV databases.[44] When the law was passed nonetheless and states were required to comply or face penalties, members of Pennsylvania's House of Representatives argued strongly for delayed implementation of the law until changes were made that preserved essential civil rights and liberties of citizens.[45] They argued that the new law exposed individuals to more risk of identity theft and invasion of privacy since state DMV databases would be accessible to law enforcement officers nationwide and to DMV databases of other states.[46] They also argued that the creation of these nationwide databases would likely contain "numerous errors and false information, creating significant hardship" for state citizens as they "perform numerous functions necessary to live in the United States."[47]

Now that Pennsylvania has opted into the REAL ID program, these privacy concerns are no less relevant for standard-issue licenses. No federal law requires states to share driver information with federal immigration agencies. This is why it no surprise that a growing number of states across the country already have such privacy protections in place for their residents.[48] Currently, fifteen states plus the District of Columbia and Puerto Rico have enacted laws making driver's licenses available to eligible residents regardless of their immigration status.[49] Of these states, many including New Jersey, Washington, New York and California have barred or limited ICE's access to the state's DMV databases.[50] Driver's licenses are a traditional concern of the States and state power over these concerns should be exercised without federal interference.[51]

On a broader level, the Pennsylvania constitution protects residents' right to privacy, including informational privacy. In 2016, the state Supreme Court held that the "right to informational privacy is guaranteed by Article 1, Section 1 of the Pennsylvania Constitution, and may not be violated unless outweighed by a public interest favoring disclosure."[52] The Court went on to say that "[p]ublic agencies are not clearinghouses of 'bulk' personal information otherwise protected by constitutional privacy rights. . . . [T]he constitutional rights of the citizens of this Commonwealth to be left alone remains a significant countervailing force."[53] When a public agency chooses to share personal information, it should do so only when the public interest in the disclosure justifies the violation of privacy. Driver information should similarly be viewed as protected by the constitutional right to privacy and should not be disclosed to outside agencies or private businesses.

Of particular concern given the heightened privacy and racial bias implications is the use of PennDOT photos for facial recognition searches. This technology has rapidly expanded in use in recent years despite extensive research showing that the technology is highly flawed. Some technology companies capable of developing facial recognition systems have refrained from doing so due to its potential abuse.[54] The Fourth Amendment protects an individual's right to be free from unreasonable searches, but because facial recognition technology is so new, no court has yet to weigh in on whether the Fourth Amendment would prevent facial recognition searches of unsuspecting drivers. With regard to other kinds of searches, the Supreme Court assesses most Fourth Amendment questions by asking whether the individual has a personal expectation of privacy and whether the expectation of privacy is one that society deems reasonable.[55] When a driver license photo is subjected to a facial recognition search without the driver's knowledge or consent and used to obtain personal information that PennDOT possesses, there are strong arguments that those searches violate driver privacy.

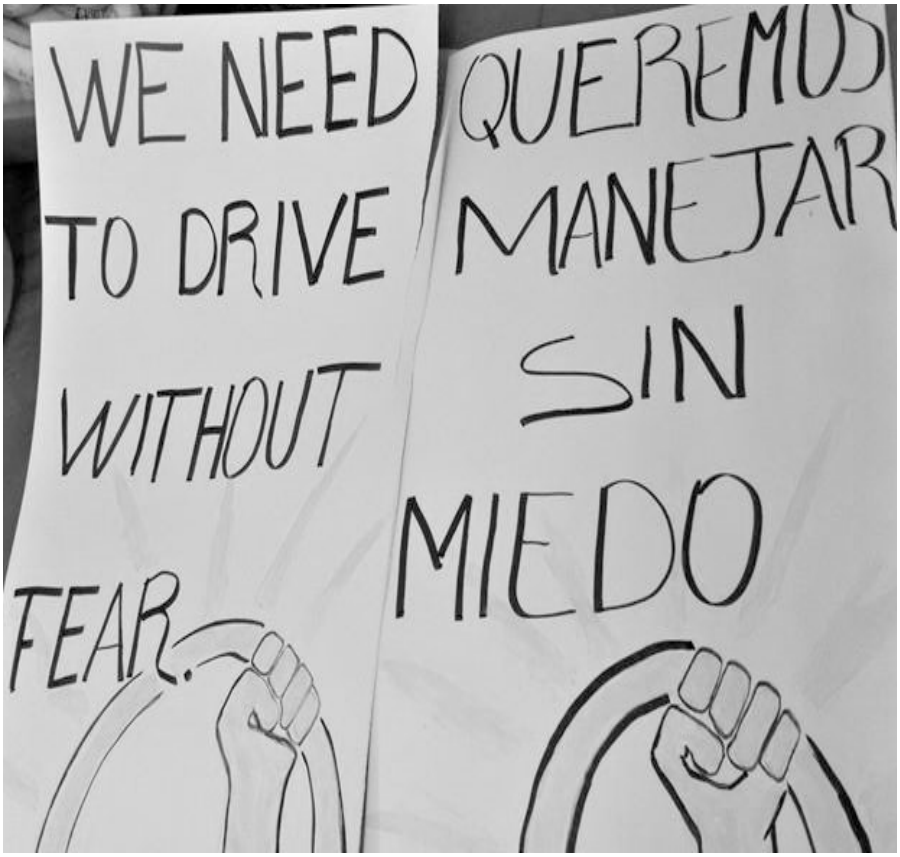
With a drivers license individuals are able to feel more protected from any discrimination and possible deportation. My mother would pick all of us up from our bus stop but one day she ran late. When my brother got off the bus he saw cops all around and walked around for an hour not knowing what to do. After being so scared that something had happened to my mom he eventually went home crying and frightened. This is something I experienced at a young age, having to face the harsh reality of our country. This is just a part of my story but there are hundreds of thousands of kids who have similar experiences such as this. We should be able to trust our community law enforcement but instead we are scared that being pulled over by then will lead to family separation.

We need to protect our driver information. Face identification is being used in order to identify individuals, without our permission. Other agencies such as ICE or other third parties could target immigrants. Their pictures can be scanned in order to find out more information such as addresses. With this they could strike against our immigrant families. For this reason we are fighting for a driver license for all regardless of status and a driver's license that protects our private information.

--Julissa, Rights Promoter with the Movement of Immigrant Leaders of PA

Beyond the privacy implications, facial recognition has a known tendency to deliver false matches for people of color. Studies of facial recognition systems have exposed detrimental inaccuracies and racial bias in facial recognition algorithms.[56] In response to the expansion of this technology in Philadelphia, Devren Washington of the Media Mobilizing Project described facial recognition as the "high tech answer to stop-and-frisk."[57] Variables such as ageing, cosmetics, inebriation, glasses, or hair are all changes that make facial recognition widely considered to be less accurate than finger printing.[58] Inaccurate facial recognition algorithms pose a colossal risk for communities who are already subjected to police surveillances and puts these groups at risk of being innocently arrested for crimes they never committed.[59] Nikki Grant of the Amistad Law Project recently testified before the Philadelphia City Council opposing the city's spending on facial recognition technology and explained that these surveillance tools empower the police to become "big brother" and normalizes the "common presence of police surveillance on the entire populace."[60]

Facial recognition companies are aware of inaccurate algorithms and the potentially devastating repercussions associated with it and because of this, some companies include disclaimers in their contracts with governmental agencies to avoid liabilities when these inaccuracies occur, leaving those agencies liable for the flawed technology.[61] Due to the serious privacy implications and the documented risk of inaccurate matches and racial bias, PennDOT should end the use of driver photos for facial recognition searches.



4 SUMMARY OF RECOMMENDATIONS

Multiple local and national news outlets have reported instances where ICE officers have utilized state driver's license databases and ran facial recognition searches on driver's license photos for enforcement purposes.[62] Considering these realities, PennDOT must ensure that the information it receives is protected. This invasion of privacy rights and lack of transparency should be corrected immediately. To protect information given to PennDOT from abuse by law enforcement officers such as ICE, the following recommendations should be put in place:

Recommendations to Protect PennDOT Information

Direct Access to PennDOT	• The Governor of Pennsylvania should issue an executive order preventing PennDOT from releasing information to ICE • PennDOT should implement a requirement for a judicial warrant before releasing any information related to an application for a license or identification card • PennDOT should issue regular public reports on the volume and nature of the requests it receives for driver information and the outcome of each request • The legislature should update the driver licensing laws to include privacy protections for all driver information
Access to Pennsylvania Databases (JNET & CLEAN)	• PennDOT should end ICE access to PennDOT information in all law enforcement databases, including JNET and CLEAN • PennDOT should make information available to the public on who can access information through these databases and make its audits of JNET and CLEAN available to the public • PennDOT should ensure that information shared with JNET and CLEAN is only available to law enforcement conducting criminal investigations who possess judicial warrants • The legislature should update the driver licensing laws to include privacy protections for information placed into law enforcement databases • The Governor of Pennsylvania should issue a moratorium on all facial recognition searches
Access to Private Data Brokers	• PennDOT's agreements to sell driver information should expressly prohibit sales to third parties, including ICE • The legislature should update the driver licensing laws to ensure that driver information is not sold to third parties without driver consent and is never sold to ICE • PennDOT should make the list of private companies available to the public and publish regular reports about the use of the data

APPENDIX I

ATTESTATION

Name of Requester: Caitlin Barry

Records Requested: Records concerning access to JNET, CLEAN and JFRS

Appeal Caption: Docket #AP-2019-2121

I, Joseph Centurione, hereby declare, pursuant to 18 Pa.C.S. § 4904, that the following statements are true and correct based upon my personal knowledge, information and belief:

1. I serve as the Business Relationship Manager within the PA Justice Network (JNET), which is an office organizationally located within the Governor's Office of Administration (Agency) and am responsible for oversight and management of JNET's business operations.

2. In my capacity as the Business Relationship Manager for JNET, I am familiar with the records of the Agency relating to JNET.

3. A current list of federal departments and their agencies, or subsidiaries,[1] as of February 24, 2020, for the purposes of settling the above-referenced appeal, which generated list is attached hereto as Exhibit "A".

4. Federal departments and agencies are not designated in their entirety as having a certain level of access for JNET data.

5. Levels of access within JNET are based on assigned roles, and those roles are specific to individual users.

6. Individual user roles within agencies are designated as either non-criminal justice (non-CJ), criminal justice (CJ) or criminal history (CH) users.

7. Before being given access to facial recognition in the JNET system, a user must be a CH user.

8. Exhibit "A" includes a designation of those federal departments or agencies that have no active users. In addition, the column labeled FR User designates that the corresponding federal agency has at least one user within that agency that has access to facial recognition through JNET, as indicated by an "x" in that column.

[1] The Requestor refers to federal departments and their subsidiaries. For purposes of this attestation, the term subsidiary and agency, when referring to a division under the "parent" federal department, may be used interchangeably.

9. Upon receipt of the Right to Know Law requests, designated in OA's files as 2019.053 and 2019.067, I conducted a thorough examination of files in the possession, custody and control of the Agency for records responsive to the request underlying this appeal. Specifically, I searched my emails, files and folders as well as shared files and folders where information of this kind would be stored. Additionally, JNET staff conducted searches in areas where similarly stored paper and electronic records would reside.

10. I also inquired with relevant Agency personnel as to whether any requested records existed in their possession, including with, staff that had in the past, or currently have, responsibility for JNET functions and processes appropriate to the request. This included the JNET Communications Manager and staff under that position and the JNET Security Administrator.

11. Based upon the above-described search of the Agency's files and inquiries with relevant Agency personnel, I have made the determination that there are no contracts (including any memorandum of understandings or agreements), between the U.S. Department of Homeland Security (DHS), or its subsidiaries, and JNET, providing DHS, or its subsidiaries, with access to JNET or the facial recognition system (FRS), within the Agency's possession, custody or control.

12. Based upon the above-described search of the Agency's files and inquiries with relevant Agency personnel, I have made the determination that there are no contracts (including any memorandum of understandings or agreements) that specifically identify DHS, or its subsidiaries, as having access to JNET or FRS, within the custody and control of the Agency.

13. Individual users within DHS, or its subsidiaries, must agree (via click through) to the JNET User Agreement prior to receiving access to JNET.

14. The Agency previously provided a redacted copy of the JNET User Agreement to the requestor.

15. JNET identified responsive emails to the portion of the underlying request (2019.053) that sought correspondence between DHS and any of its subsidiaries and OA concerning access to JNET, CLEAN or FRS.

16. The emails identified as responsive to the request outlined in paragraph 15, above, contain identifiable information concerning DHS personnel.

17. Said emails relate solely to the assignment of JNET roles, points of contact and/or account set up for specific DHS individuals and are administrative in nature.

18. The current facial recognition training provided by JNET for the facial recognition system identifies the following standards for authorized use of the facial recognition system:

    a. There is reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning a criminal activity that presents a threat to any individual, group or community.
    b. There is an active or ongoing criminal investigation.
    c. To assist in the identification of a person who lacks capacity or is otherwise unable to identify themselves, such as incapacitated, deceased or at-risk individual.
    d. To assist in the identification of potential witnesses or victims of a crime.

Date: Click here to enter a date.

Signature: 2/27/2020

Joe Centurione
Business Relationship Manager
Governor's Office of Administration

EXHBIT A

Department	Agency	Comment	FR User
US Food and Drug Administration	Office of Criminal Investigations		X
Office of National Drug Control Policy	**NO ACTIVE AGENCIES OR USERS**		
US Department of Agriculture	Office of Inspector General		
	Forest Service		
US Department of Homeland Security	Customs and Border Protection	**NO ACTIVE USERS**	
	Federal Air Marshal Service		
	Federal Protection Service		
	Immigration and Customs Enforcement		X
	Office of Inspector General		
	Secret Service		X
	Citizenship and Immigration Services		
US Department of Defence	Army		X
	Air Force		
	Defence Enterprise Support	**NO ACTIVE USERS**	
	Defence Logistics Agency		
	Navy		
	Pentagon Force Protection Agency		
US Department of the Interior	National Park Service		X
US Department of Justice	Alcohol, Tobacco and Firearms		X
	Bureau of Prisons		
	Drug Enforement Administration		X
	Federal Bureau of Investigation		X
	Marshals Service		X
	Office of Attorney General		
	Probation Office		
	Pre Trial Services	**NO ACTIVE USERS**	
US Department of Labor	Office of Inspector General		
US Department of State	Diplomatic Security Service		X
	Passport Directorate		
US Department of Transportation	**NO ACTIVE AGENCIES OR USERS**		
US Department of Education	Office of Inspector General		
US Environmental Protection Agency	Criminal Investigation Division		
	Office of Inspector General	**NO ACTIVE USERS**	
US General Services Division	Office of Inspector General		
US Department of Housing and Urban Development	Office of Inspector General		
US Office of Personnel Management	National Background Investigations Bureau		
US Postal Service	Office of Inspector General		
	Postal Inspection Service		X
US Social Security Administration	Office of Inspector General		
US Department of Treasury	Internal Revenue Service		
	Treasury Inspector General for Tax Administration		X
US Veterans Affairs	Office of Inspector General	**NO ACTIVE USERS**	
	Office of Security and Law Enforcement		

dated 2.24.2020

APPENDIX II

VILLANOVA UNIVERSITY

CHARLES WIDGER SCHOOL of LAW
FARMWORKER LEGAL AID CLINIC

September 16, 2019

Attn: OA Open Records Officer
PA Office of Administration
510 Finance Building
Harrisburg, PA 17120
Fax: (717) 346-6774; Email: RA-RTKOA@pa.gov

Re: Public Records Request – Pennsylvania Justice Network and Commonwealth Law Enforcement Assistance Network

Dear Agency Open Records Officer:

The Farmworker Legal Aid Clinic is conducting research into the federal agencies who have access to the Pennsylvania Justice Network (JNET), the Commonwealth Law Enforcement Assistance Network (CLEAN), and the JNET Facial Recognition System (JFRS).

Pursuant to Pennsylvania's Right-to-Know Law, 65 P.S. § 67.101 *et seq*. we request the following records pertaining to JNET and CLEAN. We intend this request to cover all documents, including email correspondence, memorandums, and contracts, as well as software, hardware, databases, and other technologies used by law enforcement personnel in accessing and using JNET, CLEAN, and JFRS from 2016 to present. However, we realize the following list of records is long and not all records will be relevant or available. Therefore, if it would be helpful, we welcome a phone conversation to narrow this request accordingly.

Records Requested

Please provide copies of the following records:

1. Documents pertaining to the federal Department of Homeland Security (DHS) or any of its subsidiaries, including Immigration and Customs Enforcement (ICE) and Homeland Security Investigations (HSI), and their ability to access the JNET, CLEAN or the JNET Facial Recognition System (JFRS), including:

- Any existing contracts with DHS or any of its subsidiaries providing it or its officers access to JNET, CLEAN, or JFRS.
- Contracts between the Local Technology Workgroup (LTW), which is the collaborative working group that includes the Pennsylvania State Police, Department of Corrections, Pennsylvania Board of Probation and Parole, Pennsylvania Commission on Crime and Delinquency, local police, Sherriff's and County District Attorney's, or any of its subsidiaries and DHS or any of its subsidiaries relating to access to JNET, CLEAN or JFRS.
- Correspondence between DHS and any of its subsidiaries and the PA Office of Administration relating to access to JNET, CLEAN, or JFRS.

2. Documents including the list of all users who have access to JFRS and the agencies they work for, which may include:
   - List of current criminal investigators that have been trained and granted access to JFRS.
   - List of all federal agencies who have access to JFRS or JNET Photo Search.
   - List of all users who have access to JFRS and are employed by a federal agency.
   - List of all new JFRS users who have been trained to use the system in the last two years.
3. Any documents listing the forty-four federal agencies and eight "business partners" that have access to JNET, referred to on page six of JNET's 2017-2018 Annual Report.
4. Any documents relating to DHS or any of its subsidiaries purchasing access to or providing financial resources for JFRS, JNET, or CLEAN.
5. Any documents listing the various levels of JNET, including who has access to each level.
6. Any training materials on how users access and use JFRS, JNET, or CLEAN.

This request is made on behalf of a not-for-profit organization whose mission is to teach law students and serve indigent communities. Because of our not-for-profit status and the fact that this request is about a matter of public concern, we request a fee waiver. If such a waiver is denied, please inform us in advance if the cost will be greater than $50. Additionally, we respectfully request that, if at all possible, the records be provided in electronic format and sent via email.

According to the Right-to-Know Law, a custodian of public records shall comply with a request as promptly as possible, not to exceed five business days from the date of receipt. Please furnish all responses to the Farmworker Legal Aid Clinic at flac@law.villanova.edu or:

Farmworker Legal Aid Clinic
299 North Spring Mill Road
Villanova, Pennsylvania 19085

If you have any questions or want to discuss narrowing this request, please contact me at flac@law.villanova.edu or 610-519-6839 within the above timeframe. Thank you for your prompt attention to this matter.

Sincerely,

Caitlin Barry
Director, Farmworker Legal Aid Clinic

Lauren Pugh
Student Attorney, Farmworker Legal Aid Clinic

Ricky Schneider
Student Attorney, Farmworker Legal Aid Clinic

pennsylvania
OFFICE OF OPEN RECORDS

Standard Right-to-Know Law Request Form

Good communication is vital in the RTKL process. Complete this form thoroughly and retain a copy; it is required should an appeal be necessary. You have 15 business days to appeal after a request is denied or deemed denied.

SUBMITTED TO AGENCY NAME: PA Office of Administration (Attn: AORO)

Date of Request: 9/16/2019 Submitted via: ☐ Email ☐ U.S. Mail ☐ Fax ☐ In Person

PERSON MAKING REQUEST:

Name: Caitlin Barry Company (if applicable): Farmworker Legal Aid Clinic

Mailing Address: 299 North Spring Mill Road

City: Villanova State: PA Zip: 19085 Email: flac@law.villanova.edu

Telephone: 610-519-6839 Fax: 610-519-5173

How do you prefer to be contacted if the agency has questions? ☐ Telephone ☒ Email ☐ U.S. Mail

RECORDS REQUESTED: *Be clear and concise. Provide as much specific detail as possible, ideally including subject matter, time frame, and type of record or party names. Use additional sheets if necessary. RTKL requests should seek records, not ask questions. Requesters are not required to explain why the records are sought or the intended use of the records unless otherwise required by law.*

See attached letter for records requested.

DO YOU WANT COPIES? ☒ Yes, electronic copies preferred if available
☐ Yes, printed copies preferred
☐ No, in-person inspection of records preferred (*may request copies later*)

Do you want certified copies? ☐ Yes (*may be subject to additional costs*) ☒ No

RTKL requests may require payment or prepayment of fees. See the Official RTKL Fee Schedule for more details.

Please notify me if fees associated with this request will be more than ☐ $100 (or) ☒ $50.

ITEMS BELOW THIS LINE FOR AGENCY USE ONLY

Tracking: _____ Date Received: _____ Response Due (5 bus. days): _____

30-Day Ext.? ☐ Yes ☐ No (If Yes, Final Due Date: _____) Actual Response Date: _____

Request was: ☐ Granted ☐ Partially Granted & Denied ☐ Denied Cost to Requester: $_____

☐ Appropriate third parties notified and given an opportunity to object to the release of requested records.

NOTE: In most cases, a completed RTKL request form is a public record.
More information about the RTKL is available at https://www.openrecords.pa.gov

Form updated Nov. 27, 2018

APPENDIX III

OA-2018-37

Memorandum of Understanding
DOT and JNET
(Access to Records)

Agreement No.
Federal ID No.

MEMORANDUM OF UNDERSTANDING
BETWEEN THE
DEPARTMENT OF TRANSPORTATION
AND THE
PENNSYLVANIA JUSTICE NETWORK

THIS MEMORANDUM OF UNDERSTANDING is made and entered into this 19th day of October, 2018, by and between the DEPARTMENT OF TRANSPORTATION ("PennDOT"), an executive agency of the Commonwealth of Pennsylvania;

AND

the PENNSYLVANIA JUSTICE NETWORK ("JNET"), an office under the Governor's Office of Administration of the Commonwealth of Pennsylvania.

WITNESSETH

WHEREAS, Sections 501 and 502 of the Administrative Code of 1929, as amended (71 P.S. §§ 181-182), require Commonwealth departments and agencies to coordinate their work and activities with other Commonwealth departments and agencies.

WHEREAS, PennDOT is responsible for the administration, implementation, and enforcement of the transportation, including highway, driver and vehicle services, public transit, mass transit, and aviation statutes and regulations of the Commonwealth.

WHEREAS, PennDOT collects confidential and personal information from the public, in accordance with the Pennsylvania Vehicle Code, to administer the driver license and motor vehicle programs for which it has responsibility.

WHEREAS, due to the sensitivity of the information collected, PennDOT's customer information is protected by federal and state laws and regulations that govern the collection, use, and release of personal information including, but not limited to:

a. Federal Driver's Privacy Protection Act, 18 U.S.C. §§2721 – 2725,
b. Social Security Act, 42 U.S.C. §405(c)(2)(c)(i),
c. Section 6114 of the Vehicle Code, 75 Pa. C.S. §6114,
d. Federal Privacy Act, 5 U.S.C. §552a,
e. 67 Pa. Code Chapter 95 (Sale, Publication or Disclosure of Driver, Vehicle and Accident Records and Information).

WHEREAS, the Social Security Administration (SSA) requires that any person who has access to SSA information must be advised of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for noncompliance contained

in the applicable federal and state laws; Social Security Numbers can only be provided for purposes and persons authorized under federal law.

WHEREAS, the JNET is the Commonwealth's public safety and criminal justice information broker whose integrated justice portal provides a common on-line environment for authorized users to access public safety and criminal justice information from various contributing municipal, county, state, and federal agencies.

WHEREAS, PennDOT provides suspended and expired vehicle registrations (license plate reader files), vehicle registration, operator license numbers, drivers' histories, title numbers and drivers' license photographs ("PennDOT data") via a JNET connection to Law Enforcement and Criminal Justice users.

WHEREAS, PennDOT also provides JNET with driver and vehicle data.

WHEREAS, JNET triennially audits all entities with access to JNET to ensure compliance with JNET policies, as well as federal and state statutes on security and privacy.

WHEREAS, JNET requires all users of JNET to report to JNET known events of misuse of the JNET platform and/or data, and conducts investigations into any allegations of system misuse or misuse of information obtained through the JNET system.

WHEREAS, PennDOT has an interest in ensuring that its data is used properly and JNET concurs that the integrity of PennDOT data must be maintained.

NOW, THEREFORE, the parties to this Memorandum of Understanding set forth the following as the terms and conditions of their understanding:

1. The foregoing recitals are incorporated into the terms and conditions of this Memorandum of Understanding by reference.

2. PennDOT agrees to perform the following roles and responsibilities under this Memorandum of Understanding:

    A. Provide access to Driver and Vehicle data to JNET.

    B. Provide JNET with all polices, rules, terms and conditions that govern JNET's and its users' access of PennDOT information.

    C. Review requests for access to PennDOT information and determine if granting access to PennDOT data is authorized.

    D. Determine, with the consultation of JNET, appropriate sanctions if it has been determined that PennDOT data has been misused or improperly accessed or disseminated.

    E. At its discretion, perform random access audits of users of its systems, and/or ask JNET to perform random transactional audits of PennDOT data by JNET users.

    F. Review, critique, and approve JNET developed Policies and Procedures that govern access to PennDOT Data, and ensure that they conform to the polices, rules, terms and conditions issued by PennDOT.

3. JNET agrees to perform the following roles and responsibilities under this

Memorandum of Understanding:

A. Timely review of the audit results involving the misuse of or improper access to or dissemination of PennDOT data by JNET users. Following JNET's review of the audit results JNET will:

   i. Notify the Director of PennDOT's Risk Management Office of a founded improper access or dissemination investigation of PennDOT data that was accessed through JNET in a timely manner;
   ii. Provide to the Director of PennDOT's Risk Management Office a summary of investigation or audit results involving the misuse or improper access to or dissemination of PennDOT data by JNET users;
   iii. Impose sanctions, as directed by PennDOT, for users determined to have misused or improperly accessed or disseminated PennDOT data. PennDOT shall have sole authority in the determination of all sanctions to be imposed;
   iv. Cooperate in the defense of PennDOT's determination and JNET's imposition of sanctions under this subsection.

B. Not display PennDOT provided Social Security Number on any JNET screens.

C. Ensure PennDOT policies and rules of use are documented as requested by PennDOT in user agreements, trainings, and applications.

D. Prohibit dissemination of information to unauthorized individuals or agencies.

E. Provide initial training and other subsequent training as requested or required by PennDOT to authorized users on appropriate access and use of PennDOT data (including PennDOT photos) that will include:

   a. The requirement to permanently destroy any printed and electronic information obtained through use of PennDOT systems for a matter immediately upon the conclusion or closure of the matter in accordance with laws, regulations, and applicable retention schedules. Permanent destruction is defined as the shredding or incineration of printed materials and data cleansing of electronic information in accordance with all terms and conditions of the Commonwealth website privacy and security policies that can be accessed through the following website link: http://www.oa.pa.gov/Policies/Pages/itp.aspx

   b. Procedures for using PennDOT photos.

F. Provide access to PennDOT information to criminal justice and non-criminal justice agencies/users only in accordance with PennDOT policies and with express written consent from the PennDOT Director of Information and Fiscal Services and the Director of PennDOT's Risk Management Office.

G. Terminate or suspend access to PennDOT data at the request of PennDOT.

4. JNET understands that PennDOT data is exclusively owned by PennDOT and JNET agrees not to enter into any agreement to share PennDOT data with third parties without written permission from PennDOT.

5. This Memorandum of Understanding is not intended to and does not create any contractual rights or obligations with respect to the signatory agencies or any other parties.

6. Any disputes that cannot be resolved by either party arising under this Memorandum of Understanding shall be submitted to the Office of General Counsel for final resolution.

7. This Memorandum shall take effect immediately upon execution. Either party may terminate this Memorandum after providing 30 days written notice to the other party.

IN WITNESS WHEREOF the parties hereto have executed this MEMORANDUM effective the day and year first above written.

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF TRANSPORTATION

10/5/18
Secretary (date)
FOR LESLIE S RICHARDS

COMMONWEALTH OF PENNSYLVANIA
THE GOVERNOR'S OFFICE OF ADMINISTRATION

9.4.18
Secretary (date)

Approved as to form and legality:

10/5/2018
for Chief Counsel (date)
Department of Transportation 10/5/18

8/30/18
Chief Counsel (date)
Governor's Office of Administration

10.10.18
Deputy General Counsel (date)

COMPTROLLERS APPROVAL

10/19/18
Comptroller (date)

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE OF GENERAL COUNSEL

CONFIDENTIAL AND PRIVILEGED ATTORNEY WORK PRODUCT

DATE: September 5, 2018

TO: Jason D. Sharp
Chief Counsel
Department of Transportation

FROM: Carol A. Donohoe
Office of Chief Counsel
Office of Administration

SUBJECT: #OA-2018-37 MOU between the Department of Transportation and the Office of Administration, Pennsylvania Justice Network

---

Attached is a Method of Understanding (MOU) between the Department of Transportation (PennDOT) and the Office of Administration, Pennsylvania Justice Network (JNET).

The MOU is being returned to PennDOT to route for final signatures. When the MOU is fully-executed, please return the original wet-ink signature document to my attention at the below address.

Thank you.

Attachment

Agreement Routing Sheet

Type of Agreement	**MEMORANDUM OF UNDERSTANDING**
Agreement Number	**OA201837**
Party	**PENNDOT & JNET**
City	**HARRISBURG PA**
County	**DAUPHIN**
Form Number	**None**
Federal ID Number	**00-0000000**
Amount	**0**
SAP Vendor Number	
Excess Land Number	

PLEASE SUBMIT ONLY 1 ORIGINAL - MAKE COPIES ONCE FULLY EXECUTED

EXECUTION PROCESS	RECEIVED	RETURNED
Dot Office of Chief Counsel For Preliminary Review Commonwealth Keystone Building, 9th Floor		
Secretary, DOT For Signature and Date on Agreement Commonwealth Keystone Building, 8th Floor		10.5.18
DOT Office of Chief Counsel For Final Approval 10/5/18 JMS 10/5/2018 Commonwealth Keystone Building, 9th Floor	10.5.18	10.10.18
Department Commissioner/Secretary and Office of Chief Counsel For Review and Approval		
Office of General Counsel For Review and Approval Harristown II, 333 Market Street, 17th Floor		10.10.18
DOT Office of Chief Counsel For Logging Commonwealth Keystone Building, 9th Floor	10.12.18	10.15.18
DOT Office of the Comptroller For Audit and Approval Commonwealth Keystone Building, 9th Floor RZ		10/19/18
DOT Office of Chief Counsel For Date/Final Logging Commonwealth Keystone Building	10.22.18	10.22.18

DISTRIBUTION (1 copy each):
Copy to Contractor

Copy to Comptroller-Submit electronically (no paper copies) to RA-ContractsCorresp@pa.gov. Include name of party and agreement number in the subject line.

(This address can also be located in the Outlook directory by searching for OB,ContractsCorrespondence)

APPENDIX IV

pennsylvania
OFFICE OF OPEN RECORDS

STANDARD RIGHT-TO-KNOW REQUEST FORM

DATE REQUESTED: 2/14/2019

REQUEST SUBMITTED BY: ☑ E-MAIL ☐ U.S. MAIL ☐ FAX ☐ IN-PERSON

REQUEST SUBMITTED TO (Agency name & address): PennDOT Open Records Officer, Bureau of Office Services
PennDOT, 400 North St., PO Box 3451, Harrisburg, PA 17105-3451, PENNDOT-RightToKnow@pa.gov

NAME OF REQUESTER : Vanessa Stine

STREET ADDRESS: P.O. Box 60173

CITY/STATE/COUNTY/ZIP(Required): Philadelphia, PA 19102

TELEPHONE (Optional): 215-592-1513, ext. 145 **EMAIL (optional):** vstine@aclupa.org

RECORDS REQUESTED: **Provide as much specific detail as possible so the agency can identify the information.* ***Please use additional sheets if necessary***

Please see attached sheet. Please provide records in electronic format, if possible.

DO YOU WANT COPIES? ☑ YES ☐ NO
DO YOU WANT TO INSPECT THE RECORDS? ☐ YES ☑ NO
DO YOU WANT CERTIFIED COPIES OF RECORDS? ☐ YES ☑ NO
DO YOU WANT TO BE NOTIFIED IN ADVANCE IF THE COST EXCEEDS $100? ☑ YES ☐ NO

**** PLEASE NOTE: RETAIN A COPY OF THIS REQUEST FOR YOUR FILES ****
**** IT IS A REQUIRED DOCUMENT IF YOU WOULD NEED TO FILE AN APPEAL ****

FOR AGENCY USE ONLY

OPEN-RECORDS OFFICER:

☐ I have provided notice to appropriate third parties and given them an opportunity to object to this request

DATE RECEIVED BY THE AGENCY:

AGENCY FIVE (5) BUSINESS DAY RESPONSE DUE:

***Public bodies may fill anonymous verbal or written requests. If the requestor wishes to pursue the relief and remedies provided for in this Act, the request must be in writing. (Section 702.) Written requests need not include an explanation why information is sought or the intended use of the information unless otherwise required by law. (Section 703.)*

RTK Request 1. Records identifying the databases containing PennDOT information that are accessible by law enforcement agencies, including the United States Department of Homeland Security (DHS) and/or its subcomponents.[1]

RTK Request 2. Records identifying the content and scope of each database requested in Request #1, including but not limited the information fields in the database.

RTK Request 3. Records identifying the databases, networks, or systems with which PennDOT databases are linked or interoperable, including but not limited to those operated by federal, state, county, and local governmental entities and/or private entities

RTK Request 4. Blank screen shots (i.e., without anyone's personal information displayed, or with personal information redacted) of all database screens containing PennDOT information that are accessible by law enforcement agencies, including the United States Department of Homeland Security (DHS) and/or its subcomponents, including (a) blank screen shots of all screens from the Driver's Licenses/ID database; and (b) blank screen shots of all screens from the Vehicle Registration database. For a list of DHS subcomponents, see footnote 1.

RTK Request 5. Records describing information that can be obtained through PennDOT databases by using a driver's license plate number to begin a query.

RTK Request 6. Records describing the agencies or other entities that have access to PennDOT information.

RTK Request 7. Records describing the mechanisms by which law enforcement agencies such as the United States Department of Homeland Security (DHS) and/or its subcomponents, and PennDOT share PennDOT information regarding driver's licenses and vehicle registration databases. Mechanisms include electronic access, telephone access, letter requests, subpoenas, and/or court orders by law enforcement agencies such as (DHS) and/or its subcomponents. For a list of DHS subcomponents, see footnote 1.

RTK Request 8. All current and pending DL-9002 (2-14) "Internet User Application/Licensing Agreement for Government Agencies" (or any other applications and agreements) for access to PennDOT information with United

[1] DHS subcomponents include: Immigration and Customs Enforcement (ICE), which includes Homeland Security Investigations (HSI) and Enforcement and Removal Operations (ERO); Customs and Border Protection (CBP); and United States Citizenship and Immigration Services (USCIS).

States Department of Homeland Security (DHS) and/or its subcomponents. For a list of DHS subcomponents, see footnote 1.

RTK Request 9. Records describing the access provided to PennDOT databases when Government Agencies seek access through the National Law Enforcement Telecommunications System ("NLETS").

RTK Request 10. Any records that either individually, or viewed in their entirety, constitute policies governing how other law enforcement agencies can access the vehicle and driver information databases through NLETS.

RTK Request 11. Screenshots of a request (with personal information redacted) by the United States Department of Homeland Security (DHS) and/or its subcomponents, for PennDOT information and the response thereto, including sample requests to and responses from (a) the Driver's License/ID database; (b) the Vehicle Registration database and the response thereto; (c) for "Financial Responsibility (FR)" information; and (d) "Occupational Limited Licenses (OLL)" information.

RTK Request 12. The permissible "reason codes" or other explanations of individual inquiries that law enforcement agencies, including United States Department of Homeland Security (DHS) and/or its subcomponents, may provide in order to obtain PennDOT information or records. For a list of DHS subcomponents, see footnote 1.

RTK Request 13. All communications, including but not limited to e-mail correspondence, text messages, letters, phone or electronic logs, notes on calls or meetings between PennDOT and United States Department of Homeland Security (DHS) and/or its subcomponents other than through NLETS regarding information in the Driver's License/ID database and the Vehicle Registration database from January 1, 2017 to present. For a list of DHS subcomponents, see footnote 1.

RTK Request 14. Records describing the number of all inquiries of PennDOT databases made by the United States Department of Homeland Security (DHS) and/or its subcomponents since January 1, 2017 to present, the number of such requests granted or denied during this period, and the basis for any denials.

RTK Request 15. All audits regarding access and use of databases containing PennDOT information by law enforcement agencies, including United States Department of Homeland Security (DHS) and/or its subcomponents. For a list of DHS subcomponents, see footnote 1.

RTK Request 16. All policies, guidance documents, and training material concerning PennDOT response to law enforcement requests for PennDOT information generally, including but not limited to requests for documents submitted to prove identity in the application process.

RTK Request 17. All policies, guidance documents, and training material concerning confidentiality and privacy of driver records and information.

RTK Request 18. Records that either individually, or viewed in their entirety, constitute information and/or data retention policies regarding information collected by PennDOT to verify eligibility for a driver's license and/or state identification. This includes records regarding how the information that is required pursuant to Publication 195NC(4-17) is collected and stored, as well as records regarding how PennDOT verifies immigration documents electronically with the United States Department of Homeland Security (DHS).

RTK Request 19. Records describing the information that will be made available from PennDOT databases as part of any effort to fulfill any requirement imposed by the Real ID act of 2005 to make information about driver identification and vehicle information issued in the Commonwealth of Pennsylvania available to other states.

RTK Request 20. Records describing the manner in which PennDOT will be participating in State Pointer Exchange Services ("SPEXS") and S2S platforms, networks, and services as part of any effort to fulfill any requirement imposed by the Real ID act of 2005 to make information about driver's licenses/identification issued in the Commonwealth of Pennsylvania available to other states.

RTK Request 21. Records describing PennDOT, driver and vehicle registration information that can be obtained by law enforcement agencies, including United States Department of Homeland Security (DHS) and/or its subcomponents, using data obtained through Automatic License Plate Readers ("ALPR"). For a list of DHS subcomponents, see footnote 1.

RTK Request 22. Any records that either individually, or viewed in their entirety, constitute policies regarding sharing information of driver's licenses or vehicle registration databases with the United States Department of Homeland Security (DHS) and/or its subcomponents through administrative subpoenas. For a list of DHS subcomponents, see footnote 1.

APPENDIX V

VILLANOVA UNIVERSITY

CHARLES WIDGER SCHOOL *of* LAW
FARMWORKER LEGAL AID CLINIC

September 16, 2019

Pennsylvania State Police
Bureau of Records & Identification
ATTN: Agency Open Records Officer, Mr. William Rozier
1800 Elmerton Avenue
Harrisburg, PA 17110
Fax: (717) 525-5795; Email: RA-psprighttoknow@pa.gov

Re: Public Records Request – Pennsylvania Justice Network and Commonwealth Law Enforcement Assistance Network

Dear Mr. Rozier:

The Farmworker Legal Aid Clinic is conducting research into the federal agencies who have access to the Pennsylvania Justice Network (JNET), the Commonwealth Law Enforcement Assistance Network (CLEAN), and the JNET Facial Recognition System (JFRS).

Pursuant to Pennsylvania's Right-to-Know Law, 65 P.S. § 67.101 *et seq*. we request the following records pertaining to JNET and CLEAN. We intend this request to cover all documents, including email correspondence, memorandums, and contracts, as well as software, hardware, databases, and other technologies used by law enforcement personnel in accessing and using JNET, CLEAN, and JFRS from 2016 to present. However, we realize the following list of records is long and not all records will be relevant or available. Therefore, if it would be helpful, we welcome a phone conversation to narrow this request accordingly.

Records Requested

Please provide copies of the following records:

1. Documents pertaining to the federal Department of Homeland Security (DHS) or any of its subsidiaries, including Immigration and Customs Enforcement (ICE) and Homeland Security Investigations (HSI), and their ability to access the JNET, CLEAN or the JNET Facial Recognition System (JFRS), including:
    - Any existing contracts with DHS or any of its subsidiaries providing it or its officers access to JNET, CLEAN, or JFRS.

- Contracts between the Local Technology Workgroup (LTW), which is the collaborative working group that includes the Pennsylvania State Police, Department of Corrections, Pennsylvania Board of Probation and Parole, Pennsylvania Commission on Crime and Delinquency, local police, Sherriff's and County District Attorney's, or any of its subsidiaries and DHS or any of its subsidiaries relating to access to JNET, CLEAN or JFRS.
- Correspondence between DHS and any of its subsidiaries and the PSP relating to access to JNET, CLEAN, or JFRS.

2. Documents including the list of all users who have access to JFRS and the agencies they work for, which may include:
    - List of current criminal investigators that have been trained and granted access to JFRS.
    - List of all federal agencies who have access to JFRS or JNET Photo Search.
    - List of all users who have access to JFRS and are employed by a federal agency.
    - List of all new JFRS users who have been trained to use the system in the last two years.
3. Any documents listing the forty-four federal agencies and eight "business partners" that have access to JNET, referred to on page six of JNET's 2017-2018 Annual Report.
4. Any documents relating to DHS or any of its subsidiaries purchasing access to or providing financial resources for JFRS, JNET, or CLEAN.
5. Any documents listing the various levels of JNET, including who has access to each level.
6. Any training materials on how users access and use JFRS, JNET, or CLEAN.

This request is made on behalf of a not-for-profit organization whose mission is to teach law students and serve indigent communities. Because of our not-for-profit status and the fact that this request is about a matter of public concern, we request a fee waiver. If such a waiver is denied, please inform us in advance if the cost will be greater than $50. Additionally, we respectfully request that, if at all possible, the records be provided in electronic format and sent via email.

According to the Right-to-Know Law, a custodian of public records shall comply with a request as promptly as possible, not to exceed five business days from the date of receipt. Please furnish all responses to the Farmworker Legal Aid Clinic at flac@law.villanova.edu or:

Farmworker Legal Aid Clinic
299 North Spring Mill Road
Villanova, Pennsylvania 19085

If you have any questions or want to discuss narrowing this request, please contact me at flac@law.villanova.edu or 610-519-6839 within the above timeframe. Thank you for your prompt attention to this matter.

Sincerely,

Caitlin Barry
Director, Farmworker Legal Aid Clinic

Lauren Pugh
Student Attorney, Farmworker Legal Aid Clinic

Ricky Schneider
Student Attorney, Farmworker Legal Aid Clinic

PENNSYLVANIA STATE POLICE

RIGHT-TO-KNOW LAW REQUEST

www.psp.pa.gov
1-877-RTK-PSP1 (1-877-785-7771)

REQUEST DATE: 9/16/2019

NAME OF REQUESTER: Barry (Last) Caitlin (First) (MI)
(Please Print Legibly)

MAILING ADDRESS: 299 North Spring Mill Road
(Street/PO Box)

Villanova (City) Pennsylvania (State) 19085 (Zip Code)

TELEPHONE (Optional): 610-519-6839 FAX (Optional): 610-519-5173

EMAIL (Optional): flac@law.villanova.edu

RECORDS REQUESTED: Please identify each of the documents that are subject to this request with sufficient specificity so we can ascertain whether we have these documents and how to locate them.

Please see attached letter for records requested.

To the extent that this request seeks or may be construed to seek Pennsylvania State Police records involving covert law enforcement investigations, including intelligence gathering and analysis, the Department can neither confirm, nor deny the existence of such records without risk of compromising investigations and imperiling individuals. UNDER NO CIRCUMSTANCES, therefore, should the Department's response to this request be interpreted as indicating otherwise. In all events, should such records exist, they are entirely exempt from public disclosure under the Right-to-Know Law, 65 P.S. §§ 67.101-67.3104, and the Criminal History Record Information Act, 18 Pa.C.S. §§ 9101-9183.

Production of requested public records is subject to prepayment of all RTKL fees. For security purposes, this agency will only produce public records in paper format, unless the records exclusively exist in another medium.

PLEASE MAIL, DELIVER IN PERSON, FAX, OR EMAIL YOUR REQUEST TO:

Pennsylvania State Police
Bureau of Records & Identification
ATTN: AGENCY OPEN RECORDS OFFICER
1800 Elmerton Avenue
Harrisburg, PA 17110-9758

FAX: 717-525-5795 **EMAIL: (RA-psprighttoknow@pa.gov)**

PSP/RTKL TRACKING NO.: _____ **AORO RECEIPT DATE-STAMP:** _____

FINAL RESPONSE DATE: _____ **CALCULATED RESPONSE DUE DATE:** _____

FINAL RESPONSE DUE DATE: _____

REFERENCES

1 *See generally* Soc. Just. Lawyering Clinic, Temple Univ. Beasley Sch. of L., Driver's Licenses for All: The Key to Safety and Security in Pennsylvania, (2015), https://www2.law.temple.edu/csj/files/fdl.pdf.

2 *See* Nick Sibilla, *New York and Pennsylvania Will No Longer Suspend Driver's Licenses Over Drug Crimes*, Forbes (Apr. 23, 2019), https://www.forbes.com/sites/nicksibilla/2019/04/23/new-york-and-pennsylvania-will-no-longer-suspend-drivers-licenses-over-drug-crimes/#2339145d3c33.

3 *See Gender-Neutral Designation on PennDOT Driver's Licenses and Photo ID Cards*, Pa. Dep't of Transp., https://www.dmv.pa.gov/Driver-Services/Driver-Licensing/Pages/Gender-Neutral-Designation.aspx (last visited July 10, 2020).

4 *See States Offering Driver's Licenses to Immigrants,* Nat'l Conf. of State Legislatures (Feb. 6, 2020), https://www.ncsl.org/research/immigration/states-offering-driver-s-licenses-to-immigrants.aspx.

5 *See REAL ID*, Pa. Dep't of Transp., https://www.dmv.pa.gov/REALID/pages/default.aspx (last visited July 10, 2020).

6 *See* Allie Bohm, *Yes, the States Really Reject Real ID*, Am. C.L. Union: The Campaign (Mar. 27, 2012, 3:21 PM), https://www.aclu.org/blog/national-security/yes-states-really-reject-real-id ("Montana will not agree to share its citizens' personal and private information through a national database . . . .") (quoting Brian Schweitzer, Former Governor of Montana).

7 *See New Driver's License Design*, Pa. Dep't of Transp., https://www.dmv.pa.gov/Driver-Services/Driver-Licensing/Pages/New-Driver-License-Design.aspx (last visited July 13, 2020); *see also Exciting Changes to the Pennsylvania Driver's License and Identification Card*, Pa. Dep't of Transp., PUB 802 (7-17), http://www.dot.state.pa.us/public/dvspubsforms/BDL/BDL%20Publications/PUB%20802.pdf (noting update unrelated to REAL ID Act).

8 Catie Edmundson, *ICE Used Facial Recognition to Mine State Driver's License Databases,* N.Y. Times (July 7, 2019).

9 *See* Julie Mao, Just Futures L., State Driver's License Data: Breaking Down Data Sharing and Recommendations for Data Privacy 2 (Paromita Shah & Sejal Zota eds., 2020), https://justfutureslaw.org/statedmvtech/ [hereinafter JFL Report] ("Residents should not have to choose between the risk of police arrest and ICE transfer for driving without a license and the risk of ICE showing up at their home address.").

10 *See id.* at 1 ("Data from state motor vehicle license and registration departments (herein "DMV") is one of the main sources of information that Immigration and Customs Enforcement (ICE) uses for conducting immigration enforcement."); *see also* Joseph Centurione, Pa. Office of Admin, Pa. Just. Network, Attestation, Exhibit A (Feb. 27, 2020) [hereinafter Centurione Attestation] (on file with author) (indicating ICE access to facial recognition data through JNTE).

11 *See Get a Driver's License,* Pa. Dep't of Transp., https://www.dmv.pa.gov/Driver-Services/Driver-Licensing/pages/get-driver-license.aspx (last visited July 10, 2020).

12 *See* Fact *Sheet: Identification and Legal Presence Requirements for Non-United States Citizens*, Pa. Dep't of Transp., PUB 195NC (10-19), https://www.dot.state.pa.us/Public/DVSPubsForms/BDL/BDL%20Publications/pub%20195nc.pdf.

13 *See Records Retention and Disposition Schedule*, Pa. Office of Admin. (Feb. 6, 2018) on file with author.

14 *See id.*

15 *See* Form, Pa. Dep't of Transp., Request for Data (2-19) (on file with author) (obtained through ACLU of PA Right to Know Request).

16 *See Who* is *Using JNET*, Pa. Just. Network, https://www.pajnet.pa.gov/WHO%20WE%20SERVE/Pages/Who-is-using-JNET.aspx (last visited July 10, 2020); *see also Additional Services: JNET Messaging, Web Services and Electronic Reporting*, Pa. Just. Network, https://www.pajnet.pa.gov/WHAT%20WE%20DO/Pages/Additional-Services.aspx (last visited July 10, 2020).

17 *What We Do*, Pa. Just. Network, https://www.pajnet.pa.gov/WHAT%20WE%20DO/Pages/default.aspx (last visited July 10, 2020).

18 *Id.*

19 *See Information Available on JNET*, Pa. Just. Network, https://www.pajnet.pa.gov/WHAT%20WE%20DO/Pages/Information-Available-on-JNET.aspx (last visited July 10, 2020) (indicating information available from PennDOT includes change of address, in-transit tag database, lists of expired and revoked driver's licenses, photo records, and certified vehicle records).

20 *See* Pa. Just. Network, Annual Report 2017-2018 (2018) https://www.pajnet.pa.gov/Documents/jnet_

annual_report.pdf [hereinafter JNET Annual Report 2017-2018].
21 *See id.*
22 *See id. at 6*.
23 *See id.*
24 *See* Memorandum of Understanding Between the Department of Transportation and the Pennsylvania Justice Network (Oct. 19, 2018).
25 *See Who Is Using JNET*, *supra* note 15.
26 *See* White v. Pa. Office of Admin., OOR Dkt. AP 2018-0997 (Pa. Office of Open Records July 10, 2018) (granting appeal after Office of Administration denied right-to-know request for list of JNET users); Nolen v. Pa. Office of Admin., ORR Dkt. AP 2018-0377 (Pa. Office of Open Records Apr. 13, 2018) (granting appeal after Office of Administration denied right-to-know request for contracts with JNET users).
27 *See* Pa. Just. Network, JNET & PennDOT Facial Recognition Integration (2012), https://docplayer.net/23230905-Jnet-penndot-facial-recognition-integration.html (describing how JFRS operates).
28 *See id.*
29 *See* JNET Annual Report 2017-2018, *supra* note 19.
30 *See* Centurione Attestation, *supra* note 9 at para. 18 (listing standards for authorized use of JNET's facial recognition system).
31 *See id.*, Exhibit A.
32 *See id.*
33 *See CLEAN*, Pa. State Police, https://www.psp.pa.gov/law-enforcement-services/Pages/Commonwealth-Law-Enforcement-Assistance-Network.aspx (last vistied July 11, 2020).
34 *See* Pa. State Police, Bureau of Motor Vehicles CLEAN Administration, Motor Vehicles Basic Training Presentation (Jan. 10, 2019) (unpublished PowerPoint presentation) (on file with author) (describing what driver's information is provided to CLEAN users from PennDOT).
35 *See Documents Obtained Under Freedom of Information Act: How U.S. Immigration & Customs Enforcement and State Motor Vehicle Departments Share Information*, Nat'l Immigr. L. Ctr. (May 2016), https://www.nilc.org/issues/drivers-licenses/ice-dmvs-share-information/; *see also Who We Are, Mission & Vision*, Nlets, https://www.nlets.org/about/who-we-are (last visited July 16, 2020).
36 *See* Nlets, User Policy Manual 59 (v4 ed. 2013), https://www.dropbox.com/s/anb7ah55hpptasv/3%20%20NLETS%20User%20Policy%20Manual_Redacted.pdf.
37 *See* JFL Report, supra note 8, at 9 (citing Lois Becket, *Everything We Know About What Data Brokers Know About You*, ProPublica (June 13, 2014), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you).
38 *See id.* (citing Cora Currier, *Lawyers and Scholars to LexisNexis, Thompson Reuters: Stop Helping ICE Deport People*, The Intercept (Nov. 14, 2019), https://theintercept.com/2019/11/14/ice-lexisnexis-thomson-reuters-database/).
39 *See* Commonwealth of Pa., Bureau of Audits, Report on LexisNexis Risk Solutions, Inc., (2016), https://philadelphia.cbslocal.com/wp-content/uploads/sites/15116066/2018/06/lexisnexis-report_redacted.pdf.
40 *See id.*
41 *See* McKenzie Funk, *How ICE Picks Its Targets in the Age of Surveillance*, N.Y. Times (Oct. 2, 2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html?login=email&auth=login-email.
42 *See id.* ; Max Rivlin-Nadler, *How ICE Uses Social Media to Surveil and Arrest Immigrants*, The Intercept (Dec. 22, 2019), https://theintercept.com/2019/12/22/ice-social-media-surveillance/; Joan Friedland, *How the Trump Deportation Machine Relies on Inaccurate Databases and Unregulated Data Collection*, Nat'l Immigr. L. Ctr. (Nov. 1, 2019), https://www.nilc.org/2019/11/01/inaccurate-data-unregulated-collection-fuel-deportation-machine/; *Webinar: Does ICE Have My DMV Data*, Just Futures L. (2020), https://justfutureslaw.org/wp-content/uploads/2020/03/3-10-2020.DMV_.pdf (including screen shot of a CLEAR search result).
43 *See PennDOT Making Millions of Dollars A Year Selling Drivers' Data*, CBS Philly (June 26, 2018), https://philadelphia.cbslocal.com/2018/06/26/penndot-making-millions-of-dollars-a-year-by-selling-drivers-data/; Mitch Blacher, *PennDOT Selling Drivers' Personal Information?* NBC10 Phila. (Jan. 11, 2016), https://www.nbcphiladelphia.com/news/local/penndot-selling-drivers-personal-information-nbc10-investogators/2021606/.
44 H.R. 100, Print No. 578, at 2, Gen. Assemb., Reg. Sess. (Pa. 2007) [hereinafter H.R. 100] (memorializing resolution for United States Congress to repeal or delay the creation of a national identification card and the implementation of Real ID Act of 2005) https://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=PDF&sessYr=2007&sessInd=0&billBody=H&billTyp=R&billNbr=0100&pn=0578.

45 *See id.* at 4.
46 *See id.* at 2–3.
47 *Id.* at 2.
48 *See id.* at 3.
49 *See States Offering Driver's Licenses to Immigrants*, Nat'l Conf. St. Legislatures (Feb. 6, 2020), https://www.ncsl.org/research/immigration/states-offering-driver-s-licenses-to-immigrants.aspx#:~:text=These%20states%E2%80%94California%2C%20Colorado%2C,consular%20card%20and%20evidence%20of.
50 *See id.*
51 *See* H.R. 100, *supra* note 44, at 2.
52 Pa. State Educ. Ass'n v. Commonwealth, 148 A.3d 142, 158 (Pa. 2016).
53 *Id.*
54 *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (referring to Google's chairman in 2011 saying that technology that readily identifies everyone based on his or her face could be used "in a very bad way").
55 *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
56 *See* PERPETUAL LINE-UP, *supra* note 54.
57 Samantha Melamed, *Philly Police Use of Clearview AI was Just 'a Test' — but Facial Recognition is Already Here*, Phila. Inquirer (Mar. 5, 2020), https://www.inquirer.com/news/clearview-ai-philadelphia-police-department-facial-recognition-20200305.html?fbclid=IwAR1ucTRDR9N-SyF67qIWVe5Ce0_KvLy3qhdAiH60ljswEiTc-3my9os96bjo
58 *See* PERPETUAL LINE-UP, *supra* note 54 (finding "in the wild" photos create an even high chance of inaccuracy in facial recognition).
59 *See e.g.*, Bobby Allyn, *'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man*, NPR (June 24, 2020), https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig (reporting of how police in Detroit relied on facial recognition of grainy security video to incorrectly detain a gentleman of color who was innocent of crime).
60 Nikki Gee, Amistad Law Project, Testimony before Philadelphia City Council (June 4, 2020), https://www.facebook.com/AmistadLaw/videos/271068777280294/ (arguing against use of facial recognition software by Philadelphia Police Department and against 14 million dollar increase in police budget). "The issue is twofold. Not only is this a concern about how FRS chills freedom of speech and props up mass incarceration, I am also concerned about how these technologies drain resources from our communities and siphons away tax dollars." *Id.*
61 See Perpetual Line-Up, supra note 54 (referring to FaceFirst's 2015 contract with San Diego Association of Governments, which included a disclaimer that "FaceFirst makes no representations or warranties as to the accuracy and reliability of the product in the performance of its facial recognition capabilities").
62 *See, e.g.,* Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Database*, N.Y. Times (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html; Drew Harwell, *FBI, ICE Find State Driver's License Photos are a Gold Mine for Facial-Recognition Searches*, Wash. Post (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/; Nina Shapiro, *Washington State Regularly Gives Drivers' Info to Immigration Authorities; Inslee Orders Temporary Halt*, Seattle Times (Jan. 11, 2018), https://www.seattletimes.com/seattle-news/times-watchdog/washington-state-regularly-gives-drivers-info-to-immigration-authorities-inslee-orders-temporary-halt/; Drew Harwell & Erin Cox, *ICE has run Facial-Recognition Searches on Millions of Maryland Drivers*, Wash. Post (Feb. 26, 2020), https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/.

DRIVING PA FORWARD
SEPTEMBER 2020